![PDF]

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
You have been asked to turn off the time access restrictions for a safe. Where is this setting found?

A. PrivateArk
B. RestAPI
C. Password Vault Web Access (PVWA)
D. Vault

Answer: A

Explanation:
The time access restrictions for a safe are configured in the PrivateArk Administrative Client, which is a graphical user interface that allows users to manage safes and their properties. The time access restrictions are set in the Time Access Restrictions tab of the Safe properties window. This tab enables users to specify the days and hours when the safe can be accessed. If the time access restrictions are turned off, the safe can be accessed at any time. References: PrivateArk Safe management, Advanced Safe Management

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
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

Answer: D

Explanation:
According to the web search results, all of the Privileged Session Management (PSM) solutions support live monitoring of active sessions. PSM, PSM for Windows, and PSM for SSH enable authorized users to monitor active sessions from their workstation and take part in controlling these sessions. Users can also suspend or terminate active sessions based on their group assignment. By default, active session monitoring is enabled at system level for all authorized users, and can be disabled at platform level. Active session monitoring can also be disabled at system level, but when it is disabled, it cannot be enabled at platform level. PSM can automatically suspend or terminate sessions when notified by PTA or a third party threat analytics tool1. Authorized users monitor or terminate an active session using the same connection method (RDP file or HTML5 Gateway) as the end user

NEW QUESTION 5
The vault supports Role Based Access Control.

A. TRUE
B. FALSE

Answer: A

Explanation:
The vault supports Role Based Access Control (RBAC), which is a method of granting access to resources based on the roles of users or groups. RBAC enables the administrator to define roles that represent different functions or responsibilities in the organization, and assign permissions to those roles according to the principle of least privilege. Users or groups can then be assigned to one or more roles, and inherit the permissions of those roles. RBAC simplifies the management of access control by reducing the complexity and redundancy of assigning permissions to individual users or groups. RBAC also enhances security and compliance by ensuring that users or groups only have the minimum level of access required to perform their tasks1.
References:
? 1: Role Based Access Control

NEW QUESTION 6
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

Answer: AC

Explanation:
 The server key and the public recovery key are required to be present in order to start the PrivateArk Server service. The server key opens the Vault, much like the key of a physical Vault. The public recovery key is part of the asymmetric recovery key that enables the Master User to log on to the Vault in case of a disaster. The server key and the public recovery key are usually stored on a removable media, such as a disk or CD, so that they can be safely secured in a physical safe. The recovery private key and the safe key are not needed to start the PrivateArk Server service. The recovery private key is only used for recovery purposes and the safe key is only used to access a specific safe that is defined with an external key. References: Server keys, Server Components

NEW QUESTION 7
When the CPM connects to a database, which interface is most commonly used?

A. Kerberos
B. ODBC
C. VBScript
D. Sybase

Answer: B

Explanation:
 The Central Policy Manager (CPM) in CyberArk most commonly uses the ODBC (Open Database Connectivity) interface when connecting to a database. ODBC is a standard API for accessing database management systems (DBMS). The CPM supports remote password management on all databases that support ODBC connections, and the machine running the CPM must support ODBC, version 2.7 and higher1. References:
? CyberArk Docs: Databases that support ODBC connections1

NEW QUESTION 8
A new HTML5 Gateway has been deployed in your organization. Where do you configure the PSM to use the HTML5 Gateway?

A. Administration > Options > Privileged Session Management > Configured PSM Servers> Connection Details > Add PSM Gateway
B. Administration > Options > Privileged Session Management > Add Configured PSMGateway Servers
C. Administration > Options > Privileged Session Management > Configured PSM Servers> Add PSM Gateway
D. Administration > Options > Privileged Session Management > Configured PSM Servers> Connection Details

Answer: C

Explanation:
 After deploying a new HTML5 Gateway in your organization, you configure the PSM to use the HTML5 Gateway by navigating to the Administration section in the PVWA. From there, you go to Options, then Privileged Session Management, and under Configured PSM Servers, you will find the option to Add PSM Gateway1. This is where you can specify the details of the newly deployed HTML5 Gateway to ensure that the PSM can utilize it for secure remote access to target machines through an HTML5-based session. References:
? CyberArk's official documentation provides a step-by-step guide on how to install and configure the PSM HTML5 Gateway, including the process of adding the gateway to the PSM configuration1.
? For more detailed instructions and best practices on configuring the PSM with an HTML5 Gateway, refer to the CyberArk Defender PAM course materials and study guides

NEW QUESTION 9
Which Cyber Are components or products can be used to discover Windows Services or Scheduled Tasks that use privileged accounts? Select all that apply.

A. Discovery and Audit (DMA)
B. Auto Detection (AD)
C. Export Vault Data (EVD)
D. On Demand Privileges Manager (OPM)
E. Accounts Discovery

Answer: ABE

Explanation:
 Discovery and Audit (DMA), Auto Detection (AD), and Accounts Discovery are CyberArk components or products that can be used to discover Windows Services or Scheduled Tasks that use privileged accounts.

? Discovery and Audit (DMA) is a tool that scans Windows servers and workstations
to identify privileged accounts that are used by Windows Services or Scheduled Tasks. DMA can also generate reports on the usage and risks of these accounts.
? Auto Detection (AD) is a feature of the CyberArk Privileged Account Security
Solution that automatically detects and onboards privileged accounts that are used by Windows Services or Scheduled Tasks. AD can also monitor and rotate the passwords of these accounts.
? Accounts Discovery is a feature of the CyberArk Privileged Account Security
Solution that scans the network to discover privileged accounts on various platforms, including Windows. Accounts Discovery can also identify accounts that are used by Windows Services or Scheduled Tasks.
References:
? : Discovery and Audit (DMA) User Guide
? : Auto Detection Implementation Guide
? : Accounts Discovery Implementation Guide

NEW QUESTION 10
Which Vault authorization does a user need to have assigned to able to generate the "Entitlement Report" from the reports page in PVWA? (Choose two.)

A. Manage Users
B. Audit Users
C. Read Activity
D. View Entitlements
E. List Accounts

Answer: BD

Explanation:
 D. View Entitlements: This authorization allows the user to view the entitlements, which is essential for generating reports that include access control and authorization levels on accounts.
* B. Audit Users: Having 'Audit Users' permission is crucial as it enables the user to perform audit-related activities, which are typically part of generating entitlement reports12.
These authorizations ensure that the user has the necessary permissions to access and compile the data required for the Entitlement Report within the CyberArk PVWA.

NEW QUESTION 10
As long as you are a member of the Vault Admins group you can grant any permission on any safe.

A. TRUE
B. FALSE

Answer: B

Explanation:
 The Vault Admins group is a predefined group that is automatically created during the installation or upgrade of the Vault. This group has all possible permissions in the Vault, and can create and manage other users, groups, platforms, policies, safes, and accounts. However, this group is not automatically added to every safe in the Vault, but only to some system safes that are used for administrative purposes. Therefore, being a member of the Vault Admins group does not guarantee that you can grant any permission on any safe, unless you are also a member or an owner of that safe. To grant permissions on a safe, you need to have the Authorize safe members authorization on that safe, which allows you to add or remove users or groups as safe members, and assign or revoke their authorizations. Alternatively, you can use the Administrator user, which is a predefined user that is a member of the Vault Admins group, and has all possible permissions on any safe in the Vault. References:
? Predefined users and groups
? Safe member authorizations

NEW QUESTION 11
To use PSM connections while in the PVWA, what are the minimum safe permissions a user or group will need?

A. List Accounts, Use Accounts
B. List Accounts, Use Accounts, Retrieve Accounts
C. Use Accounts
D. List Accounts, Use Accounts, Retrieve Accounts, Access Safe without confirmation

Answer: B

Explanation:
 To use PSM connections within the PVWA, a user or group needs to have permissions that allow them to list and use accounts, as well as retrieve account details. These permissions ensure that the user can view the accounts within a safe, initiate sessions using those accounts, and retrieve the necessary credentials for authentication during the session initiation process1.
References:
? CyberArk's official documentation on Safe Settings and permissions required for each safe in CyberArk's Enterprise Password Vault (EPV) components provides detailed information on the default safe configuration and permissions1.
? For more information on best practices for safe and safe member design, including the minimum permissions required for PSM connections, refer to CyberArk's best practices articles and study guides

NEW QUESTION 13
When are external vault users and groups synchronized by default?

A. They are synchronized once every 24 hours between 1 AM and 5 A
B. Most Voted
C. They are synchronized once every 24 hours between 7 PM and 12 AM.
D. They are synchronized every 2 hours.
E. They are not synchronized according to a specific schedule.

Answer: A

Explanation:
By default, external vault users and groups are synchronized once every 24 hours between 1 AM and 5 AM. This synchronization schedule is determined by the AutoSyncExternalObjects parameter in the DBParm.ini file, which specifies that the Vault's external users and groups will be synchronized with the External Directory during this time frame1.
References:
? CyberArk Docs - Synchronize External Users and Groups in the Vault with the External Directory

NEW QUESTION 15
You need to recover an account localadmin02 for target server 10.0.123.73 stored in Safe Team1.
What do you need to recover and decrypt the object? (Choose three.)

A. Recovery Private Key
B. Recover.exe
C. Vault data
D. Recovery Public Key
E. Server Key
F. Master Password

Answer: ABC

Explanation:
To recover and decrypt an account that is stored in a Safe, you need the following items:
? Recovery Private Key: This is a key that is used to decrypt the data stored in the Vault. It is located on the Master CD, which is a physical CD that contains the Private Recovery Key, a file named RecPrv.key.
? Recover.exe: This is a utility that is used to recover information from a Safe's external files in case of loss or corruption of that Safe. The files are decrypted and saved as readable files. The utility can be run from the command line or the graphical user interface.
? Vault data: This is the data that is stored in the Vault, such as accounts, safes, platforms, policies, users, groups, and audit records. The Vault data is encrypted using the Recovery Public Key, which is a key that is used to encrypt the data stored in the Vault. The Vault data can be recovered from the Vault server disk drive or from a backup file.
References: Recover, Server keys, Export Vault Information

NEW QUESTION 18
Which user(s) can access all passwords in the Vault?

A. Administrator
B. Any member of Vault administrators
C. Any member of auditors
D. Master

Answer: D

Explanation:
According to the CyberArk Defender PAM documentation1, the Master user is the only user that can access all passwords in the Vault. The Master user is a special user that is created during the initial installation of the Vault and has full permissions on all Safes and accounts in the Vault. The Master user can also perform administrative tasks, such as backup and restore the Vault, change the Vault license, and manage the recovery key. The Master user is the only user that can log on to the Vault in case of a disaster using the recovery key. The Master user's password is not stored in the Vault and cannot be changed or retrieved by any other user.
The Administrator user is a predefined user that is created during the initial installation of the Vault and has the Vault Admin authorization. The Administrator user can perform administrative tasks, such as create and manage users and groups, define platforms and policies, and monitor Vault activity. However, the Administrator user cannot access any passwords in the Vault unless they are explicitly added as a member of a Safe that contains the passwords2.
The Vault administrators group is a predefined group that is created during the initial installation of the Vault and has the Vault Admin authorization. The members of the Vault administrators group can perform the same administrative tasks as the Administrator user, but they cannot access any passwords in the Vault unless they are explicitly added as a member of a Safe that contains the passwords2.
The auditors group is a predefined group that is created during the initial installation of the Vault and has the Audit Users authorization. The members of the auditors group can view
and generate reports on the Vault activity, but they cannot access any passwords in the Vault unless they are explicitly added as a member of a Safe that contains the passwords2. References:
? Master User - CyberArk
? Predefined users and groups - CyberArk

NEW QUESTION 22
DRAG DROP
Match the Status of Service on a DR Vault to what is displayed when it is operating normally in Replication mode.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

CyberArk Hardened Windows Firewall -> Running PrivateArk Database -> Running
PrivateArk Server -> Stopped
CyberArk Vault Disaster Recovery -> Running CyberArk Event Notification Engine -> Stopped
? Comprehensive Explanation: A DR Vault is a Vault that acts as a standby replica of the Primary Vault and is ready to take its place when the Primary Vault is unavailable. The DR Vault operates in Replication mode, which means it continuously replicates the data and metadata from the Primary Vault. In Replication mode, the following services have the following status on the DR Vault:
? Cyber-Ark Hardened Windows Firewall: This service provides firewall protection for the Vault server. It should be running on the DR Vault to ensure security.
? PrivateArk Database: This service manages the database that stores the metadata of the Vault. It should be stopped on the DR Vault, because the database is not active in Replication mode. The database is only activated when the DR Vault switches to Production mode.
? PrivateArk Server: This service manages the Vault server and its communication with other components. It should be stopped on the DR Vault, because the Vault server is not active in Replication mode. The Vault server is only activated when the DR Vault switches to Production mode.
? CyberArk Vault Disaster Recovery: This service manages the replication process between the Primary Vault and the DR Vault. It should be running on the DR Vault to ensure data synchronization and readiness for failover.
? Cyber-Ark Event Notification Engine: This service manages the event notifications and alerts for the Vault. It should be stopped on the DR Vault, because the event notifications are not relevant in Replication mode. The event notifications are only activated when the DR Vault switches to Production mode.
References: Primary-DR environment - CyberArk, Replicate the Primary Vault to the Satellite Vaults - CyberArk

NEW QUESTION 27

When a DR Vault Server becomes an active vault, it will automatically revert back to DR mode once the Primary Vault comes back online.

A. True; this is the default behavior
B. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the padr.ini file
C. True, if the AllowFailback setting is set to "yes" in the padr.ini file
D. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the dbparm.ini file

Answer: B

Explanation:

According to the web search results, when a DR Vault Server becomes an active vault, it will not automatically revert back to DR mode once the Primary Vault comes back online. The Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the padr.ini file1. This file is located in the /opt/CARKaim/conf directory on the DR Vault machine2. The Vault administrator must also stop the replication process on the DR Vault and restart the PrivateArk Server service1. This procedure is known as a DR failback, which restores the original roles of the Primary Vault and the DR Vault after a failover1. The AllowFailback setting in the padr.ini file does not affect the DR failback process, as it only determines whether the DR Vault can be used as a backup for another DR Vault in a cascading DR scenario3. The dbparm.ini file is not relevant for the DR failback process, as it contains the database parameters for the Vault server.
References:
? Initiate a DR failback to the Production Vault - CyberArk
? Install the Disaster Recovery application - CyberArk
? Cascading DR - CyberArk
? [dbparm.ini file - CyberArk]

NEW QUESTION 31

What are the minimum permissions to add multiple accounts from a file when using PVWA bulk-upload? (Choose three.)

A. add accounts
B. rename accounts
C. update account content
D. update account properties
E. view safe members
F. add safes

Answer: ACD

Explanation:

When using PVWA bulk-upload to add multiple accounts from a file, the minimum permissions required are to add accounts, update account content, and update account properties. These permissions ensure that the user has the ability to create new accounts in the Vault, modify the content of the accounts, and change their properties as necessary during the bulk-upload process1.
References:
? CyberArk Docs - Add multiple accounts from a file in V10 Interface

NEW QUESTION 33

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 34
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 37
Which methods can you use to add a user directly to the Vault Admin Group? (Choose three.)

A. REST API
B. PrivateArk Client
C. PACLI
D. PVWA
E. Active Directory
F. Sailpoint

Answer: ABC

Explanation:
To add a user directly to the Vault Admin Group in CyberArk, you can use the following methods:
? REST API: The REST API allows for programmatic management of users and groups within the Vault, including adding users to the Vault Admin Group1.
? PrivateArk Client: The PrivateArk Client provides a graphical interface for managing users and groups, and it can be used to add users directly to the Vault Admin Group2.
? PACLI: The PACLI (Privileged Access Command Line Interface) is a command- line tool that enables administrators to manage the Vault, including adding users to groups2.
These methods provide different ways to manage users and their group memberships within the CyberArk Vault, offering flexibility for administrators to choose the most suitable approach for their needs.
References:
? CyberArk's official documentation on using the REST API to manage users and groups1.
? Information on managing users and groups through the PrivateArk Client and PACLI2.

NEW QUESTION 40
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 42
You have been asked to create an account group and assign three accounts which belong to a cluster. When you try to create a new group, you receive an unauthorized error; however, you are able to edit other aspects of the account properties.
Which safe permission do you need to manage account groups?

A. create folders
B. specify next account content
C. rename accounts
D. manage safe

Answer: D

Explanation:
To manage account groups, you need the manage safe permission, which allows you to create, update, and delete account groups in a safe. The other permissions are not related to account groups. The create folders permission allows you to create folders in a safe. The specify next account content permission allows you to specify the next password or SSH key for an account. The rename accounts permission allows you to rename accounts in a safe. References: Manage account groups, Safe member permissions

NEW QUESTION 46
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 50
In the Private Ark client under the Tools menu > Administrative Tools > Users and Groups, which option do you use 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 PrivateArk client, to update users' Vault group memberships, you use the Member Of tab. After logging in as an administrative user and navigating to the Users and Groups window, you select a user and click Update. In theMember Of tab, you can manage the user's group memberships by adding or removing them from groups within the Vault1.
References:
? CyberArk Docs - Manage users in PrivateArk client1

NEW QUESTION 54
What is the easiest way to duplicate an existing platform?

A. From PrivateArk, copy/paste the appropriate Policy.ini file; then rename it.
B. From the PVWA, navigate to the platforms page, select an existing platform that is similar to the new target account platform and then click Duplicate; name the new platform.
C. From PrivateArk, copy/paste the appropriate settings in PVConfiguration.xml; then update the policyName variable.
D. From the PVWA, navigate to the platforms page, select an existing platform that is similar to the new target account platform, manually update the platform settings and click "Save as" INSTEAD of save to duplicate and rename the platform.

Answer: B

Explanation:
The easiest way to duplicate an existing platform is to use the PVWA, which is the web interface that allows users to access and manage the CyberArk Defender PAM system. The PVWA has a platforms page that displays all the platforms that are available in the system, categorized by platform types. Users can duplicate an existing platform by selecting it, clicking the ellipsis button next to it, and then clicking Duplicate. This will create a copy of the platform with the same settings and properties, which can be customized according to the user's needs. Users can name the new platform and save it in the system.
References: Manage platforms - CyberArk

NEW QUESTION 56
Which of the following files must be created or configured m order to run Password Upload Utility? Select all that apply.

A. PACli.ini
B. Vault.ini
C. conf.ini
D. A comma delimited upload file

Answer: ACD

Explanation:
To run the Password Upload Utility, you need to create or configure the following files:
? A comma delimited upload file: This is a text file that contains the passwords and
their properties that will be uploaded to the Vault. The file must have a .csv extension and follow a specific format. The first line in the file defines the names of the password properties as specified in the Password Vault. Every other line represents a single password object and its property values, according to the properties specified in the first line1.
? PACli.ini: This is a configuration file that stores the parameters for the PACli, which
is a command-line interface that enables communication between the Password Upload Utility and the Vault. The PACli.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: Vault, User, Password, and LogFile2.
? conf.ini: This is a configuration file that stores the parameters for the Password
Upload Utility. The conf.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: InputFile, LogFile, and ErrorFile3.
You do not need to create or configure the following file to run the Password Upload Utility:
? Vault.ini: This is a configuration file that stores the parameters for the Vault server, such as the database name, port, and password. This file is not used by the

Password Upload Utility, and it is not located in the same folder as the Password Upload Utility executable file. The Vault.ini file is located in the Vault installation folder, and it is used by the Vault service and the PrivateArk Client4. References:
? 1: Create the Password File
? 2: PACli.ini
? 3: Password Upload Utility Parameter File (conf.ini)
? 4: [CyberArk Privileged Access Security Implementation Guide], Chapter 2: Installing the Vault, Section: Configuring the Vault, Subsection: Vault.ini

NEW QUESTION 61
Where can PTA be configured to send alerts? (Choose two.)

A. SIEM
B. Email
C. Google Analytics
D. EVD
E. PAReplicate

Answer: AB

Explanation:
CyberArk's Privileged Threat Analytics (PTA) can be configured to send alerts to a Security Information and Event Management (SIEM) system and via Email. SIEM systems are used for real-time analysis of security alerts generated by applications and network hardware, while email alerts can be sent to individual or group email addresses for immediate notification1.
References:
? CyberArk Docs: Send PTA Alerts to Email1

NEW QUESTION 63
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

Answer: B

Explanation:
The report that shows the accounts that are accessible to each user is the Entitlement report. According to the web page in the edge browser, the Entitlement report provides information about users' entitlement rights in PAM - Self-Hosted regarding user, Safe, active platform, target machine, target account, etc. This report includes each user's effective access control and authorization level on each account that the user has access to in PAM - Self-Hosted. The Entitlement report can be generated in PVWA or PrivateArk1.

NEW QUESTION 64
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.

Answer: A

Explanation:
One Time Passwords (OTPs) are passwords that are valid for only one use or a limited time period. The primary purpose of OTPs is to reduce the risk of credential theft, which is a common attack vector for hackers and malicious insiders. By using OTPs, the exposure of the credentials is minimized, and the attacker cannot reuse the stolen password to access the target system. OTPs also enhance the security of the authentication process, as they add an extra layer of verification to the user's identity. OTPs can be generated by various methods, such as SMS, email, hardware tokens, software tokens, etc1.
The other options are not the primary purpose of OTPs, because:
? B. More frequent password changes. This is not the primary purpose of OTPs, but a consequence of using them. OTPs require more frequent password changes, as they expire after one use or a limited time period. However, this is not the main goal of using OTPs, but rather a means to achieve the goal of reducing the risk of credential theft.
? C. Non-repudiation (individual accountability). This is not the primary purpose of
OTPs, but a benefit of using them. Non-repudiation means that the user cannot deny performing an action or accessing a resource, as there is sufficient evidence to prove their identity and activity. OTPs can help achieve non-repudiation, as they are unique and personal to each user, and can be traced back to the user's device or account. However, this is not the main goal of using OTPs, but rather an advantage of using them.
? D. To force a 'collusion to commit' fraud ensuring no single actor may use a
password without authorization. This is not the primary purpose of OTPs, but a feature of using them. OTPs can help prevent unauthorized access to privileged accounts, as they require the user to have both the OTP and the regular password to access the target system. This means that no single actor can use the password without authorization, as they would need the cooperation of another actor who has the OTP. However, this is not the main goal of using OTPs, but rather a capability of using them.
References:
? 1: One-time password

NEW QUESTION 69
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 72
DRAG DROP
Match each permission to where it can be found.

Add Accounts	Drag answer here	Vault
Initiate CPM account management operations	Drag answer here	Safe
Add/Update Users	Drag answer here	
Add Safes	Drag answer here	

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Add Accounts: This permission is associated with the ability to add new accounts to the CyberArk Vault. It is typically found in the Vault's administrative settings where account management is handled.
? Initiate CPM account management operations: This permission allows users to initiate operations related to the Central Policy Manager (CPM) for account management within a Safe. It is found in the Safe's permissions settings.
? Add/Update Users: This permission enables the addition or updating of user information in the Vault. It is found in the Vault's user management settings.
? Add Safes: This permission is related to the creation of new Safes in the Vault. It is found in the Vault's administrative settings where Safe management is conducted.
References:
? The permissions and their locations can be referenced in the CyberArk Defender PAM course materials and official documentation, which provide detailed information on the management of permissions within the CyberArk solution.

NEW QUESTION 73
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

Answer: A

NEW QUESTION 77
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 81
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 83
DRAG DROP
Match the log file name with the CyberArk Component that generates the log.

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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
? Log Files
? [Defender PAM Sample Items Study Guide], Question 46, page 16

NEW QUESTION 88
You are creating a Dual Control workflow for a team's safe. Which safe permissions must you grant to the Approvers group?

A. List accounts, Authorize account request
B. Retrieve accounts, Access Safe without confirmation
C. Retrieve accounts, Authorize account request
D. List accounts, Unlock accounts

Answer: C

Explanation:
When setting up a Dual Control workflow for a team's safe in CyberArk's Privileged Access Management (PAM), the Approvers group must be granted specific permissions to function effectively within the workflow. The permissions required for the Approvers group are to 'Retrieve accounts' and 'Authorize account request'. This allows the Approvers to retrieve the necessary account details and also to authorize requests for access as part of the dual control mechanism. These permissions ensure that the workflow operates smoothly and securely, with the Approvers having the ability to review and approve access requests as needed.
References: The answer is derived from the best practices and guidelines provided in the CyberArk Defender PAM course and learning resources, which include the official CyberArk documentation and study guides. Specifically, the CyberArk documentation outlines the importance of the 'Retrieve accounts' and 'Authorize account request' permissions for Approvers in a Dual Control workflow

NEW QUESTION 93
A newly created platform allows users to access a Linux endpoint. When users click to connect, nothing happens.
Which piece of the platform is missing?

A. PSM-SSH Connection Component
B. UnixPrompts.ini
C. UnixProcess.ini
D. PSM-RDP Connection Component

Answer: A

Explanation:
A platform is a set of parameters that defines how CyberArk manages passwords and sessions for a specific type of account or system. To allow users to access a Linux endpoint, the platform needs to have a PSM-SSH connection component, which enables transparent connections to Linux machines using the SSH protocol. The PSM-SSH connection component is configured in the Master Policy and defines the settings for the PSM connection, such as the port, the authentication method, and the terminal type. If the platform is missing the PSM-SSH connection component, the users will not be able to click to connect to the Linux endpoint. References: Connection Components, PSM-SSH Connection Component

NEW QUESTION 98
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

Answer: B

Explanation:
The Accounts Feed is a feature of the CyberArk Privileged Access Security Solution that enables the discovery and provisioning of privileged accounts in the environment. The Accounts Feed contains the accounts that were discovered by CyberArk that have not yet been onboarded to the Vault. These accounts are displayed in the Pending Accounts page in the PVWA, where the user can view, analyze, and onboard them according to various criteria. The Accounts Feed helps the user to identify and manage the unmanaged privileged accounts that pose a security risk1.
The other options are not correct, because:
? A. Accounts that were discovered by CyberArk in the last 30 days. This is not correct, because the Accounts Feed does not contain all the accounts that were discovered by CyberArk in the last 30 days, but only the ones that have not yet been onboarded. The accounts that were already onboarded to the Vault are not part of the Accounts Feed, but are displayed in the Accounts page in the PVWA1.
? C. All accounts added to the vault in the last 30 days. This is not correct, because the Accounts Feed does not contain the accounts that were added to the Vault, but the ones that are waiting to be onboarded. The accounts that were added to the Vault are not part of the Accounts Feed, but are displayed in the Accounts page in the PVWA1.
? D. All users added to CyberArk in the last 30 days. This is not correct, because the Accounts Feed does not contain the users that were added to CyberArk, but the accounts that are waiting to be onboarded. The users that were added to CyberArk are not part of the Accounts Feed, but are displayed in the Users page in the PVWA1.
References:
? 1: Accounts Feed

NEW QUESTION 100
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 105
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 107
Which report could show all accounts that are past their expiration dates?

A. Privileged Account Compliance Status report
B. Activity log
C. Privileged Account Inventory report
D. Application Inventory report

Answer: A

Explanation:
The Privileged Account Compliance Status report shows the compliance status of all privileged accounts in the Vault, based on the expiration date and password change policy. This report can help identify accounts that are past their expiration dates and need to be updated or removed. References:
? [Defender PAM Sample Items Study Guide], page 18, question 90
? [CyberArk Privileged Access Security Documentation], version 12.3, Reports Guide, page 27, Privileged Account Compliance Status report

NEW QUESTION 109
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 often 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: B

Explanation:
The Immediate Interval setting in a CPM policy is used to control how often the CPM looks for User Initiated CPM work, such as manual password changes, retrievals, or requests. The Immediate Interval setting defines the frequency, in minutes, that the CPM will check the accounts that are associated with the policy and perform the actions that were initiated by the users. For example, if the Immediate Interval is set to 2, the CPM will check the accounts every 2 minutes and change, retrieve, or authorize the passwords according to the user requests. The Immediate Interval setting does not affect System Initiated CPM work, such as password changes, verifications, or reconciliations that are triggered by the policy settings, such as Expiration Period or One Time Password. These actions are controlled by the Interval setting in the CPM policy. The Immediate Interval setting also does not control how often the CPM rests between password changes or the maximum amount of time the CPM will wait for a password change to complete. These parameters are configured in the CPM.ini file, which is stored in the root folder of the <CPM username> Safe. References:
? [Defender PAM eLearning Course], Module 5: Password Management, Lesson 5.1: CPM Policies, Slide 9: CPM Policy Settings
? [Defender PAM Sample Items Study Guide], Question 6: CPM Policy Settings
? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 5: Managing Passwords, Section: CPM Policy Settings, Subsection: Immediate Interval

NEW QUESTION 114
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 117
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

Answer: A

Explanation:
A Vault Admin may still access a safe outside of the hours that it has been configured to be accessible, as long as he has the Bypass Safe Time Restrictions authorization on the Vault. The Bypass Safe Time Restrictions authorization enables a user to access any safe in the Vault, regardless of the time restrictions that are defined for that safe. This authorization is useful for emergency situations or maintenance tasks that require access to safes outside of the normal working hours. By default, the Vault Admins group has this authorization, as well as other administrative authorizations on the Vault1. References:
? 1: Vault Member Authorizations

NEW QUESTION 121
You have been asked to secure a set of shared accounts in CyberArk whose passwords will need to be used by end users. The account owner wants to be able to track who was using an account at any given moment.
Which security configuration should you recommend?

A. Configure one-time passwords for the appropriate platform in Master Policy.
B. Configure shared account mode on the appropriate safe.
C. Configure both one-time passwords and exclusive access for the appropriate platform in Master Policy.
D. Configure object level access control on the appropriate safe.

Answer: C

Explanation:
One-time passwords and exclusive access are security features that can be configured for a platform in the Master Policy. These features enhance the security and accountability of shared accounts by ensuring that each password is used only once and by only one user at a time. One-time passwords generate a new password for each check-out and check-in of an account, preventing password reuse and exposure. Exclusive access prevents multiple users from accessing the same account simultaneously, avoiding conflicts and confusion. By configuring both one-time passwords and exclusive access for the appropriate platform, the account owner can track who was using an account at any given moment and ensure that the passwords are always secure and unique. References
: One-Time Passwords, Exclusive Access, Master Policy

NEW QUESTION 125
Which processes reduce the risk of credential theft? (Choose two.)

A. require dual control password access approval
B. require password change every X days
C. enforce check-in/check-out exclusive access
D. enforce one-time password access

Answer: BD

NEW QUESTION 130
You have been asked to identify the up or down status of Vault services. Which CyberArk utility can you use to accomplish this task?

A. Vault Replicator
B. PAS Reporter
C. Remote Control Agent
D. Syslog

Answer: C

Explanation:
 The Remote Control Agent (PARAgent) is a CyberArk utility that can be used to monitor the status of Vault services remotely. It can also perform other tasks, such as starting and stopping the Vault, backing up and restoring the Vault, and running other utilities. The PARAgent communicates with the Remote Control Client (PARClient), which is a graphical user interface that displays the Vault status and allows the user to execute commands on the Vault. The PARAgent can also send SNMP traps to a remote terminal if the Vault service is down. References: How do I monitor the Vault status remotely?, Monitor system health

NEW QUESTION 134
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 138
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 139
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

PAM-DEF Practice Exam Features:

* PAM-DEF Questions and Answers Updated Frequently

* PAM-DEF Practice Questions Verified by Expert Senior Certified Staff

* PAM-DEF Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PAM-DEF Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year