# CyberArk

## Exam Questions PAM-DEF

CyberArk Defender - PAM

**NEW QUESTION 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

**Answer:** B

**Explanation:**
This parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests. It is set in the Master Policy under the Dual Control section. The value of this parameter determines the frequency of the CPM's verification process for accounts that have been accessed by users who have received confirmation from authorized Safe owners. The CPM will change the password of these accounts according to the value of this parameter. References:
? Dual Control - CyberArk
? Dual control in V10 Interface - docs.cyberark.com
? PAM-DEF CyberArk Defender – PAM

**NEW QUESTION 2**
A Vault Administrator team member can log in to CyberArk, but for some reason, is not given Vault Admin rights.
Where can you check to verify that the Vault Admins directory mapping points to the correct AD group?

A. PVWA > User Provisioning > LDAP Integration > Mapping Criteria
B. PVWA > User Provisioning > LDAP Integration > Map Name
C. PVWA > Administration > LDAP Integration > Mappings
D. PVWA > Administration > LDAP Integration > AD Groups

**Answer:** C

**Explanation:**
The directory mappings are the rules that define how users and groups from an external directory, such as Active Directory (AD), are mapped to roles and authorizations in CyberArk. To verify that the Vault Admins directory mapping points to the correct AD group, you need to check the Mappings page in the PVWA. This page displays the list of existing directory mappings in the Vault and their properties, such as mapping name, LDAP branch, domain groups, and mapping authorizations. You can edit or delete a directory mapping from this page, or create a new one using the Create Directory Mapping
button. References: Directory Maps, Create directory mapping, Get directory mapping list

**NEW QUESTION 3**
The primary purpose of exclusive accounts is to ensure non-repudiation (Individual accountability).

A. TRUE
B. FALSE

**Answer:** A

**Explanation:**
The primary purpose of exclusive accounts is to ensure non-repudiation (individual accountability). Exclusive accounts are accounts that can only be used by one user at a time, and are locked during usage. This means that no other user can access the same account until the current user releases it or the session expires. By using exclusive accounts, the organization can enforce individual accountability and traceability for the actions performed on the target systems. Exclusive accounts also reduce the risk of credential theft and unauthorized access, as the passwords are changed every time they
are retrieved by a user1. Exclusive accounts can be configured in the Master Policy under the Password Management section, by enabling the Exclusive Access rule2. References:
? 1: The Master Policy, One Time Password subsection
? 2: The Master Policy, Exclusive Access subsection

**NEW QUESTION 4**
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 Operations Staff 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 Operations Managers never need to be able to use the show, copy or connect buttons themselves.
Which safe permission do you need to grant Operations Staff? Check all that apply.

A. Use Accounts
B. Retrieve Accounts
C. Authorize Password Requests
D. Access Safe without Authorization

**Answer:** AB

**Explanation:**
To use the show, copy, and connect buttons on the accounts in the safe UnixRoot, the Operations Staff need to have the Use Accounts permission, which allows them to request access to the accounts and perform actions on them. However, since dual control is enabled for some of the accounts, they also need to have the Retrieve Accounts permission, which allows them to view the password of the account after it is authorized by another user. The Authorize Password Requests permission is not needed, as it is only required for the users who can approve the requests, not the ones who make them. The Access Safe without Authorization permission is not needed, as it would bypass the dual control mechanism and allow the Operations Staff to access the accounts without approval. References:
? [Defender PAM Sample Items Study Guide], page 10, question 5
? [CyberArk Privileged Access Security Implementation Guide], page 30, table 2-1
? [CyberArk Privileged Access Security Administration Guide], page 43, section 3.2.2.1

**NEW QUESTION 5**
Which option in the Private Ark client is used to update users' Vault group memberships?

A. Update > General tab
B. Update > Authorizations tab
C. Update > Member Of tab
D. Update > Group tab

**Answer:** C

**Explanation:**
In the Private Ark client, to update users' Vault group memberships, you use the Update > Member Of tab. This tab allows administrators to manage which groups a user is a member of. By adding or removing groups in this tab, you can effectively update the user's group memberships and, consequently, their access permissions within the Vault1.
References:
? CyberArk's official documentation on managing users in the Private Ark client, which includes instructions on how to update users' group memberships

**NEW QUESTION 6**
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.

**Answer:** D

**Explanation:**
A linked account is an account that is associated with another account to enable the password management process. A linked account can be used for various purposes, such as logging on to a target system, changing the password of another account, or enabling privileged commands. A linked account can be defined either on the platform level or on the account level, depending on the type and scope of the linked account. The types of linked accounts that are supported by CyberArk are1:
? Logon account: An account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the CPM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the CPM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account.
? Reconcile account: An account that contains the password used in reconciliation processes. Reconciliation is a process that restores the password of a privileged account to the value that is stored in the Vault, in case it is changed or out of sync. A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the target account, the CPM can use the reconcile account to restore the password of the target account, in case it is changed or out of sync.
? Other additional accounts: Additional accounts can be used in various cases. For example:
The other options are not the purpose of a linked account, because:
? A. To ensure that a particular collection of accounts all have the same password.
This is not the purpose of a linked account, but of a group account. A group account is an account that is associated with multiple target systems that share the same credentials. A group account allows the CPM to manage the password of multiple systems with a single password object in the Vault2.
? B. To ensure a particular set of accounts all change at the same time. This is not the purpose of a linked account, but of a password change schedule. A password change schedule is a feature that allows the administrator to define a time frame for changing the passwords of a set of accounts. A password change schedule can be configured either in the Master Policy or in the Platform settings3.
? C. To connect the CPNI to a target system. This is not the purpose of a linked account, but of a service account. A service account is an account that is used by a service or an application to connect to a target system. A service account can be managed by the Central Credential Provider (CCP), which is a component that provides applications and services with the credentials they need to access target systems4.
References:
? 1: Linked Accounts
? 2: Group Accounts
? 3: Password Change Schedule
? 4: Service Accounts

**NEW QUESTION 7**
What is the purpose of the PrivateArk Database service?

A. Communicates with components
B. Sends email alerts from the Vault
C. Executes password changes
D. Maintains Vault metadata

**Answer:** D

**Explanation:**
The purpose of the PrivateArk Database service is to maintain the Vault metadata, which includes the information about the Safes, accounts, policies, users, groups, and audit records that are stored in the Vault. The PrivateArk Database service is a Windows service that manages the database files that contain the Vault data. The PrivateArk Database service is responsible for creating, updating, deleting, and backing up the database files, as well as performing encryption and compression operations on the data1. The PrivateArk Database service is installed automatically as part of the Vault server installation and can be configured using the DBParm.ini file2.
The other options are not the purpose of the PrivateArk Database service, although they may be related to other services or components of the Vault. The PrivateArk Server service is the service that communicates with the components, such as the PVWA, the CPM, the PSM, and the PTA, and handles the requests from the clients and components3. The Event Notification Engine service is the service that sends email alerts from the Vault, based on predefined events and recipients4. The Central Policy Manager component is the component that executes password changes, verifications, and reconciliations for the accounts that are managed by the Vault. References:
? Server Components - CyberArk, section “The PrivateArk Server process (Dbmain)”
? DBParm.ini - CyberArk, section “Main parameters”

? Server Components - CyberArk, section “The PrivateArk Server process (Dbmain)”
? Event Notification Engine - CyberArk, section “Event Notification Engine”
? [Change Passwords - CyberArk], section “Change Passwords”

**NEW QUESTION 8**
A user is receiving the error message “ITATS006E Station is suspended for User jsmith” when attempting to sign into the Password Vault Web Access (PVWA).
Which utility would a Vault administrator use to correct this problem?

A. createcredfile.exe
B. cavaultmanager.exe
C. PrivateArk
D. PVWA

**Answer:** C

**Explanation:**
The PrivateArk is a utility that allows the Vault administrator to access and manage the Vault data, users, groups, policies, and settings. The PrivateArk can be used to correct the problem of a user receiving the error message “ITATS006E Station is suspended for User jsmith” when attempting to sign into the PVWA. The error message means that the user has exceeded the number of invalid password attempts and has been locked out from the Vault. To unlock the user, the Vault administrator can use the PrivateArk to activate the suspended station for the user in the Trusted Net Areas1.
The other options are not utilities that can be used to correct this problem. The createcredfile.exe is a utility that creates a credential file for the CPM to connect to the target systems2. The cavaultmanager.exe is a utility that performs various Vault maintenance tasks, such as backup, restore, and encryption3. The PVWA is not a utility, but a web interface that allows the users to access and use the Vault features, such as
managing accounts, requesting passwords, and initiating sessions. References:
? Vault - ITATS006E Station is suspended for User Administrator - force.com, section “Resolution”
? Create a Credential File - CyberArk, section “Create a Credential File”
? Vault Maintenance - CyberArk, section “Vault Maintenance”
? [Password Vault Web Access - CyberArk], section “Password Vault Web Access”

**NEW QUESTION 9**
You want to give a newly-created group rights to review security events under the Security pane. You also want to be able to update the status of these events.
Where must you update the group to allow this?

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

**Answer:** D

**Explanation:**
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security- Events.htm?TocPath=End%20User%7CSecurity%20Events%7C
2#Permissions

**NEW QUESTION 10**
Which command configures email alerts within PTA if settings need to be changed post install?

A. /opt/tomcat/utility/emailConfiguration.sh
B. /opt/PTA/emailConfiguration.sh
C. /opt/PTA/utility/emailConfig.sh
D. /opt/tomcat/utility/emailSetup.sh

**Answer:** A

**Explanation:**
The command to configure email alerts within PTA (Privileged Threat Analytics) after the initial installation is /opt/tomcat/utility/emailConfiguration.sh. This command is used to start the PTA utility that allows you to set up email notifications for various alerts. During the configuration process, you will be prompted to enter details such as the SMTP/S protocol, email server IP address, SMTP port, sender’s email address, and recipient’s email address. If the mail server requires authentication, you will also need to provide the username and password for the user that will send email notifications1. References:
? CyberArk’s official documentation provides a detailed procedure on how to configure PTA to send alerts to emails, including the use of the
/opt/tomcat/utility/emailConfiguration.sh command

**NEW QUESTION 10**
What does the minvalidity parameter on a platform policy determine?

A. time between a password retrieval and the account becoming eligible for a password change
B. timeout for users signed into the PVWA as configured in the global settings
C. minimum amount of time that Just in Time access is valid
D. time in minutes before an empty safe will be automatically deleted

**Answer:** A

**Explanation:**
The minvalidity parameter on a platform policy in CyberArk determines the minimum amount of time that must pass between the retrieval of a password and when the account becomes eligible for a password change. This parameter ensures that a user has a guaranteed period to use the password before it is changed again, providing stability and predictability in password management1. References: The information provided is based on general knowledge of CyberArk PAM best practices and the functionality of the minvalidity parameter as outlined in CyberArk’s official documentation

**NEW QUESTION 15**
You are concerned about the Windows Domain password changes occurring during business hours.
Which settings must be updated to ensure passwords are only rotated outside of business hours?

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

**Answer:** B

**Explanation:**
To ensure that Windows Domain password changes occur outside of business hours, the settings that must be updated are found in the Master Policy under the Account Change Window section. Here, you can specify the ToHour and FromHour to define the time frame outside of which the passwords should be rotated. This setting allows you to control when password changes can occur, ensuring
that they do not interfere with business operations by taking place during non-business hours1.
References:
? CyberArk Docs - Set password policies

**NEW QUESTION 17**
It is possible to restrict the time of day, or day of week that a [b]verify[/b] process can occur

A. TRUE
B. FALSE

**Answer:** A

**Explanation:**
It is possible to restrict the time of day, or day of week that a verify process can occur by using the Verify Time Window parameter in thePlatform Management page. This parameter allows the administrator to define a time window for each platform, during which the verify process can be performed. The verify process will not run outside of this time window, unless it is manually initiated by the administrator. This feature can help reduce the load on the target systems and the network during peak hours. References:
? [Defender PAM Course], Module 4: Managing Accounts, Lesson 2: Account Verification, Slide 8: Verify Time Window
? [Defender PAM Documentation], Version 12.3, Administration Guide, Chapter 4: Managing Platforms, Section: Verify Time Window

**NEW QUESTION 18**
When a DR Vault Server becomes an active vault, it will automatically fail back to the original state once the Primary Vault comes back online.

A. True; this is the default behavior
B. False; this is not possible
C. True, if the AllowFailback setting is set to “yes” in the padr.ini file
D. True, if the AllowFailback setting is set to “yes” in the dbparm.ini file

**Answer:** C

**Explanation:**
When a DR Vault Server becomes an active vault, it will automatically fail back to the original state once the Primary Vault comes back online, if the AllowFailback setting is set to “yes” in the padr.ini file. The padr.ini file is the configuration file for the Disaster Recovery application, which enables the DR Vault to replicate data from the Primary Vault and take over its role in case of a failure. The AllowFailback setting determines whether the DR Vault will automatically switch back to the passive mode when the Primary Vault is restored. The default value of this setting is “no”, which means that the DR Vault will remain active until a manual failback is performed1. To enable the automatic
failback, the setting must be changed to “yes” and the padr service must be restarted1. The dbparm.ini file is not relevant to this setting, as it is the main configuration file for the Vault database2. References:
? Configure the DR Vault - CyberArk, section “AllowFailback”
? DBParm.ini - CyberArk, section “Main parameters”

**NEW QUESTION 22**
To ensure all sessions are being recorded, a CyberArk administrator goes to the master policy and makes configuration changes.
Which configuration is correct?

A. Require privileged session monitoring and isolation = inactive; Record and save session activity = active.
B. Require privileged session monitoring and isolation = inactive; Record and save session activity = inactive.
C. Require privileged session monitoring and isolation = active; Record and save session activity = active.
D. Require privileged session monitoring and isolation = active; Record and save session activity = inactive.

**Answer:** C

**Explanation:**
This configuration ensures that privileged sessions are monitored and isolated, and all session activities are recorded and saved for future reference 1.

**NEW QUESTION 25**
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

**Answer:**

C

**Explanation:**
According to the CyberArk Defender PAM documentation1, the Vault administrator can apply a new license file by uploading the license.xml file to the Vault Internal Safe and restarting the PrivateArk Server service. The Vault Internal Safe is a special Safe that contains the Vault configuration files, including the license file. The Vault administrator can access this Safe from the PrivateArk Client and replace the existing license file with the new one. After that, the Vault administrator must restart the PrivateArk Server service for the changes to take effect. This procedure can be done either from the Vault machine or from a remote machine.
References:
? Manage the CyberArk License - CyberArk

**NEW QUESTION 29**
An auditor needs to login to the PSM in order to live monitor an active session. Which user ID is used to establish the RDP connection to the PSM server?

A. PSMConnect
B. PSMMaster
C. PSMGwUser
D. PSMAdminConnect

**Answer:** A

**Explanation:**
The PSMConnect user is a local user on the PSM server that is used to establish RDP connections to the PSM server. The PSMConnect user has the following permissions: Log on locally, Log on as a batch job, and Allow log on through Remote Desktop Services. The PSMConnect user is also a member of the local group PSMUsers, which has access to the PSM web console. The other user IDs are not used for RDP connections to the PSM server. The PSMMaster user is a local user on the PSM server that is used to run the PSM services. The PSMGwUser user is a local user on the PSM server that is used to run the PSM Gateway service. The PSMAdminConnect user is a local user on the PSM server that is used to connect to the PSM web console as an administrator. References: Privileged Session Manager, Defender - PAM, PSM for Web Console, Connect through PSM for SSH

**NEW QUESTION 33**
Which certificate type do you need to configure the vault for LDAP over SSL?

A. the CA Certificate that signed the certificate used by the External Directory
B. a CA signed Certificate for the Vault server
C. a CA signed Certificate for the PVWA server
D. a self-signed Certificate for the Vault

**Answer:** A

**Explanation:**
To enable SSL-based encryption for LDAP integration, the Vault machine and the PVWA machine need to trust the certificate used by the External Directory. This can be achieved by importing the CA Certificate that signed the certificate used by the External Directory into the Windows certificate store on both the Vault and PVWA machines. This will facilitate an SSL connection between the Vault and the External Directory. References: Configure the Vault for LDAP, Configure LDAPS in CyberArk. What certificate I need to use?

**NEW QUESTION 35**
The Vault administrator can change the Vault license by uploading the new license to the system Safe.

A. True
B. False

**Answer:** A

**Explanation:**
According to the web search results, the Vault administrator can change the Vault license by uploading the new license to the system Safe123. This can be done either from the Vault machine or from a remote machine using the PrivateArk client. The new license file should be named license.xml and replace the current one in the system Safe. This can be done without having to reinstall the Vault or restart the service.

**NEW QUESTION 39**
What do you need on the Vault to support LDAP over SSL?

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

**Answer:** A

**Explanation:**
To support LDAP over SSL, the Vault requires the CA Certificate(s) that were used to sign the certificate of the External Directory. This is necessary to establish a trusted SSL connection between the Vault and the External Directory. The CA Certificate(s) must be imported into the Windows certificate store on the Vault machine to facilitate this SSL connection1. References: The information provided is based on general knowledge of CyberArk PAM best practices and the requirements for configuring LDAP over SSL as outlined in CyberArk’s official documentation1.

**NEW QUESTION 41**
Which of the following properties are mandatory when adding accounts from a file? (Choose three.)

A. Safe Name

B. Platform ID
C. All required properties specified in the Platform
D. Username
E. Address
F. Hostname

**Answer:** ABC

**Explanation:**
When adding accounts from a file, certain properties are mandatory to ensure that the accounts can be properly managed within the CyberArk Privileged Access Security system. The Safe Name is required to determine where the account will be stored.
The Platform ID is necessary to apply the correct management policies to the account. Additionallya, ll required properties specified in the Platform must be included to meet the specific requirements for account management as defined by the platform configuration1.
References:
? CyberArk's official documentation on adding multiple accounts from a file, which outlines the mandatory information needed for each account, including Safe Name, Platform ID, and other required properties based on the account's policy requirements1.

**NEW QUESTION 46**
A password compliance audit found:
1) One-time password access of 20 domain accounts that are members of Domain Admins group in Active Directory are not being enforced.
2) All the sessions of connecting to domain controllers are not being recorded by CyberArk PSM.
What should you do to address these findings?

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

**Answer:** A

**Explanation:**
To address the findings of the password compliance audit, you should edit the Master Policy in CyberArk Privileged Access Manager. The Master Policy is where you can enforce one-time password access and record session activity. One-time password access ensures that each password is used only once and then changed, which is a security measure to prevent unauthorized reuse of passwords1. Recording session activity is a feature of the Privileged Session Manager (PSM) that allows all activities during a session to be recorded for auditing purposes2. By enabling these settings in the Master Policy, you ensure that the domain accounts have one-time password access enforced and that all sessions connecting to domain controllers are recorded by CyberArk PSM. References:
? CyberArk Docs: One-time passwords and exclusive accounts1

**NEW QUESTION 48**
Before failing back to the production infrastructure after a DR exercise, what must you do to maintain audit history during the DR event?

A. Ensure that the Production Instance replicates changes that occurred from the Disaster Recovery Instance.
B. Briefly stop and start the Disaster Recovery Instance before attempting to fail components back to the Production Instance.
C. Stop the CPM services before starting the production server.
D. Perform an IIS Reset on all PVWA servers.

**Answer:** A

**Explanation:**
Before failing back to the production infrastructure after a Disaster Recovery (DR) exercise, it is crucial to ensure that the Production Instance replicates all changes that occurred from the Disaster Recovery Instance. This includes all audit history and any other changes made during the DR event. The replication process ensures that no data is lost and that the audit history is maintained consistently across both the DR and Production environments1.
References:
? CyberArk Docs - Reports and Audits1
? CyberArk Docs - Vault Audit Action Codes2
? CyberArk Blog - Failover and Failback Process

**NEW QUESTION 53**
You are creating a shared safe for the help desk.
What must be considered regarding the naming convention?

A. Ensure your naming convention is no longer than 20 characters.
B. Combine environments, owners and platforms to minimize the total number of safes created.
C. Safe owners should determine the safe name to enable them to easily remember it.
D. The use of these characters V:*<>".| is not allowed.

**Answer:** D

**Explanation:**
When creating a shared safe for the help desk in CyberArk's Privileged Access Management (PAM), it is important to adhere to the naming conventions set forth by CyberArk. One of the key considerations is that certain characters are not permitted in the safe name. Specifically, the characters V:*<>".| are not allowed in the naming of safes. This is to ensure compatibility and prevent issues with the file system or the CyberArk application itself, as these characters may interfere with normal operations or be reserved for specific functions within the operating system or the application.
References: The information regarding safe naming conventions is based on CyberArk's best practices and guidelines, which are detailed in the official CyberArk documentation and study guides. It is important to consult the CyberArk Defender PAM resources and documents to ensure compliance with these standards

**NEW QUESTION 57**
When running a "Privileged Accounts Inventory" Report through the Reports page in PVWA on a specific safe, which permission/s are required on that safe to

show complete account inventory information?

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

**Answer:** A

**Explanation:**
The Privileged Accounts Inventory Report provides information about all the privileged accounts in the system, based on different filters, such as safe, platform, policy, and owner. To run this report through the Reports page in PVWA on a specific safe, the user needs to have the following permissions on that safe:
? List Accounts: This permission allows the user to view the accounts in the safe and their properties, such as name, address, platform, and policy.
? View Safe Members: This permission allows the user to view the members of the safe and their authorizations, such as owners, users, and groups.
These permissions are required to show complete account inventory information for the specific safe. Other permissions, such as Manage Safe Owners, Access Safe without confirmation, Manage Safe, and View Audit, are not relevant for this report. References: Reports and Audits - CyberArk, Safe Member Authorizations

**NEW QUESTION 61**
What is the maximum number of levels of authorization you can set up in Dual Control?

A. 1
B. 2
C. 3
D. 4

**Answer:** B

**Explanation:**
Dual Control is a feature that allows you to set up a workflow for approving access requests to sensitive accounts. You can configure up to two levels of authorization for each account, meaning that you need up to two different authorizers to approve the request before the user can access the account. The authorizers can be either users or groups, and they can have different approval methods, such as email, SMS, or CyberArk interface. References:
? [Defender PAM] course, Module 5: Privileged Session Management, Lesson 5.2:
Dual Control
? [Defender PAM Sample Items Study Guide], Question 31
? [CyberArk Documentation], Dual Control

**NEW QUESTION 63**
What is the configuration file used by the CPM scanner when scanning UNIX/Linux devices?

A. UnixPrompts.ini
B. plink.exe
C. dbparm.ini
D. PVConfig.xml

**Answer:** A

**Explanation:**
The configuration file used by the CPM scanner when scanning UNIX/Linux devices is UnixPrompts.ini. This file is located in the CPM scanner installation folder and can be customized according to the UNIX/Linux machine's specific configuration. The file contains parameters that define the prompts and paths for various commands and files used by the CPM scanner, such as login password, sudo password, sudo error, passwd file, group file, shadow file, and sudoers file.
References: Configure the CPM
Scanner, CPM Scanner parameters file (CACPMScanner.exe.config)

**NEW QUESTION 67**
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. Edith 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:** D

**Explanation:**
Dual Control is a feature that requires the approval of another user before accessing a password. It is based on a Master Policy rule that applies to all accounts attached to platforms that have this rule enabled. However, there may be situations where a group of users needs to access a password without approval, such as in an emergency or for troubleshooting purposes. In this case, an exception can be made by granting the group the 'Access safe without confirmation' authorization on the safe in which the account is stored. This authorization bypasses the Dual Control workflow and allows the group to retrieve the password without waiting for approval. However, the password retrieval will still be audited and recorded in the Vault.

**NEW QUESTION 68**
Which of the following are secure options for storing the contents of the Operator CD, while still allowing the contents to be accessible upon a planned Vault restart? (Choose three.)

A. Store the CD in a physical safe and mount the CD every time Vault maintenance is performed
B. Copy the entire contents of the CD to the system Safe on the Vault
C. Copy the entire contents of the CD to a folder on the Vault Server and secure it with NTFS permissions
D. Store the server key in a Hardware Security Module (HSM) and copy the rest the keys from the CD to a folder on the Vault Server and secure it with NTFS

permissions

**Answer:** ABD

**Explanation:**
? A. Store the CD in a physical safe and mount the CD every time Vault maintenance is performed. This option ensures that the CD is kept in a secure location when not in use, and that the keys are available when needed. This is the default option suggested by CyberArk1.
? B. Copy the entire contents of the CD to the system Safe on the Vault. This option allows the Vault to access the keys from the system Safe, which is a special Safe that stores the Vault configuration files and keys. The system Safe is encrypted and protected by the Vault, and can only be accessed by authorized users2.
? D. Store the server key in a Hardware Security Module (HSM) and copy the rest the keys from the CD to a folder on the Vault Server and secure it with NTFS permissions. This option provides an additional layer of security for the server key, which is the most critical key for the Vault. An HSM is a physical device that stores and manages cryptographic keys in a tamper-resistant and isolated environment. The Vault can integrate with an HSM to store and retrieve the server key3. The rest of the keys can be stored in a folder on the Vault Server and secured with NTFS permissions, which restrict access to authorized users and groups.
The following option is not secure and should be avoided:
? C. Copy the entire contents of the CD to a folder on the Vault Server and secure it with NTFS permissions. This option exposes the keys to potential risks, such as unauthorized access, data corruption, or deletion. NTFS permissions are not sufficient to protect the keys from malicious or accidental actions. Moreover, this option does not comply with the CyberArk best practices, which recommend to store the keys on a removable media or an HSM

**NEW QUESTION 73**
Your organization has a requirement to allow users to “check out passwords” and connect to targets with the same account through the PSM.
What needs to be configured in the Master policy to ensure this will happen?

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

**Answer:** A

**Explanation:**
The Master Policy in CyberArk allows organizations to permit users to check out a ‘one-time’ password and lock it so that no other users can retrieve it at the same time. After the user has used the password, they check the password back into the Vault, ensuring exclusive usage of the privileged account. This is achieved by setting the ‘Enforce check-in/check-out exclusive access’ to active. Additionally, to ensure that all sessions are monitored and isolated, the ‘Require privileged session monitoring and isolation’ must also be set to active. This combination of settings guarantees both the exclusive access to privileged accounts and the necessary session monitoring for security and compliance purposes1.
References:
? CyberArk’s official documentation on Account check-out and check-in1.
? The Master Policy overview provided by CyberArk2.

**NEW QUESTION 77**
According to the DEFAULT Web Options settings, which group grants access to the REPORTS page?

A. PVWAUsers
B. Vault Admins
C. Auditors
D. PVWAMonitor

**Answer:** C

**Explanation:**
According to the CyberArk Defender-PAM study guide, the REPORTS page is used to generate reports on various aspects of the CyberArk Privileged Access Management Solution, such as user activity, password usage, and compliance status. The default group that grants access to the REPORTS page is the Auditors group, which is a built-in group in the Vault that has the AuditUsers authorization. Members of the Auditors group can view and generate reports, but cannot modify them. References:
? CyberArk Defender-PAM study guide, page 17, section 3.2.1
? CyberArk Privileged Access Security Documentation, page 48, section 2.3.2.1

**NEW QUESTION 80**
Where can you check that the LDAP binding is using TCP/636?

A. in Active Directory under "Users OU" => "User Properties" => "External Bindings" => "Port"
B. in PVWA, under "LDAP Integration" => "LDAP" => "Directories" => "" => "Hosts" => "Host"
C. in PrivateArk Client, under "Tools" => "Administrative Tools" => "Directory Mapping" => ""
D. From the PVWA, connect to the domain controller using Test-NetConnection on Port 636.

**Answer:** D

**Explanation:**
To check that the LDAP binding is using TCP/636, you can use the Test- NetConnection cmdlet from the PVWA to connect to the domain controller on Port 636. This method allows you to verify that the LDAP service is listening on the secure port and that the connection can be established using SSL/TLS, which is typically associated with port 6361.
References:
? CyberArk Docs - LDAP Integration2
? CyberArk Knowledge Article - How to test outgoing LDAP external directory connectivity to the vault

**NEW QUESTION 85**
Which of the following components can be used to create a tape backup of the Vault?

A. Disaster Recovery

B. Distributed Vaults
C. Replicate
D. High Availability

**Answer:** C

**Explanation:**
The Replicate component can be used to create a tape backup of the Vault. The Replicate component is a utility that exports the encrypted contents of the Safes and the Vault metadata to a computer outside the Vault environment. A global backup system can then access the replicated files and copy them to a tape or any other backup media. The Replicate component is part of the CyberArk Backup Process, which provides a secure and easy method of backing up and restoring the Vault data12. The other components are not related to the tape backup of the Vault. Disaster Recovery is a feature that enables the Vault to recover from a catastrophic failure by using a standby Vault server3. Distributed Vaults is a feature that enables the Vault to synchronize data with other Vaults in different locations4. High Availability is a feature that enables the Vault to maintain continuous operation by using a primary and a secondary Vault server. References:
? Use the CyberArk Backup Process - CyberArk, section “Use the CyberArk Backup
Process”
? Install the Vault Backup Utility - CyberArk, section “Backup utilities”
? Disaster Recovery - CyberArk, section “Disaster Recovery”
? Distributed Vaults - CyberArk, section “Distributed Vaults”
? [High Availability - CyberArk], section “High Availability”

**NEW QUESTION 90**
You created a new safe and need to ensure the user group cannot see the password, but can connect through the PSM.
Which safe permissions must you grant to the group? (Choose two.)

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

**Answer:** BD

**Explanation:**
To ensure that a user group can connect through the Privileged Session Manager (PSM) without seeing the password, you must grant the Use Accounts and Retrieve Files permissions to the group for the safe. TheUse Accounts permission allows users to initiate sessions using accounts without viewing the account details or
passwords. TheRetrieve Files permission enables users to retrieve files during PSM sessions without having access to the passwords1.
References:
? CyberArk Docs - Safe Permissions

**NEW QUESTION 92**
Which service should NOT be running on the DR Vault when the primary Production Vault is up?

A. PrivateArk Database
B. PrivateArk Server
C. CyberArk Vault Disaster Recovery (DR) service
D. CyberArk Logical Container

**Answer:** C

**Explanation:**
The user that is automatically added to all Safes and cannot be removed is the Master user. The Master user is a predefined user that is created during the Vault installation and has full permissions on all Safes and accounts. The Master user is the only user that can perform certain tasks, such as creating other predefined users, managing the Vault configuration, and restoring the Vault from a backup. The Master user cannot be deleted or modified by any other user, and is always a member of every Safe12. References:
? Predefined users and groups - CyberArk, section “Master”
? Safes and Safe members - CyberArk, section “Safe members overview”

**NEW QUESTION 96**
What is the correct process to install a custom platform from the CyberArk Marketplace?

A. Locate the custom platform in the Marketplace and click Import.
B. Download the platform from the Marketplace and import it using the PVWA.
C. Contact CyberArk Support for guidance on how to import the platform.
D. Duplicate an existing platform and align the setting to match the platform from the Marketplace.

**Answer:** B

**Explanation:**
The correct process to install a custom platform from the CyberArk Marketplace involves downloading the platform package from the Marketplace and then importing it using the Privileged Vault Web Access (PVWA). This process allows you to add new platforms that are not included in the default installation directly into the CyberArk Privileged Access Manager (PAM) - Self-Hosted1.
References:
? CyberArk Docs - Add New Platforms1
? CyberArk Docs - Manage platforms2

**NEW QUESTION 97**
It is possible to control the hours of the day during which a user may log into the vault.

A. TRUE
B. FALSE

**Answer:** A

**Explanation:**
It is possible to control the hours of the day during which a user may log into the vault by using the Time Restrictions feature. This feature allows administrators to define the days and times that users can access the vault. Users who try to log in outside the permitted hours will be denied access and receive a message informing them of the restriction. Time restrictions can be applied to individual users or groups of users. References:
? [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.3:
User Management, Slide 7: Time Restrictions
? [Defender PAM Sample Items Study Guide], Question 2: Time Restrictions
? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 4: Managing Users and Groups, Section: Time Restrictions

**NEW QUESTION 101**
In a default CyberArk installation, which group must a user be a member of to view the “reports” page in PVWA?

A. PVWAMonitor
B. ReportUsers
C. PVWAReports
D. Operators

**Answer:** A

**Explanation:**
In a default CyberArk installation, to view the “reports” page in the PVWA (Privileged Web Access), a user must be a member of the PVWAMonitor group1. This group is specified in the ManageReportsGroup parameter in the Reports section of the Web Access Options in the System Configuration page. Being a member of this group grants the user the necessary permissions to generate and view reports within the PVWA. References:
? CyberArk’s official documentation on Reports in PVWA outlines the requirement
for users to belong to the PVWAMonitor group to access the reports page and generate reports1.

**NEW QUESTION 105**
Where can a user with the appropriate permissions generate a report? (Choose two.)

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

**Answer:** AB

**Explanation:**
A user with the appropriate permissions can generate a report in the PVWA (Privileged Vault Web Access) under theReports section1. Users who belong to the group specified in the ManageReportsGroup parameter in the Reports section of the Web Access Options in the System Configuration page are able to generate reports in the PVWA. By default, this group is the PVWAMonitor group1. Additionally, reports can be generated using the PrivateArk Client, which is a desktop application that provides a direct interface to manage the CyberArk Vault and its contents, including the generation of
reports2.
References:
? CyberArk Docs - Reports in PVWA1
? CyberArk Docs - Generate the Report2

**NEW QUESTION 106**
In addition to add accounts and update account contents, which additional permission on the safe is required to add a single account?

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

**Answer:** C

**Explanation:**
In addition to the permissions to add accounts and update account contents, the permission to Update Account Properties is required to add a single account to a safe in CyberArk. This permission allows the user to modify the properties of an account, which is a necessary step when adding a new account to ensure that all relevant details and configurations are correctly set1. References: The information provided is based on general knowledge of CyberArk PAM best practices and the permissions required for account management as outlined in CyberArk’s official documentation

**NEW QUESTION 108**
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:** B

**Explanation:**

Customers who have the ‘Access Safe without confirmation’ safe permission on a safe where accounts are configured for Dual control, do not need to request approval to use the account. The ‘Access Safe without confirmation’ safe permission allows users to access accounts without confirmation from authorized users, even if the Master Policy or an exception enforces Dual Control1. This means that users who have this permission can bypass the workflow process and access the account password or connect to the target system immediately. This permission can be granted to users or groups on a safe level by the safe owner or another user with the Manage Safe authorization2. References:
? 1: Dual Control, Advanced Settings subsection
? 2: CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section: Safe Authorizations, Table 2-1: Safe Authorizations

**NEW QUESTION 113**
Select the best practice for storing the Master CD.

A. Copy the files to the Vault server and discard the CD
B. Copy the contents of the CD to a Hardware Security Module (HSM) and discard the CD
C. Store the CD in a secure location, such as a physical safe
D. Store the CD in a secure location, such as a physical safe, and copy the contents of the CD to a folder secured with NTFS permissions on the Vault

**Answer:** C

**Explanation:**
The best practice for storing the Master CD is to store it in a secure location, such as a physical safe. The Master CD contains the server key, the public recovery key, and the private recovery key, which are essential for starting, operating, and recovering the Vault. These keys are sensitive and should be protected from unauthorized access, loss, or damage. Therefore, storing the CD in a physical safe ensures that the keys are kept in a secure location when not in use, and that they are available when needed. This is the recommended option by CyberArk1.
The other options are not best practices and should be avoided, as they expose the keys to potential risks, such as theft, corruption, or deletion. Copying the files to the Vault server and discarding the CD is not secure, as it makes the keys accessible to anyone who can access the Vault server or compromise its security. Copying the contents of the CD to a Hardware Security Module (HSM) and discarding the CD is not feasible, as the HSM can only store the server key, not the recovery keys2. Storing the CD in a secure location, such as a physical safe, and copying the contents of the CD to a folder secured with NTFS permissions on the Vault is not necessary, as it creates redundant copies of the keys that may not be synchronized or updated. Moreover, NTFS permissions are not sufficient to protect the keys from malicious or accidental actions. References:
? Server Keys - CyberArk, section “Server Keys”
? Store the Server Key in an HSM - CyberArk, section “Store the Server Key in an HSM”

**NEW QUESTION 116**
Which change could CyberArk make to the REST API that could cause existing scripts to fail?

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

**Answer:** C

**Explanation:**
Changes to the REST API that could cause existing scripts to fail include removing parameters. When parameters are removed from an API, scripts that rely on those parameters being present may no longer function correctly because they expect certain data to be available. This can lead to errors or unexpected behavior in the scripts that use the API1.
References:
? CyberArk Docs: REST APIs1

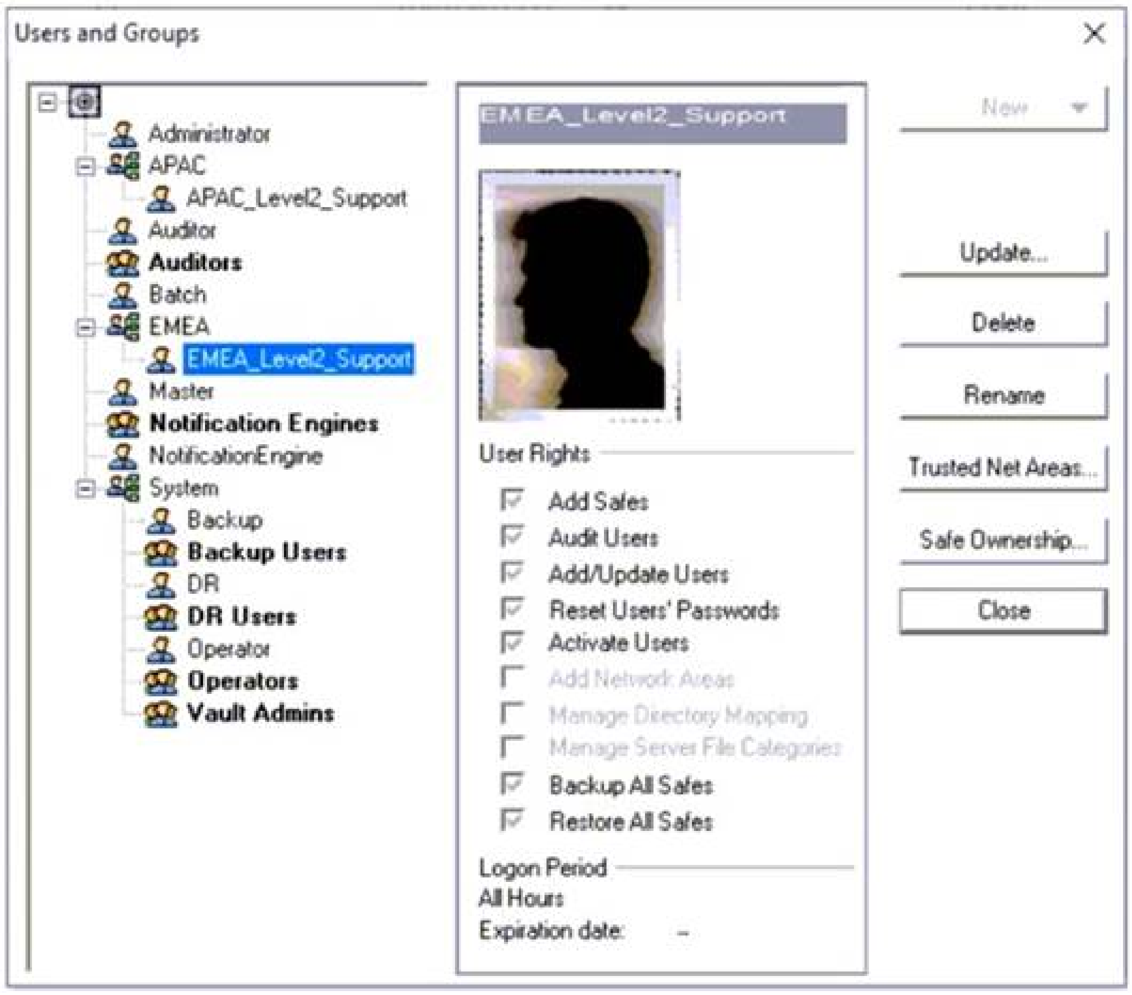
**NEW QUESTION 119**
In PVWA, you are attempting to play a recording made of a session by user jsmith, but there is no option to “Fast Forward” within the video. It plays and only allows you to skip between commands instead. You are also unable to download the video.
What could be the cause?

A. Recording is of a PSM for SSH session.
B. The browser you are using is out of date and needs an update to be supported.
C. You do not have the “View Audit” permission on the safe where the account is stored.
D. You need to update the recorder settings in the platform to enable screen capture every 10000 ms or less.

**Answer:** A

**Explanation:**
The inability to “Fast Forward” within a video recording in the PVWA and the restriction to only skip between commands suggests that the recording is of a PSM for SSH session. PSM for SSH sessions are typically recorded as text-based logs that capture command-level activities, which allows for skipping between commands but not fast- forwarding through a video timeline. Additionally, the lack of an option to download the video is consistent with the behavior of text-based session recordings, which do not provide a video file for download1.
References:
? CyberArk’s official documentation on Recorded Sessions, which explains the playback functionalities and limitations of different types of session recordings1.
? Information on configuring video and text recordings in PSM, which details how recordings are managed and the options available for different session types2.

**NEW QUESTION 122**
Refer to the exhibit.



EMEA_Level2_Support

User Rights

- ☑ Add Safes
- ☑ Audit Users
- ☑ Add/Update Users
- ☑ Reset Users' Passwords
- ☑ Activate Users
- □ Add Network Areas
- □ Manage Directory Mapping
- □ Manage Server File Categories
- ☑ Backup All Safes
- ☑ Restore All Safes

Logon Period
All Hours
Expiration date: -

Why is user "EMEALevel2Support" unable to change the password for user "Operator"?

A. EMEALevel2Support's hierarchy level is not the same or higher than Operator.
B. EMEALevel2Support does not have the "Manage Directory Mapping" role.
C. Operator can only be reset by the Master user.
D. EMEALevel2Support does not have rights to reset passwords for other users.

**Answer:** D

**Explanation:**
The image description indicates that "EMEALevel2Support" has the following rights: Add/Update Users, Manage Server File Categories, Manage Directory Mapping, Backup All Files, Restore All Files. Since there is no mention of the right to reset passwords for other users, this suggests that "EMEALevel2Support" lacks the necessary permission to change the password for "Operator".

**NEW QUESTION 123**
Users 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:** B

**Explanation:**
Users who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, do not need to request approval to use the account. The 'Access Safe without confirmation' safe permission is a special permission that allows a user to bypass the Dual control mechanism and access the accounts in the safe without requiring confirmation from other authorized users. This permission can be useful for emergency situations or trusted users who need immediate access to the accounts. However, this permission also increases the risk of unauthorized or malicious access, so it should be granted with caution and monitored closely1.
References:
? 1: Access without confirmation

**NEW QUESTION 128**
Which file must be edited on the Vault to configure it to send data to PTA?

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

**Answer:** A

**Explanation:**
To configure the CyberArk Vault to send data to Privileged Threat Analytics (PTA), you must edit the dbparm.ini file on the Vault. This file contains parameters that specify how the Vault should forward syslog events to PTA, ensuring that the Vault can send secured syslog data to PTA for analysis and threat detection1.
References:
? CyberArk Docs: Configure Vault Trusted Connection to PTA2
? Netenrich: CyberArk Vault via Syslog1

**NEW QUESTION 131**
You are troubleshooting a PVWA slow response. Which log files should you analyze first? (Choose two.)

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

**Answer:** CD

**Explanation:**
When troubleshooting a slow response in the Privileged Vault Web Access (PVWA), the first log files to analyze are the CyberArk.WebApplication.log and CyberArk.WebConsole.log. These logs contain detailed information about the activities carried out by the PVWA and can help identify any problems that may occur. The log files are created by the PVWA and stored on the Web server in the location specified in the LogFolder parameter in the web.config file1. By examining these logs, you can track business flows and troubleshoot failures without having to enable debug mode. References:
? CyberArk Docs - PVWA Logging1

**NEW QUESTION 133**
Which utilities could you use to change debugging levels on the vault without having to restart the vault. Select all that apply.

A. PAR Agent
B. PrivateArk Server Central Administration
C. Edit DBParm.ini in a text editor.
D. Setup.exe

**Answer:** AB

**Explanation:**
To change debugging levels on the vault without having to restart the vault, you can use the following utilities:
? PAR Agent: This is a utility that runs on the vault server and allows you to change the debug level of the vault by editing the PARAgent.ini file. You can set the EnableTrace parameter to yes and specify the debug level in the DebugLevel parameter. The changes will take effect immediately without restarting the vault. The log file is located in the PARAgent.log file1.
? PrivateArk Server Central Administration: This is a graphical user interface that runs on the vault server and allows you to change the debug level of the vault by selecting the vault server and clicking the Debug button. You can choose the debug level from a list of predefined options or enter a custom value. The changes will take effect immediately without restarting the vault. The log files are located in the Trace.dX files, where X is a number from 0 to 42.
You cannot use the following utilities to change debugging levels on the vault without having to restart the vault:
? Edit DBParm.ini in a text editor: This is a configuration file that stores the vault parameters, such as the database name, port, and password. Editing this file does not affect the debug level of the vault, and requires restarting the vault for the changes to take effect3.
? Setup.exe: This is an installation program that runs on the vault server and allows you to install, upgrade, or uninstall the vault. It does not allow you to change the debug level of the vault, and requires restarting the vault for any changes to take effect4. References:
? 1: Configure Debug Levels, Vault section, PARAgent subsection
? 2: Configure Debug Levels, Vault section, PrivateArk Server Central Administration subsection
? 3: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault, Section: Configuring the Vault, Subsection: DBParm.ini
? 4: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault, Section: Installing the Vault

**NEW QUESTION 137**
You want to generate a license capacity report. Which tool accomplishes this?

A. Password Vault Web Access
B. PrivateArk Client
C. DiagnoseDB Report
D. RestAPI

**Answer:** B

**Explanation:**
The license capacity report is a tool that provides information about the licensed user types and objects in the Vault. It enables users to see the maximum number of licenses for each user type or object, and the number of used licenses for each one. Only user types and objects that are limited by the license are displayed in this report. To generate a license capacity report, users need to use the PrivateArk Client, which is a graphical user interface that allows users to manage safes and their properties. Users can access the report from the Tools menu in the PrivateArk Client. References: Reporting License Usage, Manage the CyberArk License

**NEW QUESTION 141**
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

**Answer:** B

**Explanation:**
Security Admins are the built-in group that can view and configure Automatic Remediation and Session Analysis and Response in the PVWA. These features are part of the Privileged Threat Analytics (PTA) module, which is designed to detect and respond to anomalous activities and risky behaviors in the privileged environment. Security Admins have the permissions to access the PTA settings and configure the policies and actions for Automatic Remediation and Session Analysis and Response. References:
? Defender PAM Sample Items Study Guide, page 18, question 49
? Privileged Threat Analytics Implementation Guide, page 9, section “Security Admins”

**NEW QUESTION 145**
SAFE Authorizations may be granted to . Select all that apply.

A. Vault Users
B. Vault Group
C. LDAP Users
D. LDAP Groups

**Answer:** ABCD

**Explanation:**
SAFE Authorizations may be granted to Vault Users, Vault Groups, LDAP Users, and LDAP Groups. These are the four types of users that can be defined in the Vault and assigned permissions to access Safes and manage passwords. Vault Users and Vault Groups are created and managed within the Vault, while LDAP Users and LDAP Groups are imported from an external directory service such as Active Directory. References:
? Defender PAM Course, Module 4: Managing Safes, Lesson 4.2: Safe Authorizations, slide 4
? Defender PAM Sample Items Study Guide, Question 39, page 15
? CyberArk Privileged Access Security Documentation, Vault Administration Guide, Chapter 4: Managing Safes, Section: Safe Authorizations, page 4-12

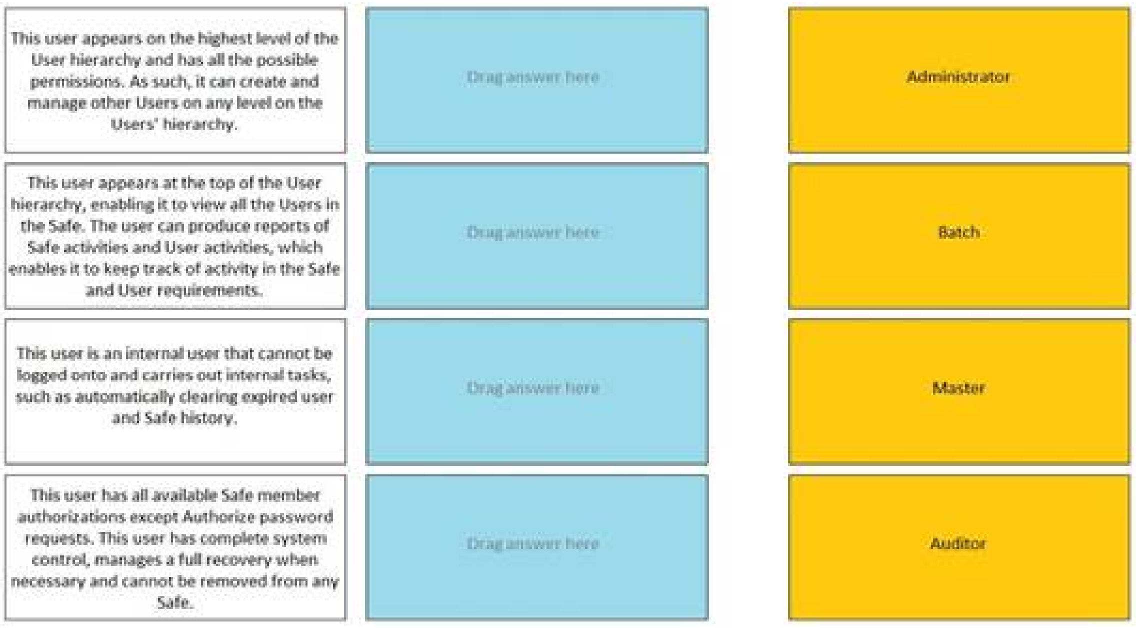
**NEW QUESTION 146**
In the Private Ark client, how do you add an LDAP group to a CyberArk group?

A. Select Update on the CyberArk group, and then click Add > LDAP Group
B. Select Update on the LDAP Group, and then click Add > LDAP Group
C. Select Member Of on the CyberArk group, and then click Add > LDAP Group
D. Select Member Of on the LDAP group, and then click Add > LDAP Group

**Answer:** C

**Explanation:**
To add an LDAP group to a CyberArk group, you need to use the Private Ark client and follow these steps1:
? In the Users and Groups tree, select the CyberArk group that you want to add the
LDAP group to.
? In the Properties pane, click Member Of.
? Click Add > LDAP Group.
? In the LDAP Group dialog box, enter the name of the LDAP group and click OK. References: Add an LDAP group to a Vault group

**NEW QUESTION 151**
DRAG DROP
Match the built-in Vault User with the correct definition.

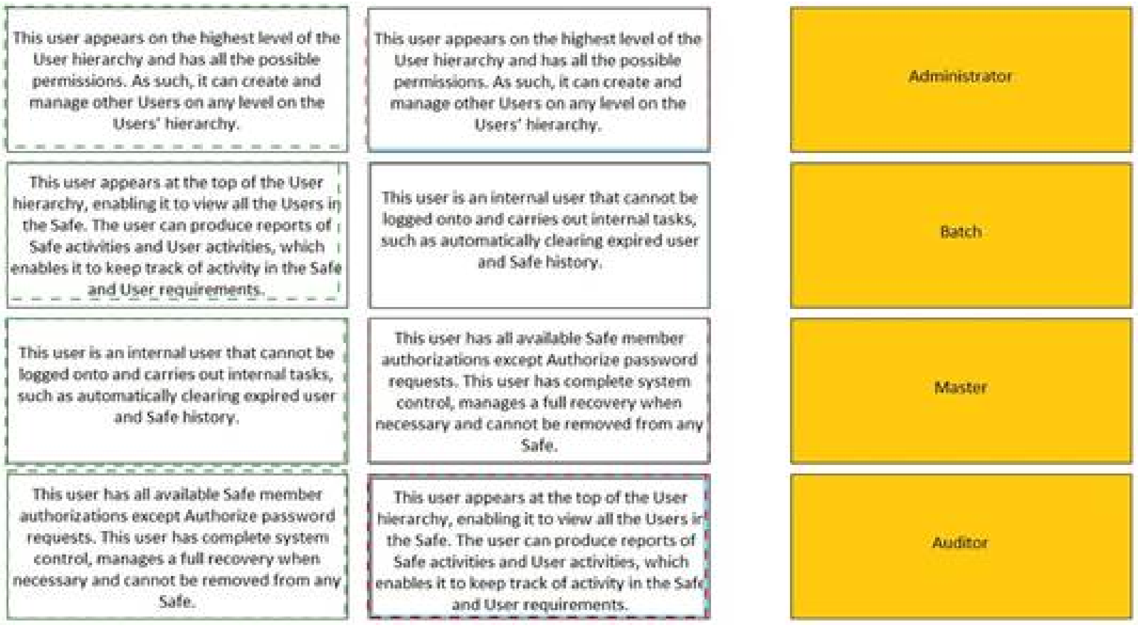


| | | |
|---|---|---|
| This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy. | Drag answer here | Administrator |
| This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements. | Drag answer here | Batch |
| This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history. | Drag answer here | Master |
| This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe. | Drag answer here | Auditor |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



| | | |
|---|---|---|
| This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy. | This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy. | Administrator |
| This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements. | This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history. | Batch |
| This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history. | This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe. | Master |
| This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe. | This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements. | Auditor |

**NEW QUESTION 155**
Which statement is true about setting the reconcile account at the platform level?

A. This is the only way to enable automatic reconciliation of account passwords.
B. CPM performance will be improved when the reconcile account is set at the platform level.
C. A rule can be used to specify the reconcile account dynamically or a specific reconcile account can be selected.
D. This configuration prevents the association from becoming broken if the reconcile account is moved to a different safe.

**Answer:** C

**Explanation:**
Setting the reconcile account at the platform level allows for flexibility in how the reconcile account is specified. A rule can be used to dynamically determine the appropriate reconcile account, or a specific reconcile account can be selected and configured directly in the platform settings. This approach provides the ability to manage reconciliation accounts more efficiently and adapt to different scenarios1.
References:
? CyberArk Community - Associate reconcile account with a specific platform

**NEW QUESTION 156**
You are onboarding an account that is not supported out of the box. What should you do first to obtain a platform to import?

A. Create a service ticket in the customer portal explaining the requirements of the custom platform.
B. Search common community portals like stackoverflow, reddit, github for an existing platform.
C. From the platforms page, uncheck the “Hide non-supported platforms” checkbox and see if a platform meeting your needs appears.
D. Visit the CyberArk marketplace and search for a platform that meets your needs.

**Answer:** D

**Explanation:**
The CyberArk marketplace is a platform that simplifies delivery of privileged access security solutions, such as CyberArk Privileged Account Security Solution. It features the industry’s broadest and deepest portfolio of technology integrations, including platforms for various types of accounts. Customers can find and deploy integrations with CyberArk Marketplace in as little as four clicks. If there is no platform that meets the customer’s needs, they can request a custom platform from CyberArk or create their own using the Platform Development Kit (PDK). References: CyberArk Marketplace, Platform Development Kit

**NEW QUESTION 161**
Which command generates a full backup of the Vault?

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

**Answer:** A

**Explanation:**
The command PAReplicate.exe with the /FullBackup option is used to generate a full backup of the CyberArk Vault. This command requires the Vault configuration file (typically Vault.ini) and a credential file (specified with /LogonFromFile) that contains the user’s encrypted logon credentials. The /FullBackup option indicates that a full backup of the Vault is to be performed, as opposed to an incremental backup1. References:
? CyberArk Docs: Install the Vault Backup Utility2
? CyberArk Knowledge Article: PAReplicate Configuration and Usage

**NEW QUESTION 162**
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

**Answer:** C

**Explanation:**
The Onboarding RestAPI functions are a set of web services that allow you to integrate CyberArk with your accounts provisioning process. You can use the Onboarding RestAPI functions to create, update, delete, or verify accounts in the CyberArk Vault, as well as to retrieve information about accounts, platforms, and safes. The Onboarding RestAPI functions are part of the Central Credential Provider component, which is installed on a dedicated server that communicates with the Vault. References:
? [Defender PAM Course], Module 4: Onboarding Accounts, Lesson: Onboarding
RestAPI Functions
? [Onboarding RestAPI Functions Guide], Introduction

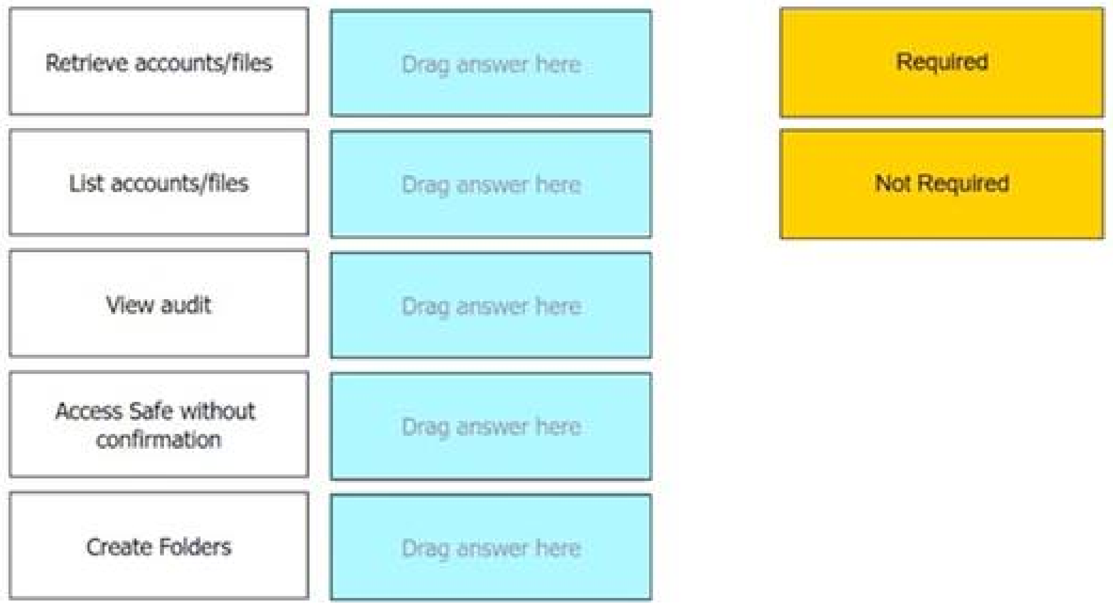
**NEW QUESTION 167**
When Dual Control is enabled a user must first submit a request in the Password Vault Web Access (PVWA) and receive approval before being able to launch a secure connection via PSM for Windows (previously known as RDP Proxy).

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

**Answer:** A

**Explanation:**
According to the CyberArk Defender PAM documentation1, 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). This is a security feature that ensures that passwords can only be retrieved after permission or ‘confirmation’ has been granted from an authorized Safe Owner(s). The user must specify the reason for accessing the account, whether they will access it once or multiple times, and the time period during which they will access it. The request is then sent to the authorized Safe Owners, who can either confirm or reject it. The number of confirmations required is defined in the Master Policy. Only after the user receives the required confirmations, they can activate the request and access the account through PSM for Windows. This way, Dual Control adds an additional measure of protection and accountability for accessing sensitive accounts.

**NEW QUESTION 169**
DRAG DROP
Which authorizations are required in a recording safe to allow a group to view recordings?



| | | |
|---|---|---|
| Retrieve accounts/files | Drag answer here | Required |
| List accounts/files | Drag answer here | Not Required |
| View audit | Drag answer here | |
| Access Safe without confirmation | Drag answer here | |
| Create Folders | Drag answer here | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
? Retrieve accounts/files: Required
? List accounts/files: Required
? View audit: Required
? Access Safe without confirmation: Not Required
? Create Folders: Not Required
Comprehensive Explanation: To allow a group to view recordings in a recording safe, the required authorizations are Retrieve accounts/files, List accounts/files, and View audit.
These authorizations enable the group members to access and view the session recordings stored within the safe. The Retrieve accounts/files permission allows users to retrieve files during PSM sessions. The List accounts/files permission enables users to see the list of accounts and files within the safe. TheView audit authorization is necessary for users to view the audit records associated with the recordings1.
References:
? CyberArk Docs - Monitor Privileged Sessions

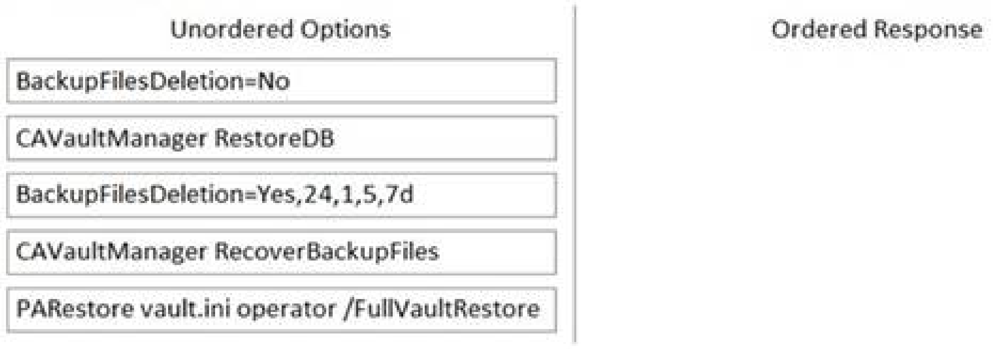
**NEW QUESTION 172**
PTA can automatically suspend sessions if suspicious activities are detected in a privileged session, but only if the session is made via the CyberArk PSM.

A. True
B. False, the PTA can suspend sessions whether the session is made via the PSM or not

**Answer:** B

**Explanation:**
The PTA can automatically suspend sessions if suspicious activities are detected in a privileged session, regardless of the session method. The PTA can suspend sessions that are made via the PSM, the PVWA, or directly to the target system. The PTA can also suspend sessions that are made via SSH, RDP, or other protocols. References:
? Defender PAM Sample Items Study Guide, page 24
? PTA User Guide, page 17

**NEW QUESTION 176**
DRAG DROP
Arrange the steps to restore a Vault using PARestore for a Backup in the correct sequence.



| Unordered Options | Ordered Response |
|---|---|
| BackupFilesDeletion=No | |
| CAVaultManager RestoreDB | |
| BackupFilesDeletion=Yes,24,1,5,7d | |
| CAVaultManager RecoverBackupFiles | |
| PARestore vault.ini operator /FullVaultRestore | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
BackupFilesDeletion=No
PARestore vault.ini operator /FullVaultRestore CAVaultManager RecoverBackupFiles CAVaultManager RestoreDB BackupFilesDeletion=Yes,24,1,5,7d
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Restoring-Safes-or-the-Vault.htm

**NEW QUESTION 178**
What is the purpose of the password change process?

A. To test that CyberArk is storing accurate credentials for accounts
B. To change the password of an account according to organizationally defined password rules
C. To allow CyberArk to manage unknown or lost credentials
D. To generate a new complex password

**Answer:** B

**Explanation:**
The purpose of the password change process is to change the password of an account according to organizationally defined password rules. The password change process is a feature of CyberArk that enables the Central Policy Manager (CPM) to manage the passwords of privileged accounts that are stored in the Vault. The CPM can change the passwords automatically or manually, based on predefined policies, schedules, or user requests. The password change process ensures that the passwords are secure, compliant, and synchronized with the target systems and the Vault. The password change process also supports different types of accounts, such as one-time passwords, exclusive accounts, and dual accounts1.
The other options are not the main purpose of the password change process, although they may be related to some aspects of it. The password change process does not test that CyberArk is storing accurate credentials for accounts, although it may verify the password validity before changing it. The password change process does not allow CyberArk to manage unknown or lost credentials, although it may reconcile the passwords if they are out of sync with the target systems. The password change process does not generate a new complex password, although it may use a random password generation mechanism to create a new password that meets the password policy requirements. References:
? Change Passwords - CyberArk, section “Change Passwords”

**NEW QUESTION 181**
......