CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM

NEW QUESTION 1
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 2
Which accounts can be selected for use in the Windows discovery process? (Choose two.)

A. an account stored in the Vault
B. an account specified by the user
C. the Vault Administrator
D. any user with Auditor membership
E. the PasswordManager user

Answer: AB

Explanation:
During the Windows discovery process in CyberArk Defender PAM, accounts that can be selected for use include an account that is already stored in the Vault and an account that is specified by the user. The discovery process scans predefined machines for new and modified accounts and their dependencies. After the scan, accounts that should be onboarded into the Vault for secure and automatic management are identified12. References: The information provided is based on general knowledge of CyberArk PAM best practices and the account discovery process as outlined in CyberArk's official documentation1

NEW QUESTION 3
Which parameters can be used to harden the Credential Files (CredFiles) while using CreateCredFile Utility? (Choose three.)

A. Operating System Username
B. Host IP Address
C. Client Hostname
D. Operating System Type (Linux/Windows/HP-UX)
E. Vault IP Address
F. Time Frame

Answer: BCE

Explanation:
When using the CreateCredFile Utility to harden Credential Files (CredFiles), it is important to include parameters that enhance security. The Host IP Address, Client Hostname, and Vault IP Address are parameters that can be used to specify the environment in which the CredFile is valid, thereby restricting its use to specific machines or networks1. This helps prevent unauthorized access to the CredFile and ensures that it is only used in the intended context.
References:
? CyberArk's official documentation on the CreateCredFile utility provides insights into the security mechanisms used to protect credential files, including the use of environmental key materials such as application-based, machine-based, and component-based materials1.
? For a deeper understanding of how to secure Credential Files and the use of the CreateCredFile Utility, refer to the CyberArk Defender PAM course materials and study guide2.

NEW QUESTION 4
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 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
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 7
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 8
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 9
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
In a rule using “Privileged Session Analysis and Response” in PTA, which session options are available to configure as responses to activities?

A. Suspend, Terminate, None
B. Suspend, Terminate, Lock Account
C. Pause, Terminate, None
D. Suspend, Terminate

Answer: A

Explanation:
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security- Configuration.htm?TocPath=End%20User%7CSecurity%20Events%7C3
These are the session response options that can be configured in a rule using Privileged Session Analysis and Response in PTA. These options determine how PTA reacts to suspicious activities detected in a privileged session. Suspend means that the session is paused and the user is notified. Terminate means that the session is ended and the user is disconnected. None means that no action is taken on the session, but the event is still recorded and reported. You can find more information about these options and how to configure them in the reference below.
Reference:
Configure security events

NEW QUESTION 10
Which of the following statements are NOT true when enabling PSM recording for a target Windows server? (Choose all that apply)

A. The PSM software must be instated on the target server
B. PSM must be enabled in the Master Policy (either directly, or through exception)
C. PSMConnect must be added as a local user on the target server
D. RDP must be enabled on the target server

Answer: AC

Explanation:
The following statements are not true when enabling PSM recording for a target Windows server:
? A. The PSM software must be instated on the target server. This is not true, because the PSM software is installed on a dedicated server that acts as a proxy between the user and the target server. The PSM server intercepts the user’s connection request, initiates the connection to the target server, and records the privileged session. The target server does not need to have the PSM software installed on it1.
? C. PSMConnect must be added as a local user on the target server. This is not true, because PSMConnect is a predefined user that is created on the PSM server during the installation. This user is used to establish the connection between the PSM server and the target server, and to run the PSM processes. The target server does not need to have a local user named PSMConnect on it2.
The following statements are true when enabling PSM recording for a target Windows server:
? B. PSM must be enabled in the Master Policy (either directly, or through exception). This is true, because the Master Policy is a centralized overview of the security and compliance policy of privileged accounts in the organization. It allows the administrator to configure compliance driven rules that are defined as the baseline for the enterprise. One of the rules in the Master Policy is the Session Isolation rule, which determines whether or not privileged sessions are isolated and recorded by PSM. This rule can be enabled either directly in the Master Policy, or through an exception for a specific scope of accounts3.
? D. RDP must be enabled on the target server. This is true, because RDP is the protocol that is used by PSM to connect to Windows servers. The target server

must have RDP enabled and configured properly to allow the PSM server to access it. The PSM server must also have the RDP client installed on it4.
References:
? 1: Privileged Session Manager
? 2: PSMConnect and PSMAdminConnect
? 3: Session Isolation
? 4: Configure RDP for PSM

NEW QUESTION 15
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 16
Which statement about the Master Policy best describes the differences between one-time password and exclusive access functionality?

A. Exclusive access means that only a specific group of users may use the accoun
B. After an account on a one-time password platform is used, the account is deleted from the safe automatically.
C. Exclusive access locks the account indefinitel
D. One-time password can be used replace invalid account passwords.
E. Exclusive access is enabled by default in the Master Polic
F. One-time password should only be enabled for emergencies.
G. Exclusive access allows only one person to check-out an account at a tim
H. One-time password schedules an account for a password change after the MinValidityPeriod period expires.

Answer: D

Explanation:
The Master Policy in CyberArk defines the behavior of one-time passwords and exclusive accessExclusive access ensures that only one user can check out an account at any given time, effectively locking the account during its use to prevent simultaneous access1. On the other hand, one-time password functionality is designed to change the account's password after it is used, based on a timer set by the MinValidityPeriod parameter in the policy file. This means that once the password is checked out and the timer expires, the Central Policy Manager (CPM) will change the password2. These settings are often used together to maintain accountability and security for the usage of shared privileged accounts. References:
? CyberArk Docs: One-time passwords and exclusive accounts1
? CyberArk Knowledge Article: CPM: What is the difference between "One Time" and "Exclusive" passwords?2

NEW QUESTION 20
Which statement is correct concerning accounts that are discovered, but cannot be added to the Vault by an automated onboarding rule?

A. They are added to the Pending Accounts list and can be reviewed and manually uploaded.
B. They cannot be onboarded to the Password Vault.
C. They must be uploaded using third party tools.
D. They are not part of the Discovery Process.

Answer: A

Explanation:
When accounts are discovered by CyberArk but do not match any automated onboarding rule, they are added to the Pending Accounts list. This allows administrators to review these accounts and decide whether to onboard them manually into the Vault. The Pending Accounts list serves as a holding area for accounts that require further review or do not meet the criteria set by existing onboarding rules1.
References:
? CyberArk's official documentation on Onboarding Rules, which explains the process of managing accounts that are discovered but not automatically onboarded1.

NEW QUESTION 23
A user has successfully conducted a short PSM session and logged off. However, the user cannot access the Monitoring tab to view the recordings.
What is the issue?

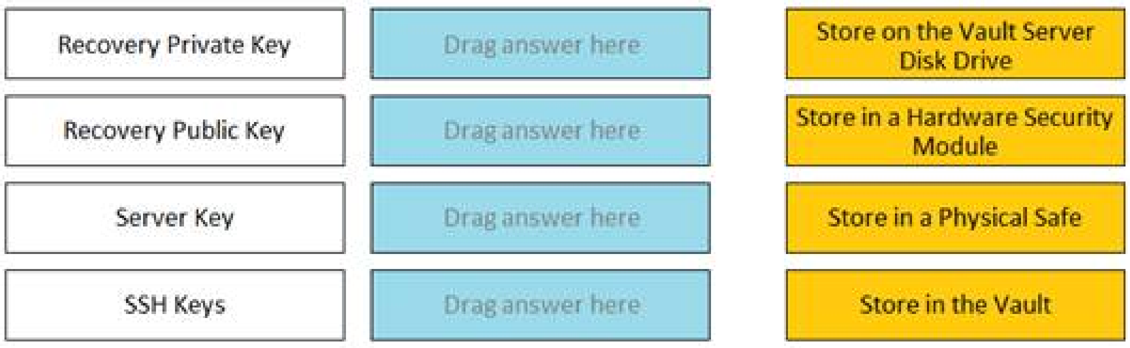
A. The user must login as PSMAdminConnect
B. The PSM service is not running
C. The user is not a member of the PVWAMonitor group
D. The user is not a member of the Auditors group

Answer: D

Explanation:
To access the Monitoring tab and view the recordings of the PSM sessions, the user must have membership in the Auditors group or membership in the relevant

Account Safes and Recording Safes with the appropriate permissions1. The user must also use the same connection method (RDP file or HTML5 Gateway) as the end user who conducted the session1. The other options are not relevant to the issue, as the user does not need to login as PSMAdminConnect, the PSM service is running if the user was able to conduct a session, and the PVWAMonitor group is not a valid group in CyberArk. References:
? Monitor Privileged Sessions - CyberArk, section “The MONITORING page”

NEW QUESTION 26
DRAG DROP
Match each key to its recommended storage location.



Recovery Private Key	Drag answer here	Store on the Vault Server Disk Drive
Recovery Public Key	Drag answer here	Store in a Hardware Security Module
Server Key	Drag answer here	Store in a Physical Safe
SSH Keys	Drag answer here	Store in the Vault

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? The recommended storage locations for each key are as follows:
? Recovery Private Key: It is recommended to store the Recovery Private Key on the Vault Server Disk Drive. This is because the Recovery Private Key is used to decrypt the data stored in the Vault.
? Recovery Public Key: It is recommended to store the Recovery Public Key in a Hardware Security Module. This is because the Recovery Public Key is used to encrypt the data stored in the Vault.
? Server Key: It is recommended to store the Server Key in a Physical Safe. This is because the Server Key is used to open the Vault, much like the key of a physical Vault. The key is required to start the Vault, after which the Server Key can be removed until the Server is restarted. When the Vault is stopped, the information stored in the Vault is completely inaccessible without that key.
? SSH Keys: It is recommended to store the SSH Keys in the Vault. This is because the SSH Keys are used to connect to remote machines using the SSH protocol. The Vault can manage the passwords and sessions for the SSH Keys and provide secure access to the target systems.
References: Server keys - CyberArk, Cyberark Key Storage Plugin (Enterprise) - Rundeck

NEW QUESTION 28
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 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 36
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 38
Accounts Discovery allows secure connections to domain controllers.

A. TRUE
B. FALSE

Answer: B

NEW QUESTION 42
It is possible to leverage DNA to provide discovery functions that are not available with auto-detection.

A. TRUE
B. FALSE

Answer: A

Explanation:
It is possible to leverage DNA to provide discovery functions that are not available with auto-detection. Auto-detection is a feature that enables the CPM to automatically discover and onboard accounts on target systems that are associated with a specific platform. Auto-detection can be configured in the Platform Management settings for each platform that supports this functionality. However, auto-detection has some limitations, such as requiring the CPM to have access to the target system, not supporting all platforms, and not providing comprehensive information about the accounts and their security risks1. DNA, on the other hand, is a standalone scanning tool that can discover and audit privileged accounts across the network, regardless of the platform or the CPM access. DNA can provide additional discovery functions, such as identifying machines vulnerable to Pass-the-Hash attacks, collecting reliable and comprehensive audit information, and generating reports and visual maps that evaluate the privileged account security status in the organization2. DNA can also be used before or independently of the CyberArk PAM solution, as it does not require agents to be installed on target systems2. References:
? 1: Auto-detection
? 2: CyberArk DNA Overview

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 49
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 51
You are configuring CyberArk to use HTML5 gateways exclusively for PSM connections. In the PVWA, where do you set DefaultConnectionMethod to HTML5?

A. Options > Privileged Session Management UI
B. Options > Privileged Session Management
C. Options > Privileged Session Management Defaults
D. Options > Privileged Session Management Interface

Answer: A

Explanation:
To configure CyberArk to use HTML5 gateways exclusively for PSM connections, you need to set the DefaultConnectionMethod to HTML5 in the PVWA. This is done by logging in to the PVWA with an administrative user, navigating to Options > Privileged Session Management UI, and setting the DefaultConnectionMethod to HTML51. This configuration ensures that HTML5 sessions are triggered only for PSM machines associated with the HTML5 Gateway1.
References:
? CyberArk Docs - Secure Access with an HTML5 Gateway1

NEW QUESTION 55
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 58
When creating an onboarding rule, it will be executed upon .

A. All accounts in the pending accounts list
B. Any future accounts discovered by a discovery process
C. Both “All accounts in the pending accounts list” and “Any future accounts discovered by a discovery process”

Answer: C

Explanation:
According to the CyberArk Defender PAM documentation1, when creating an onboarding rule, it will be executed upon both all accounts in the pending accounts list and any future accounts discovered by a discovery process. This means that the rule will automatically onboard and provision the accounts that match the rule criteria, regardless of when they were discovered. The rule will also apply to any new accounts that are discovered by subsequent discovery processes. This way, the onboarding rule can minimize the time and effort required to securely manage the accounts in the vault.

NEW QUESTION 61
It is possible to restrict the time of day, or day of week that a [b]reconcile[/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 reconcile process can occur by using the Reconcile Safe option in thePlatform Management section of thePrivateArk Client. This option allows the administrator to define the reconcile schedule for each platform, which specifies when the reconcile process can run

and how often it should be performed. The reconcile schedule can be set to run daily, weekly, monthly, or on specific days and times. By restricting the reconcile process, the administrator can reduce the risk of unauthorized access to the accounts and improve the performance of the system. References:
? [Defender PAM Course], Module 5: Reconcile and Rotate, Lesson 1: Reconcile and Rotate Overview, Slide 9: Reconcile Safe
? [Defender PAM Study Guide], Section 5.1: Reconcile and Rotate Overview, Page 24: Reconcile Safe
? [CyberArk Documentation], Privileged Access Security Implementation Guide, Chapter 5: Configure the Vault, Section 5.4: Configure Platforms, Subsection 5.4.2: Reconcile Safe

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 66
One can create exceptions to the Master Policy based on .

A. Safes
B. Platforms
C. Policies
D. Accounts

Answer: B

Explanation:
The Master Policy is a set of rules that apply to all accounts in the Vault. However, one can create exceptions to the Master Policy based on platforms, which are logical groupings of accounts that share common characteristics, such as operating system, device type, or application. By creating platform-specific policies, one can override the Master Policy settings for certain accounts and customize the security and management options for different platforms. References:
? Defender PAM Sample Items Study Guide, page 9
? CyberArk Core Privileged Access Security Documentation, Master Policy Overview and Platform-Specific Policies

NEW QUESTION 67
What does the Export Vault Data (EVD) utility do?

A. exports data from the Vault to TXT or CSV files, or to MSSQL databases
B. generates a backup file that can be used as a cold backup
C. exports all passwords and imports them into another instance of CyberArk
D. keeps two active vaults in sync

Answer: A

Explanation:
The Export Vault Data (EVD) utility is used to export data from the CyberArk Vault to TXT or CSV files, or to MSSQL databases. This utility enables the creation of reports such as a list of Safes or incoming requests by exporting data from the Vault. Each report is saved in a separate file, which can then be imported into third-party applications or databases for further analysis or reporting purposes12.
References:
? CyberArk Docs - Export Vault Data (EVD) utility1
? CyberArk Docs - Export data to files

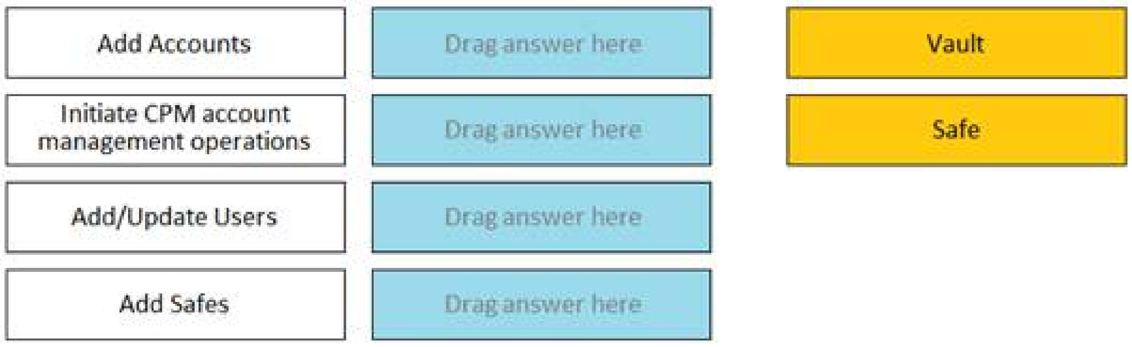
NEW QUESTION 70
The vault supports Subnet Based Access Control.

A. TRUE
B. FALSE

Answer: A

Explanation:
According to the web page in the edge browser, the vault supports Subnet Based Access Control. This is a feature that allows you to restrict access to a key vault to a specified virtual network and subnet. You can also use firewall settings to deny internet traffic and allow only specific IP addresses. This way, you can enhance the security and privacy of your key vault data12

NEW QUESTION 73
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 78
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 81
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 82
Which permissions are needed for the Active Directory user required by the Windows Discovery process?

A. Domain Admin
B. LDAP Admin
C. Read/Write
D. Read

Answer: D

Explanation:
The Active Directory user required by the Windows Discovery process needs to have Read permissions in the OU to scan and all sub-OUs1. This allows the Discovery process to scan predefined machines for new and modified accounts and their dependencies without requiring elevated privileges such as Domain Admin or LDAP Admin rights. The Read permission is sufficient for the Discovery process to retrieve the necessary information about the accounts that should be onboarded into the Vault. References:
? CyberArk's official documentation on managing discovery processes outlines the permissions required for the Discovery process, including the need for Read permissions for the Active Directory user performing the discovery1.
? Additional details on the required credentials for scanning and the Discovery process can be found in the supported target machines section of CyberArk's documentation2.

NEW QUESTION 87
Via Password Vault Web Access (PVWA), a user initiates a PSM connection to the target Linux machine using RemoteApp. When the client's machine makes an RDP connection to the PSM server, which user will be utilized?

A. Credentials stored in the Vault for the target machine
B. Shadowuser
C. PSMConnect
D. PSMAdminConnect

Answer: C

Explanation:
According to the CyberArk Defender PAM documentation1, when a user initiates a PSM connection to the target Linux machine using RemoteApp via PVWA, the client's machine makes an RDP connection to the PSM server using the PSMConnect user. The PSMConnect user is a local or domain user that starts PSM sessions on the PSM machine. The PSMConnect user has limited permissions and access rights on the PSM server, and its credentials are managed by the CPM. The PSMConnect user retrieves the credentials of the target account from the vault and uses them to establish a secure connection to the target machine. The user can then interact with the target machine through the PSM session, while the PSM server records and audits the session activity.

NEW QUESTION 90
What is the purpose of the CyberArk Event Notification Engine service?

A. It sends email messages from the Central Policy Manager (CPM)
B. It sends email messages from the Vault
C. It processes audit report messages
D. It makes Vault data available to components

Answer: B

Explanation:
The purpose of the CyberArk Event Notification Engine service is to send email notifications about Privileged Access Security solution activities automatically to predefined users. It is installed automatically as part of the Vault server installation as a service. The Event Notification Engine (ENE) can be configured to send email notifications for various events, such as password changes, password verifications, account onboarding, account deletion, audit reports, alerts, and more. The ENE can also support encrypted and authenticated email notifications, as well as high availability implementations1. References:
? Event Notification Engine - CyberArk, section "Event Notification Engine"

NEW QUESTION 93
You created a new platform by duplicating the out-of-box Linux through the SSH platform.
Without any change, which Text Recorder Type(s) will the new platform support? (Choose two.)

A. SSH Text Recorder
B. Universal Keystrokes Text Recorder
C. Events Text Recorder
D. SQL Text Recorder
E. Telnet Commands Text Recorder

Answer: AB

Explanation:
When a new platform is created by duplicating the out-of-the-box Linux through the SSH platform, it will support the SSH Text Recorder and theUniversal Keystrokes Text Recorder by default. The SSH Text Recorder is designed to record all the keystrokes that are typed during privileged sessions on SSH connections1. The Universal Keystrokes Text Recorder can record all the keystrokes that are typed during privileged sessions on all supported connections1. These text recorders are automatically enabled at the Master Policy level and can be customized at the platform level1. References:
? CyberArk Docs: Recordings and Audits

NEW QUESTION 95
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 98
If the AccountUploader Utility is used to create accounts with SSH keys, which parameter do you use to set the full or relative path of the SSH private key file that will be attached to the account?

A. KeyPath
B. KeyFile
C. ObjectName
D. Address

Answer: B

Explanation:
When using the AccountUploader Utility to create accounts with SSH keys, the parameter used to set the full or relative path of the SSH private key file that will be attached to the account is KeyFile. This parameter specifies the location of the SSH private key file, which is then associated with the account being onboarded into the CyberArk Privileged Access Security system. The correct configuration of this parameter is crucial for the successful attachment of the SSH key to the account1.
References:
? CyberArk's official documentation on the AccountUploader Utility, which provides detailed information on the parameters and usage for onboarding accounts with SSH keys1.

NEW QUESTION 100
According to CyberArk, which issues most commonly cause installed components to display as disconnected in the System Health Dashboard? (Choose two.)

A. network instabilities/outages
B. vault license expiry
C. credential de-sync
D. browser compatibility issues
E. installed location file corruption

Answer: AC

Explanation:
The System Health Dashboard in CyberArk provides a visual representation of the health status of different CyberArk components. When components are displayed as disconnected, the most common issues are network instabilities/outages and credential de- sync. Network issues can disrupt the connectivity between components and the Vault, while credential de-sync indicates that a component is no longer able to authenticate to the Vault due to synchronization problems with the credentials12. References:
? CyberArk Docs: Monitor system health1
? CyberArk Docs: System Health Dashboard details

NEW QUESTION 102
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 107
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

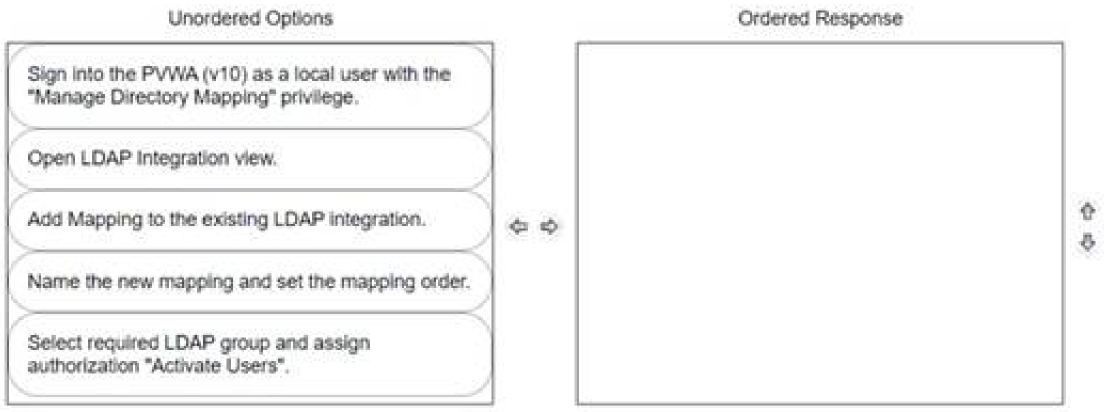
NEW QUESTION 110
The Password upload utility can be used to create safes.

A. TRUE
B. FALSE

Answer: A

Explanation:
The Password Upload utility can be used to create safes, as well as password objects, folders, and platforms. The Password Upload utility works with the CyberArk Password Vault to create password objects from a passwords list and store them in the Vault. This enables you to upload large numbers of passwords automatically and makes the Vault implementation process quicker and more automatic. The Password Upload utility initiates the Vault environment required to store passwords in the safe and start working with them. This includes creating new safes, adding the CPM user as a safe owner, and sharing the safe with the Password Vault Web Access1. References:
? 1: Password Upload Utility

NEW QUESTION 113
DRAG DROP
You have been asked to delegate the rights to unlock users to Tier 1 support. The Tier 1 support team already has an LDAP group for its members.
Arrange the steps to do this in the correct sequence.



Unordered Options

Sign into the PVWA (v10) as a local user with the "Manage Directory Mapping" privilege.

Open LDAP Integration view.

Add Mapping to the existing LDAP integration.

Name the new mapping and set the mapping order.

Select required LDAP group and assign authorization "Activate Users".

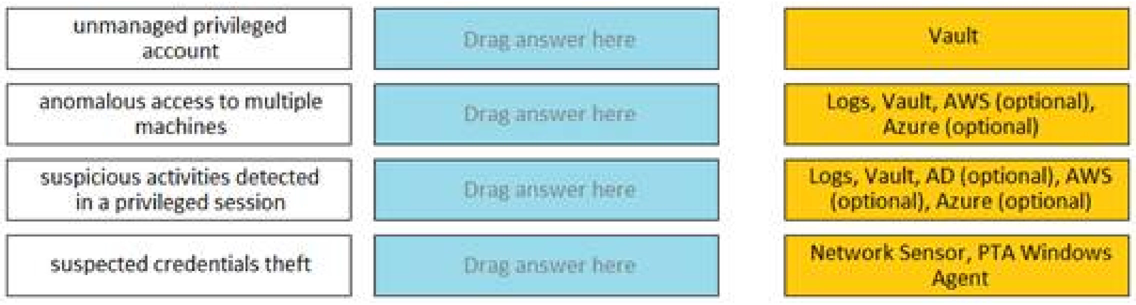
Ordered Response

A. Mastered
B. Not Mastered

Answer: A

Explanation:
The correct sequence to delegate the rights to unlock users to Tier 1 support with an existing LDAP group is as follows:
? Sign into the PWA (V10) as a local user with the “Manage Directory Mapping”
privilege.
? Open LDAP Integration view.
? Add Mapping to the existing LDAP integration.
? Name the new mapping and set the mapping order.
? Select required LDAP group and assign authorization “Activate Users”. Comprehensive Explanation: To delegate the rights to unlock users, you must first access the Privileged Web Access (PWA) with the appropriate privileges to manage directory mappings. Then, navigate to the LDAP Integration view to add a new mapping to the existing LDAP integration. This mapping should be named and ordered correctly. Finally, select the LDAP group that represents Tier 1 support and assign the specific authorization needed to unlock users, which is “Activate Users” in this context12. References:
? CyberArk Docs: LDAP Integration in V102
? CyberArk Knowledge Article: How to delegate permissions to unlock Active Directory accounts1

NEW QUESTION 115
DRAG DROP
Match each PTA alert category with the PTA sensors that collect the data for it.



unmanaged privileged account	Drag answer here	Vault
anomalous access to multiple machines	Drag answer here	Logs, Vault, AWS (optional), Azure (optional)
suspicious activities detected in a privileged session	Drag answer here	Logs, Vault, AD (optional), AWS (optional), Azure (optional)
suspected credentials theft	Drag answer here	Network Sensor, PTA Windows Agent

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Comprehensive Explanation: The Privileged Threat Analytics (PTA) sensors are designed to collect specific types of data to detect potential security threats. For

the alert category of Unmanaged privileged account, the Network Sensor andPTA Windows Agent are responsible for collecting the relevant data. Similarly, for the alert category of Anomalous access to multiple machines, data is collected from Logs, the Vault, and optionally from AWS andAzure. The Suspicious activities detected in a privileged session category relies on data fromLogs, the Vault, and optionally from AD, AWS, and Azure. Lastly, the Suspected credentials theft category also utilizes theNetwork Sensor andPTA Windows Agent for data collection.
References:
? CyberArk's official training materials and documentation provide detailed information on PTA sensors and the types of data they collect for different alert categories.

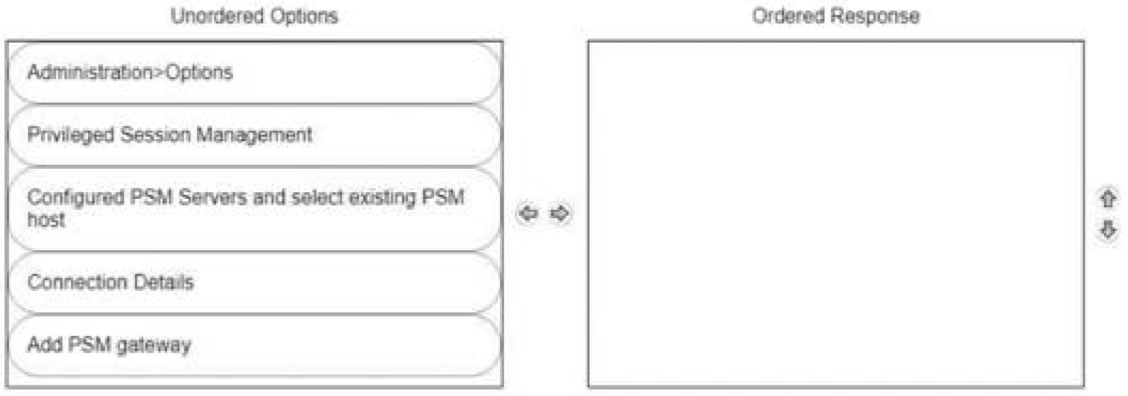
NEW QUESTION 117
How much disk space do you need on the server for a PAReplicate?

A. 500 GB
B. 1 TB
C. same as disk size on Satellite Vault
D. same as disk size on Primary Vault

Answer: D

Explanation:
The PAReplicate utility exports the Safe files from the CyberArk Vault to a computer on the local network where the Backup utility has been installed. The Safes are copied in a similar format and structure to the one in the Server. Therefore, the disk space required on the server for a PAReplicate is the same as the disk size on the Primary Vault1. References: Use the CyberArk Backup Process

NEW QUESTION 119
DRAG DROP
A new HTML5 Gateway has been deployed in your organization.
From the PVWA, arrange the steps to configure a PSM host to use the HTML5 Gateway in the correct sequence.



Unordered Options

Administration>Options

Privileged Session Management

Configured PSM Servers and select existing PSM host

Connection Details

Add PSM gateway

Ordered Response

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To configure a PSM host to use the HTML5 Gateway from the PVWA, you would typically follow these steps:
? Log into the PVWA with an administrative user.
? Navigate to Administration > Options.
? Right-click on Privileged Session Management and select Add Configured PSM Gateway Servers.
? Right-click Configured PSM Gateway Servers, then Add PSM Gateway Server.
? Select the newly added gateway server and enter a unique ID for the PSM HTML5 Gateway.
? Expand the newly created gateway server and enter the necessary configuration details.
Please note that these steps are based on general procedures for configuring a PSM host with an HTML5 Gateway and should be verified against the official CyberArk documentation or by a qualified CyberArk professional. For detailed instructions and best practices, refer to the CyberArk documentation123.

NEW QUESTION 121
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 122
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.

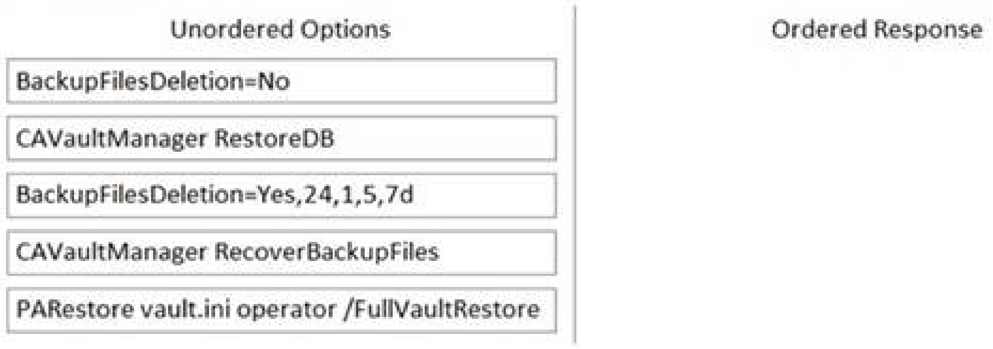
NEW QUESTION 125
You receive this error:
"Error in changepass to user domain\user on domain server(\domain.(winRc=5) Access is denied."
Which root cause should you investigate?

A. The account does not have sufficient permissions to change its own password.
B. The domain controller is unreachable.
C. The password has been changed recently and minimum password age is preventing the change.
D. The CPM service is disabled and will need to be restarted.

Answer: A

Explanation:
The error message "Error in changepass to user domain\user on domain server(\domain.(winRc=5) Access is denied" suggests that the account attempting to change the password does not have the necessary permissions to do so. This could be due to several reasons, such as the account not being part of the appropriate group with password change privileges, or specific restrictions set on the account that prevent password changes. It's important to verify the account's permissions and ensure it has the ability to change its own password within the domain.
References: The conclusion is based on common issues encountered in CyberArk's Privileged Access Management (PAM) when managing account passwords and the associated error codes. The CyberArk documentation and community discussions provide insights into troubleshooting such errors, where insufficient permissions are a frequent cause

NEW QUESTION 127
DRAG DROP
Arrange the steps to restore a Vault using PARestore for a Backup in the correct sequence.



Unordered Options

BackupFilesDeletion=No
CAVaultManager RestoreDB
BackupFilesDeletion=Yes,24,1,5,7d
CAVaultManager RecoverBackupFiles
PARestore vault.ini operator /FullVaultRestore

Ordered Response

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 128
Which report provides a list of account stored in the vault.

A. Privileged Accounts Inventory
B. Privileged Accounts Compliance Status
C. Entitlement Report
D. Active Log

Answer: A

Explanation:
The report that provides a list of accounts stored in the vault is the Privileged Accounts Inventory report. This report can be generated in the Reports page in the PVWA by users who belong to the group that is specified in the ManageReportsGroup parameter in the Reports section of the Web Access Options in the System Configuration page1. The Privileged Accounts Inventory report contains information such as the safe, folder, name, platform ID, username, address, group, last accessed date, last accessed by, last modified date, last modified by, verification date, checkout date, checked out by, age, change failure, verification failure, master pass folder, master pass name, disabled by, and disabled reason of each account stored in the vault2. References:
? 1: Reports in PVWA
? 2: Users List Report

NEW QUESTION 131
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 136
......