# CyberArk

## Exam Questions PAM-DEF

CyberArk Defender - PAM

**NEW QUESTION 1**
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 2**
Which one the following reports is NOT generated by using the PVWA?

A. Accounts Inventory
B. Application Inventory
C. Sales List
D. Convince Status

**Answer:** C

**Explanation:**
The PVWA can generate various reports on the privileged accounts and applications in the system, based on different filters and criteria. However, the Safes List report is not one of them. The Safes List report is generated by using the PrivateArk Client, and it provides a list of Safes and their properties according to location.
References:
Defender-PAM Study Guide, Reports and Audits

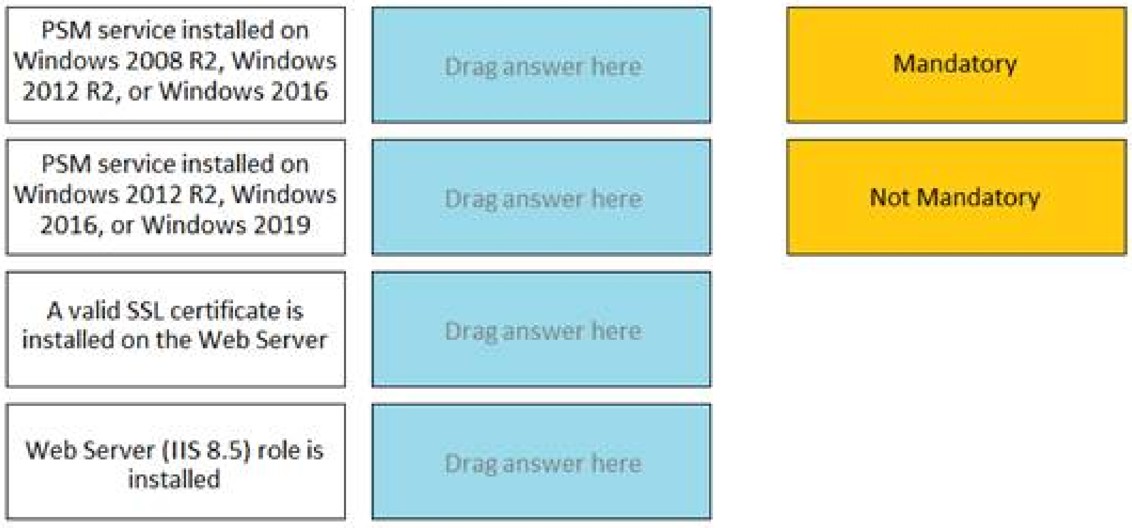
**NEW QUESTION 3**
The primary purpose of exclusive accounts is to ensure non-repudiation (Individual accountability).

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**
DRAG DROP
For each listed prerequisite, identify if it is mandatory or not mandatory to run the PSM Health Check.



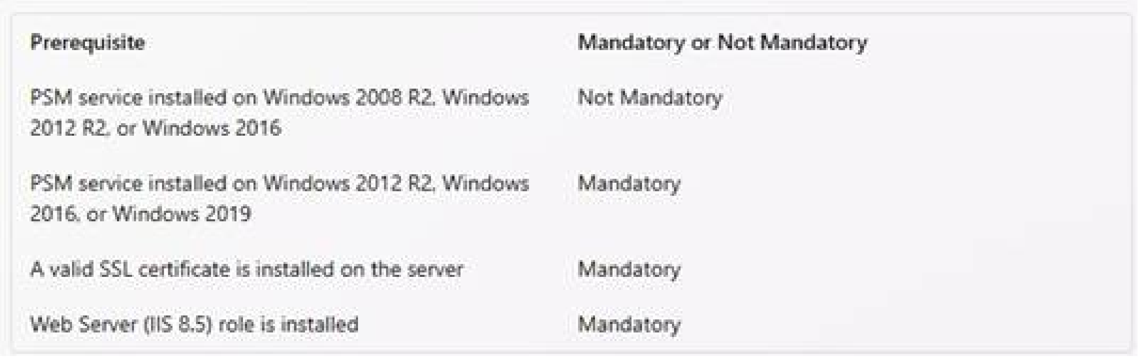
| | | |
|---|---|---|
| PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016 | Drag answer here | Mandatory |
| PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019 | Drag answer here | Not Mandatory |
| A valid SSL certificate is installed on the Web Server | Drag answer here | |
| Web Server (IIS 8.5) role is installed | Drag answer here | |

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**

According to the CyberArk documentation1, the prerequisites for running the PSM Health Check are:
? PSM service installed on Windows 2016 or Windows 2019
? Web Server (IIS 8.5) role is installed
? A valid SSL certificate is installed on the Web Server
Therefore, these prerequisites are mandatory for the PSM Health Check to work properly. The PSM service installed on Windows 2008 R2 is not mandatory, as it is not supported by the PSM Health Check2.
References: PSM Health Check, PSM Health Check - CyberArk



| Prerequisite | Mandatory or Not Mandatory |
|---|---|
| PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016 | Not Mandatory |
| PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019 | Mandatory |
| A valid SSL certificate is installed on the server | Mandatory |
| Web Server (IIS 8.5) role is installed | Mandatory |

**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 required to enable access over SSH to a Unix account through both PSM and PSMP?

A. The platform must contain connection components for PSM-SSH and PSMP-SSH.
B. PSM and PSMP must already have stored the SSH Fingerprint for the Unix host.
C. The 'Enable PSMP' setting in the Unix platform must be set to Yes.
D. A duplicate platform (Called) with the PSMP settings must be created.

**Answer:** A

**Explanation:**
To enable access over SSH to a Unix account through both Privileged Session Manager (PSM) and Privileged Session Manager Proxy (PSMP), the platform must contain the necessary connection components for both PSM-SSH and PSMP-
SSH. This ensures that the system can handle SSH connections through PSM for a native user experience and through PSMP for secure, transparent connections to remote systems12. References:
? CyberArk Docs: Connect through PSM for SSH1
? CyberArk Docs: Connect to Unix machines (using PSM for SSH)2

**NEW QUESTION 8**
Which command configures email alerts within PTA if settings need to be changed post install?

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

**Answer:** A

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

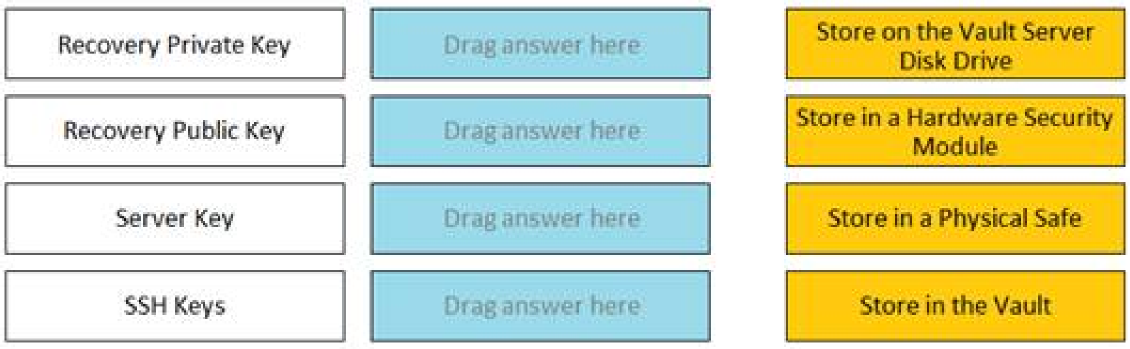
**NEW QUESTION 9**
You are onboarding 5,000 UNIX root accounts for rotation by the CPM. You discover that the CPM is unable to log in directly with the root account and will need to use a secondary account.
How should this be configured to allow for password management using least privilege?

A. Configure each CPM to use the correct logon account.
B. Configure each CPM to use the correct reconcile account.
C. Configure the UNIX platform to use the correct logon account.
D. Configure the UNIX platform to use the correct reconcile account.

**Answer:** C

**Explanation:**
When onboarding a large number of UNIX root accounts for password rotation by the Central Policy Manager (CPM), and the CPM cannot log in directly with the root account, it is necessary to configure the UNIX platform to use a secondary logon account that has the appropriate privileges. This secondary account should have the minimum necessary permissions to perform password management tasks, adhering to the principle of least privilege1. By configuring the UNIX platform with the correct logon account, the CPM can use this account to manage the root accounts securely and efficiently.
References:
? CyberArk's official documentation on Least Privileges and Privileged Access Manager provides guidance on configuring on-demand privileges for UNIX environments, which includes setting up the correct logon account for tasks that require elevated privileges1.
? Additional information on managing UNIX and Linux accounts, including the configuration of logon and reconcile accounts, can be found in the Unix plugin documentation for CyberArk

**NEW QUESTION 10**
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 10**
Which PTA sensors are required to detect suspected credential theft?

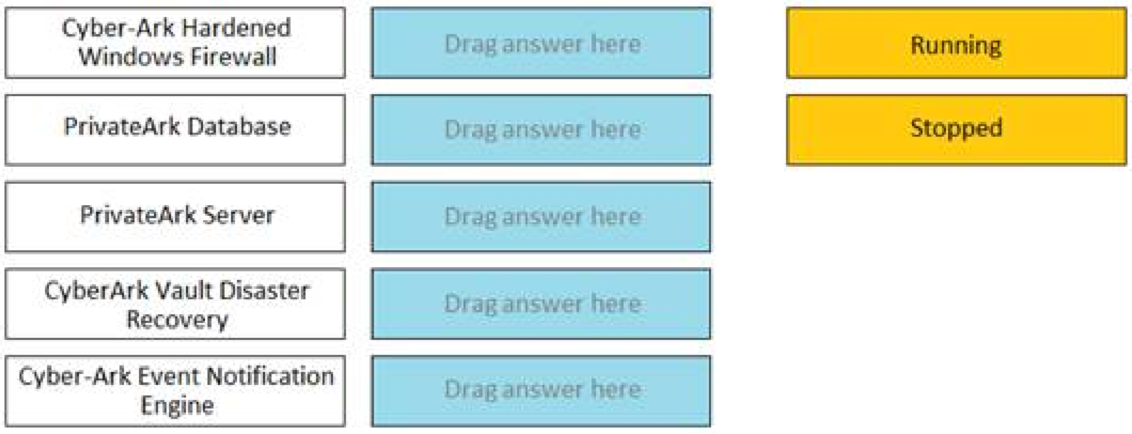
A. Logs, Vault Logs
B. Logs, Network Sensor, Vault Logs
C. Logs, PSM Logs, CPM Logs
D. Logs, Network Sensor, EPM

**Answer:** B

**Explanation:**
Suspected credential theft is a detection that PTA reports when a user connects to a machine or a cloud service without first retrieving the required credentials from the Vault. To detect this event, PTA requires the following sensors:
? Logs: This sensor collects log data from various sources, such as SIEM, Unix, AWS, and Azure, and forwards it to the PTA Server for analysis.

? Network Sensor: This sensor taps the network and collects network traffic data, which is used by the PTA Server to run deep packet inspection algorithms and detect cyber attacks, such as PAC, OverPass the Hash, and Golden Ticket.
? Vault Logs: This sensor collects log data from the Vault and forwards it to the PTA Server for analysis. The Vault logs contain information about the users' activities in the Vault, such as password retrieval, session initiation, and audit records.
References: What Detections Does PTA Report?, PTA Network Sensors

**NEW QUESTION 11**
DRAG DROP
Match the Status of Service on a DR Vault to what is displayed when it is operating normally in Replication mode.



| | | |
|---|---|---|
| Cyber-Ark Hardened Windows Firewall | Drag answer here | Running |
| PrivateArk Database | Drag answer here | Stopped |
| PrivateArk Server | Drag answer here | |
| CyberArk Vault Disaster Recovery | Drag answer here | |
| Cyber-Ark Event Notification Engine | Drag answer here | |

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 14**
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 17**
What is the purpose of the HeadStartInterval setting m a platform?

A. It determines how far in advance audit data is collected tor reports
B. It instructs the CPM to initiate the password change process X number of days before expiration.
C. It instructs the AIM Provider to 'skip the cache' during the defined time period
D. It alerts users of upcoming password changes x number of days before expiration.

**Answer:** B

**Explanation:**
The purpose of the HeadStartInterval setting in a platform is to instruct the CPM to initiate the password change process X number of days before expiration. This setting is used when the platform has the One Time Password feature enabled, which means that the passwords are changed every time they are retrieved by a user. The HeadStartInterval setting defines the number of days before the password expires (according to the ExpirationPeriod parameter) that the CPM will start the password change process. This gives the CPM enough time to change the password before it becomes invalid, and ensures that the user will always receive a

valid password when they request it1. The HeadStartInterval setting can be configured in the Platform Management settings for each platform that supports One Time Passwords. The default value is 0, which means that the CPM will start the password change process on the same day as the password expiration date1.
The other options are not the purpose of the HeadStartInterval setting in a platform:
? A. It determines how far in advance audit data is collected for reports. This option
is not related to the HeadStartInterval setting, which does not affect the audit data collection or reporting. The audit data is collected by the Vault server and stored in the Audit database, and the reports are generated by the PVWA or the PrivateArk Client based on the audit data2.
? C. It instructs the AIM Provider to ‘skip the cache’ during the defined time period.
This option is not related to the HeadStartInterval setting, which does not affect the AIM Provider or the cache mechanism. The AIM Provider is a component that enables applications to securely retrieve credentials from the Vault without requiring human intervention. The cache mechanism is a feature that allows the AIM Provider to store credentials locally for a limited time, in case of a temporary network failure or Vault unavailability3.
? D. It alerts users of upcoming password changes x number of days before
expiration. This option is not related to the HeadStartInterval setting, which does not alert users of anything. The HeadStartInterval setting only instructs the CPM to initiate the password change process, not to notify the users. The users do not need to be aware of the password changes, as they are performed automatically by the CPM and do not affect the user experience1. References:
? 1: Privileged Account Management, Min Validity Period subsection
? 2: Reports and Audits
? 3: Application Identity Manager

**NEW QUESTION 20**
To change the safe where recordings are kept for a specific platform, which setting must you update in the platform configuration?

A. SessionRecorderSafe Most Voted
B. SessionSafe
C. RecordingsPath
D. RecordingLocation

**Answer:** A

**Explanation:**
To change the safe where recordings are kept for a specific platform, you must update the SessionRecorderSafe setting in the platform configuration. This setting specifies the name of the safe where the Privileged Session Manager (PSM) recordings will be stored. After updating the SessionRecorderSafe setting, you need to restart the PSM service or wait for the new settings to be applied, which typically takes about 10 minutes. Once the new settings are in effect, any new PSM sessions initiated will have their recordings stored in the newly specified safe1.
References:
? CyberArk Docs - How to Create/Change/Configure PSM Recording Safes

**NEW QUESTION 24**
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 25**
PSM for Windows (previously known as “RDP Proxy”) supports connections to the following target systems

A. Windows
B. UNIX
C. Oracle
D. All of the above

**Answer:** D

**Explanation:**
PSM for Windows supports connections to various types of target systems, including Windows, UNIX, Oracle, and others. PSM for Windows uses different connection components to establish and manage the sessions, depending on the type and protocol of the target system. For example, PSM-RDP is used for Windows systems, PSM-SSH and PSM-Telnet are used for UNIX systems, PSM-Toad and PSM-SQLPlus are used for Oracle databases, and so on. References:
? PSM for Windows
? Connect through Privileged Session Manager for Windows
? Supported connection components

**NEW QUESTION 29**
In your organization the “click to connect” button is not active by default. How can this feature be activated?

A. Policies > Master Policy > Allow EPV transparent connections > Inactive

B. Policies > Master Policy > Session Management > Require privileged session monitoring and isolation > Add Exception
C. Policies > Master Policy > Allow EPV transparent connections > Active
D. Policies > Master Policy > Password Management

**Answer:** C

**Explanation:**
The “click to connect” button is a feature that allows users to connect to target systems without entering their credentials manually. It is also known as EPV transparent connections or PSM transparent connections. To activate this feature, you need to enable the Allow EPV transparent connections parameter in the Master Policy. This parameter determines whether users can use the “click to connect” button to initiate a privileged session from the PVWA. If the parameter is set to Active, the button is enabled and users can connect to target systems with one click. If the parameter is set to Inactive, the button is disabled and users need to copy the credentials and paste them in the target system login screen. References: Connect and configure - CyberArk, How to enable/disable Connect button in PVWA console - force.com

**NEW QUESTION 30**
An auditor initiates a live monitoring session to PSM server to view an ongoing live session. When the auditor’s machine makes an RDP connection the PSM server, which user will be used?

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

**Answer:** A

**Explanation:**
According to the web search results, when an auditor initiates a live monitoring session to PSM server to view an ongoing live session, the auditor’s machine makes an RDP connection to the PSM server using the PSMAdminConnect user. The PSMAdminConnect user is a local or domain user that starts PSM sessions on the PSM machine for authorized users who want to monitor or terminate active sessions1. The PSMAdminConnect user has limited permissions and access rights on the PSM server, and its credentials are managed by the CPM. The PSMAdminConnect user retrieves the credentials of the target account from the vault and uses them to establish a secure connection to the target machine. The auditor can then view the live session through the PSM session, while the PSM server records and audits the session activity.

**NEW QUESTION 32**
What is the maximum number of levels of authorization you can set up in Dual Control?

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

**Answer:** B

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

**NEW QUESTION 36**
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 39**
PSM captures a record of each command that was executed in Unix.

A. TRIE
B. FALSE

**Answer:** A

**Explanation:**
PSM captures a record of each command that was executed in Unix by using the SSH text recorder. This is a feature that enables PSM to record all the keystrokes that are typed during privileged sessions on SSH connections, including Unix systems. The SSH text recorder can be configured in the Platform Management settings for each platform that uses the SSH protocol. The text recordings are stored and protected in the Vault server and are accessible to authorized auditors. The text recordings can also be used for auditing and compliance purposes, as they provide a detailed trace of the actions performed by the users on the target systems1. References:
? 1: Introduction to PSM for SSH, How it works subsection, Text recordings paragraph

**NEW QUESTION 43**
If PTA is integrated with a supported SIEM solution, which detection becomes available?

A. unmanaged privileged account
B. privileged access to the Vault during irregular days
C. riskySPN
D. exposed credentials

**Answer:** D

**Explanation:**
When Privileged Threat Analytics (PTA) is integrated with a supported Security Information and Event Management (SIEM) solution, the detection of exposed credentials becomes available. This integration allows PTA to detect when a user is connected to a machine with a privileged account without first retrieving the credential from the CyberArk Digital Vault. In such cases, PTA can prompt an immediate credential rotation and send an alert to the SIEM, indicating a suspected credential theft1.
References:
? CyberArk Docs - SIEM Integration2
? CyberArk Blog - Integrate CyberArk with a SIEM Solution1

**NEW QUESTION 46**
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 51**
Your organization has a requirement to allow users to "check out passwords" and connect to targets with the same account through the PSM.
What needs to be configured in the Master policy to ensure this will happen?

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

**Answer:** A

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

**NEW QUESTION 53**
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 55**
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 56**
A Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control.

A. True
B. False

**Answer:** A

**Explanation:**
According to the web search results, a Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control. SMTP is a protocol that enables the sending and receiving of email messages. By integrating SMTP with CyberArk Defender PAM, the Event Notification Engine (ENE) can automatically send email notifications about PAM activities to predefined users1. For example, the ENE can notify users about password requests, password confirmations, password changes, password verifications, password reconciliations, password access, password usage, password expiration, and password violations1. The ENE can also notify users about system events, such as Vault backup, Vault restore, Vault shutdown, Vault startup, and Vault license expiration1. These notifications help to monitor the Vault activity and ensure compliance with the security policies.
SMTP integration is also essential for facilitating workflow processes, such as Dual Control. Dual Control is a feature that enables authorized Safe owners to either grant or deny requests to access accounts. This feature adds an additional measure of protection, in that it enables you to see who wants to access the information in the Safe, when, and for what purpose. The Master Policy enables organizations to ensure that passwords can only be retrieved after permission or 'confirmation' has been granted from an authorized Safe Owner(s). This is known as Dual Control2. SMTP integration enables the ENE to send email notifications to the requesters and the confirmers about the status of the password requests. The ENE can also send reminders to the confirmers if they have not responded to the requests within a specified time period2. These notifications help to streamline the workflow process and ensure timely and secure access to the accounts.
References:
? Email notifications - CyberArk
? Dual Control - CyberArk

**NEW QUESTION 60**
Where can you check that the LDAP binding is using TCP/636?

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

**Answer:** D

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

**NEW QUESTION 65**
Which of the following components can be used to create a tape backup of the Vault?

A. Disaster Recovery
B. Distributed Vaults
C. Replicate
D. High Availability

**Answer:** C

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

**NEW QUESTION 66**
Your organization requires all passwords be rotated every 90 days. Where can you set this regulatory requirement?

A. Master Policy
B. Safe Templates
C. PVWAConfig.xml
D. Platform Configuration

**Answer:** D

**Explanation:**
The platform configuration defines the password management settings for each type of account, such as the password complexity, rotation frequency, verification method, and reconciliation options. You can set the regulatory requirement for password rotation in the platform configuration by specifying the number of days in the Password Change Interval parameter. This parameter determines how often the CPM will change the passwords of the accounts that are associated with the platform. For example, if you set the Password Change Interval to 90, the CPM will change the passwords every 90 days. References: Credentials Rotation - CyberArk, How do I manage or change passwords stored in CyberArk?

**NEW QUESTION 71**
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 73**
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 75**
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 76**
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 79**
Within the Vault each password is encrypted by:

A. the server key
B. the recovery public key
C. the recovery private key
D. its own unique key

**Answer:** D

**Explanation:**
According to the web search results, within the Vault each password is encrypted by its own unique key. This key is generated by the Vault when the password is added to the Vault and is stored in the Vault's database. The password key is encrypted by the safe key, which is the key of the safe that contains the password. The safe key is encrypted by the server key, which is the key that opens the Vault. The server key is encrypted by the public recovery key, which is part of the asymmetric recovery key that enables the Master User to log on to the Vault in case of a disaster. This layered encryption scheme ensures that each password is protected by multiple keys and that no single key can compromise the security of the Vault

**NEW QUESTION 81**
Which built-in report from the reports page in PVWA displays the number of days until a password is due to expire?

A. Privileged Accounts Inventory
B. Privileged Accounts Compliance Status
C. Activity Log
D. Privileged Accounts CPM Status

**Answer:** A

**Explanation:**
ThePrivileged Accounts Inventory report in PVWA includes a column that displays the Age of the password, which indicates the number of days since the password was created1. This information can be used to determine how many days are left until a password is due to expire, based on the password policy's expiration settings.
References:
? CyberArk's official documentation on PVWA reports provides a list of available reports and their descriptions, including the Privileged Accounts Inventory report which contains details about password age and other relevant information1.

**NEW QUESTION 84**
What is the chief benefit of PSM?

A. Privileged session isolation
B. Automatic password management
C. Privileged session recording
D. 'Privileged session isolation' and 'Privileged session recording'

**Answer:** D

**Explanation:**
According to the web search results, the chief benefit of PSM is to provide both privileged session isolation and privileged session recording. Privileged session isolation means that the PSM server acts as a proxy between the user and the target machine, preventing the user from directly accessing the target machine or

exposing the privileged account credentials. Privileged session recording means that the PSM server captures and stores a video and a transcript of the user's activity on the target machine, enabling auditing and monitoring of the privileged session. These benefits help to enhance the security and compliance of the privileged access management solution, as they prevent credential exposure, restrict unauthorized access, detect malicious activity, and provide evidence for forensic analysis

**NEW QUESTION 88**
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 89**
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 92**
By default, members of which built-in groups will be able to view and configure Automatic Remediation and Session Analysis and Response in the PVWA?

A. Vault Admins
B. Security Admins
C. Security Operators
D. Auditors

**Answer:** B

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

**NEW QUESTION 95**
When managing SSH keys, the CPM stores the Public Key

A. In the Vault
B. On the target server
C. A & B
D. Nowhere because the public key can always be generated from the private key.

**Answer:** B

**Explanation:**
When managing SSH keys, the CPM stores the public key on the target server. The CPM generates a new random SSH key pair and updates the public SSH key on the target machine. The public SSH key is stored in the home directory of the privileged user on the target machine, usually in the file ~/.ssh/authorized_keys. The public SSH key is not stored in the Vault, as this would be redundant and unnecessary. The public SSH key cannot be generated from the private key, as this would defeat the purpose of asymmetric encryption. References:

? Manage SSH Keys
? SSH Key Manager
? Use SSH Keys

**NEW QUESTION 98**
You received a notification from one of your CyberArk auditors that they are missing Vault level audit permissions. You confirmed that all auditors are missing the Audit Users Vault permission.
Where do you update this permission for all auditors?

A. Private Ark Client > Tools > Administrative Tools > Directory Mapping > Vault Authorizations
B. Private Ark Client > Tools > Administrative Tools > Users and Groups > Auditors > Authorizations tab
C. PVWA User Provisioning > LDAP integration > Vault Auditors Mapping > Vault Authorizations
D. PVWA> Administration > Configuration Options > LDAP integration > Vault Auditors Mapping > Vault Authorizations

**Answer:** B

**Explanation:**
To update the Vault level audit permissions for all auditors, you would use the Private Ark Client. Specifically, you would navigate to the Tools menu, select Administrative Tools, then Users and Groups. Within the Users and Groups section, you would select the Auditors group and go to theAuthorizations tab. Here, you can manage and update the permissions for the Auditor group, including the Audit Users Vault permission. This ensures that all members of the Auditors group have the necessary permissions to perform their audit functions within the Vault1.
References:
? CyberArk's official documentation on predefined users and groups, which includes information on the Auditor user and the permissions associated with this role1.
? Information on the administrative tools available in the Private Ark Client, which are used for managing users and groups, including auditors2.

**NEW QUESTION 101**
dbparm.ini is the main configuration file for the Vault.

A. True
B. False

**Answer:** B

**Explanation:**
dbparm.ini is not the main configuration file for the Vault. It is one of the several configuration files that control the initial settings and method of operation of the Server. The main configuration file for the Vault is DBParm.ini, which contains the general parameters of the database, such as the Vault name, the Vault IP address, the Vault port, the encryption algorithm, the log retention, and the debug mode1. References:
? DBParm.ini - CyberArk, section "Main parameters"

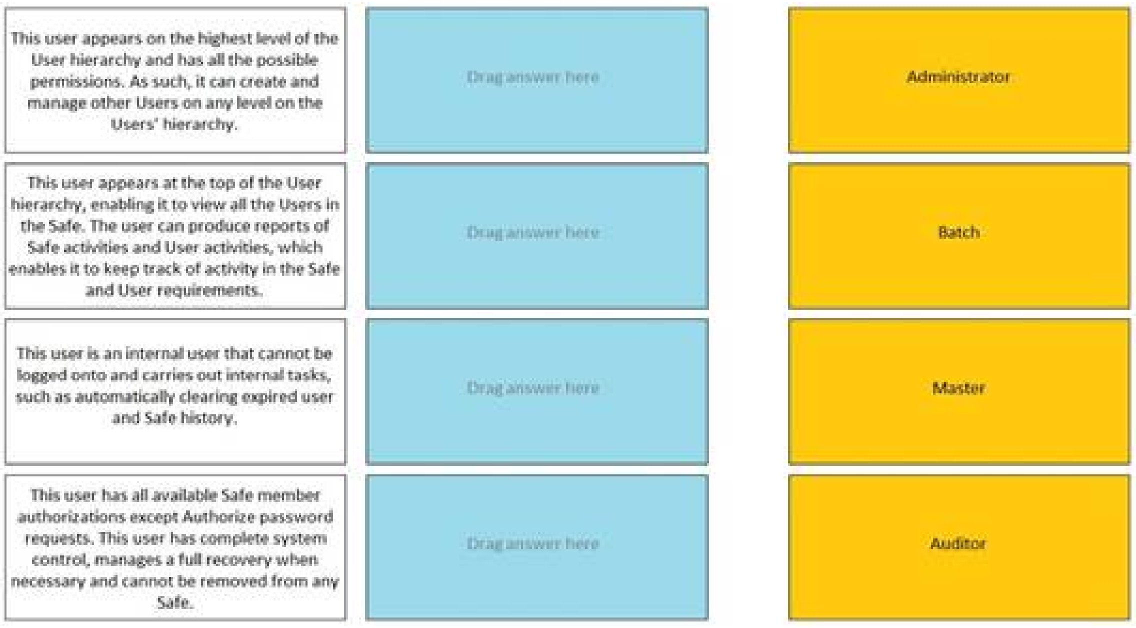
**NEW QUESTION 106**
The Password upload utility can be used to create safes.

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 111**
DRAG DROP
Match the built-in Vault User with the correct definition.

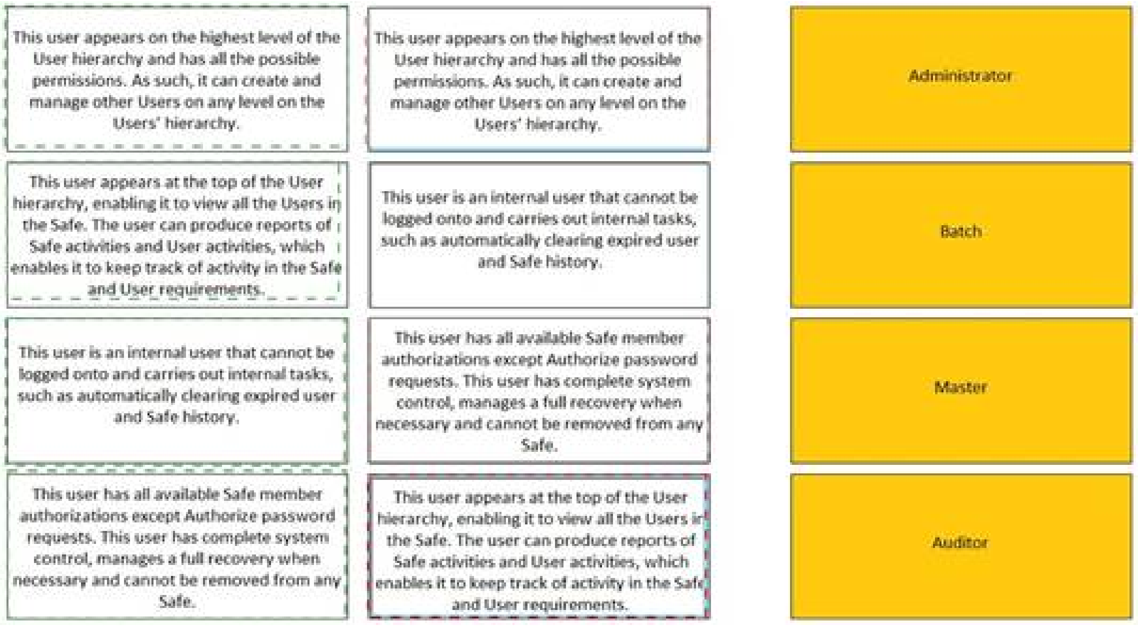


| | | |
|---|---|---|
| This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy. | Drag answer here | Administrator |
| This user appears at the top of the User hierarchy, enabling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

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**



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

**NEW QUESTION 114**
Which of the following PTA detections require the deployment of a Network Sensor or installing the PTA Agent on the domain controller?

A. Suspected credential theft
B. Over-Pass-The-Hash
C. Golden Ticket
D. Unmanaged privileged access

**Answer:** C

**Explanation:**
According to the CyberArk Defender PAM documentation1, the PTA detection that requires the deployment of a Network Sensor or installing the PTA Agent on the domain controller is Golden Ticket. A Golden Ticket is a type of attack that involves creating a forged Kerberos Ticket Granting Ticket (TGT) that grants the attacker access to any resource in the domain. The attacker needs to compromise the domain controller and steal the KRBTGT account password hash to create the Golden Ticket. The PTA Network Sensor or the PTA Agent can detect this attack by analyzing the network traffic and identifying anomalies in the Kerberos protocol, such as TGTs with abnormal lifetime, encryption type, or renewal time. The PTA Server then alerts the security team and provides details about the attack, such as the source IP, the target domain, and the ticket properties. References:
? PTA Network Sensors - CyberArk

**NEW QUESTION 118**
Users are unable to launch Web Type Connection components from the PSM server. Your manager asked you to open the case with CyberArk Support.
Which logs will help the CyberArk Support Team debug the issue? (Choose three.)

A. PSMConsole.log
B. PSMDebug.log
C. PSMTrace.log
D. <Session_ID>.Component.log
E. PMconsole.log
F. ITAlog.log

**Answer:** ACD

**Explanation:**
When users are unable to launch Web Type Connection components from the PSM server, the CyberArk Support Team will require specific logs to debug the issue. The logs that are typically helpful in such cases include:
? PSMConsole.log: This log file contains informational messages and errors related to the PSM function, which can help identify issues with the PSM server's operation1.
? PSMTrace.log: This log file includes errors and trace messages, which can provide detailed insights into the issues occurring during the PSM server's processes1.
? <Session_ID>.Component.log: This log file contains errors and trace messages related to the connection component, which can be crucial for troubleshooting issues with launching Web Type Connection components1.
These logs can provide the necessary information to understand the problem and assist the support team in resolving the issue effectively.
References:
? CyberArk's official documentation on PSM for Web Troubleshooting, which outlines the types of logs available and their purposes in the troubleshooting process1.
? Additional resources on managing and interpreting PSM logs, which provide guidance on using logs for diagnosing and resolving issues with the PSM server2

**NEW QUESTION 121**
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 122**
You notice an authentication failure entry for the DR user in the ITALog. What is the correct process to fix this error? (Choose two.)

A. PrivateArk Client > Tools > Administrative Tools > Users and Groups > DR User > Update > Authentication > Update Password.
B. Create a new credential file, on the DR Vault, using the CreateCredFile utility and the newly set password.
C. Create a new credential file, on the Primary Vault, using the CreateCredFile utility and the newly set password.
D. PVWA > User Provisioning > Users and Groups > DR User > Update Password.
E. PrivateArk Client > Tools > Administrative Tools > Users and Groups > PAReplicate User > Update > Authentication > Update Password.

**Answer:** AB

**Explanation:**
When an authentication failure for the DR user is noticed in the ITALog, the correct process to fix this error involves two steps. First, you need to update the password for the DR user. This is done through the PrivateArk Client by navigating to Tools > Administrative Tools > Users and Groups > DR User > Update > Authentication > Update Password. After updating the password, the next step is to create a new credential file on the DR Vault using the CreateCredFile utility with the newly set password. This ensures that the DR Vault has the updated credentials necessary for the DR user to authenticate successfully12.
References:
? CyberArk's official documentation on troubleshooting authentication issues, which includes steps on updating user passwords and creating new credential files1.
? Community discussions and support articles on resolving DR user authentication failures, which provide practical insights and recommended actions2

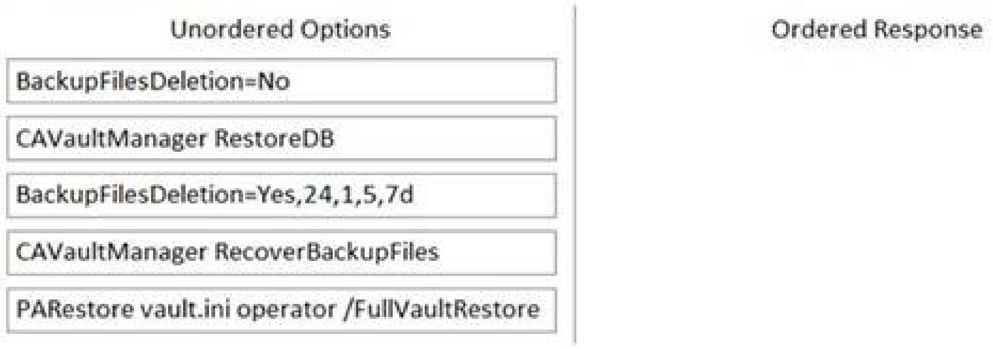
**NEW QUESTION 125**
When Dual Control is enabled a user must first submit a request in the Password Vault Web Access (PVWA) and receive approval before being able to launch a secure connection via PSM for Windows (previously known as RDP Proxy).

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 126**
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 129**
What must you specify when configuring a discovery scan for UNIX? (Choose two.)

A. Vault Administrator
B. CPM Scanner
C. root password for each machine
D. list of machines to scan
E. safe for discovered accounts

**Answer:** BD

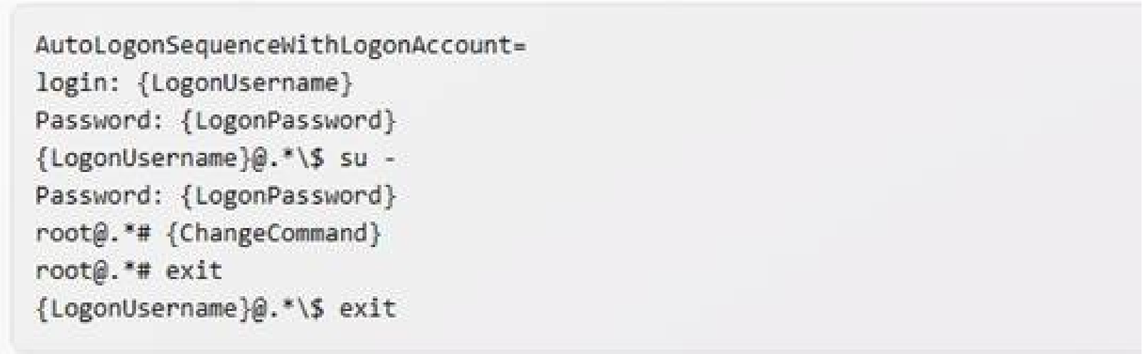
**Explanation:**
When configuring a discovery scan for UNIX, you must specify theCPM Scanner and thelist of machines to scan. The CPM Scanner is the component responsible for executing the discovery process, and it requires a list of target machines to scan for new and modified accounts and their dependencies. This list can be provided in the form of a CSV file for UNIX machines1. The discovery process will then scan the predefined machines to identify privileged accounts that should be onboarded into the Vault for secure and automated management according to enterprise compliance policies2. References:
? CyberArk Docs - Manage discovery processes1
? CyberArk Docs - Scan for accounts using Account Discovery

**NEW QUESTION 133**
You have associated a logon account to one your UNIX cool accounts in the vault. When attempting to [b]change [/b] the root account’s password the CPM will…..

A. Log in to the system as root, then change root's password
B. Log in to the system as the logon account, then change roofs password
C. Log in to the system as the logon account, run the su command to log in as root, and then change root’s password.
D. None of these

**Answer:** C

**Explanation:**
When attempting to change the root account’s password, the CPM will log in to the system as the logon account, run the su command to log in as root, and then change root’s password. This is because the logon account is used to initiate sessions to machines that do not permit direct logon, such as Unix systems that restrict root access. When a logon account is associated with a privileged account, it will be used to log onto the remote machine and then elevate itself to the role of the privileged user. As different types of machines might have different logon prompts or elevation commands, the CPM can use the AutoLogonSequenceWithLogonAccount parameter to define the logon process and the elevation to the privileged account. This parameter contains regular expression prompts and responses that define the logon process and subsequent activities. The regular expressions can include dynamic values that the CPM reads from the account properties, user parameters, or client-specific parameters1. For example, the following is a possible AutoLogonSequenceWithLogonAccount parameter for a Unix platform:



```
AutoLogonSequenceWithLogonAccount=
login: {LogonUsername}
Password: {LogonPassword}
{LogonUsername}@.*\$ su -
Password: {LogonPassword}
root@.*# {ChangeCommand}
root@.*# exit
{LogonUsername}@.*\$ exit
```

This parameter instructs the CPM to log in to the system as the logon account, enter the logon password, run the su - command to switch to the root user, enter the logon password again, run the change command to change the root password, exit the root session, and exit the logon session1.
The other options are not correct, as follows:
? A. Log in to the system as root, then change root’s password. This option is not possible, because the root account cannot be used for direct logon. The logon account is associated with the root account to enable the CPM to access the system and change the password1.
? B. Log in to the system as the logon account, then change root’s password. This option is not effective, because the logon account does not have the permission to change the root’s password. The logon account needs to elevate itself to the root user by using the su command before changing the password1.
? D. None of these. This option is not valid, because there is a correct answer among the choices.
References:
? 1: Logon Accounts for SSH and Telnet Connections

**NEW QUESTION 134**
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 137**
......