CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM

NEW QUESTION 1
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 2
Which Automatic Remediation is configurable for a PTA detection of a “Suspected Credential Theft”?

A. Add to Pending
B. Rotate Credentials
C. Reconcile Credentials
D. Disable Account

Answer: B

Explanation:
For a Privileged Threat Analytics (PTA) detection of a “Suspected Credential Theft,” the automatic remediation that can be configured is Rotate Credentials. This remediation action is designed to automatically initiate password changes when PTA identifies a suspected credential threat, such as a credential theft event. By rotating the credentials, CyberArk ensures that the potentially compromised credentials are changed, thus mitigating the risk of unauthorized access1.
References:
? CyberArk’s official documentation on configuring PTA remediations, which includes information on automatic password rotation for suspected credential threats2.
? Additional details on the remediation actions that can be configured for different types of PTA detections, including Suspected Credential Theft1.

NEW QUESTION 3
Which of the Following can be configured in the Master Poky? Choose all that apply.

A. Dual Control
B. One Time Passwords
C. Exclusive Passwords
D. Password Reconciliation
E. Ticketing Integration
F. Required Properties
G. Custom Connection Components
H. Password Aging Rules

Answer: ABCH

Explanation:
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. The Master Policy includes the following main concepts1:
? Basic policy rules: These rules allow the administrator to define specific aspects of privileged account management, such as privileged access workflows, password management, session monitoring and auditing.
? Advanced policy rules: Some basic policy rules have related advanced settings that provide more granular control over the policy enforcement.
? Exceptions: These are policy rules that differ from the overall Master Policy for a specific scope of accounts, such as accounts associated with a specific platform.
The Master Policy rules are divided into four sections2:
? Privileged Access Workflows: These rules define how the organization manages access to privileged accounts, such as requiring dual control, one-time passwords, exclusive passwords, transparent connections, reason for access, etc.
? Password Management: These rules determine how passwords are managed, such as requiring password change, password verification, password reconciliation, ticketing integration, required properties, custom connection components, etc.
? Session Management: These rules determine whether or not privileged sessions are recorded and how they are monitored, such as requiring session isolation, session recording, session audit, etc.
? Audit: This rule determines how Safe audits are retained, such as specifying the audit retention period.
Based on the above information, the following options can be configured in the Master Policy:
? A. Dual Control: This is a basic policy rule in the Privileged Access Workflows
section that determines whether users need to get approval from authorized users before accessing a privileged account2.
? B. One Time Passwords: This is a basic policy rule in the Privileged Access
Workflows section that determines whether users can only use a password once before it is changed2.
? C. Exclusive Passwords: This is a basic policy rule in the Privileged Access
Workflows section that determines whether users need to check out a password and prevent other users from accessing it until it is checked in2.
? H. Password Aging Rules: This is a basic policy rule in the Password Management
section that determines how often passwords need to be changed2. The following options cannot be configured in the Master Policy:
? D. Password Reconciliation: This is not a policy rule, but 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 sync3.
? E. Ticketing Integration: This is not a policy rule, but a feature that enables the

integration of the Vault with external ticketing systems, such as ServiceNow, Jira, etc.
? F. Required Properties: This is not a policy rule, but a platform setting that determines which properties are mandatory for adding accounts to a platform.
? G. Custom Connection Components: This is not a policy rule, but a platform setting that determines which connection components are used to connect to target systems, such as PVWA, PSM, PSMP, etc.
References:
? 1: The Master Policy
? 2: Master Policy Rules
? 3: Password Reconciliation
? : Ticketing Integration
? : Required Properties
? : Custom Connection Components

NEW QUESTION 4
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.

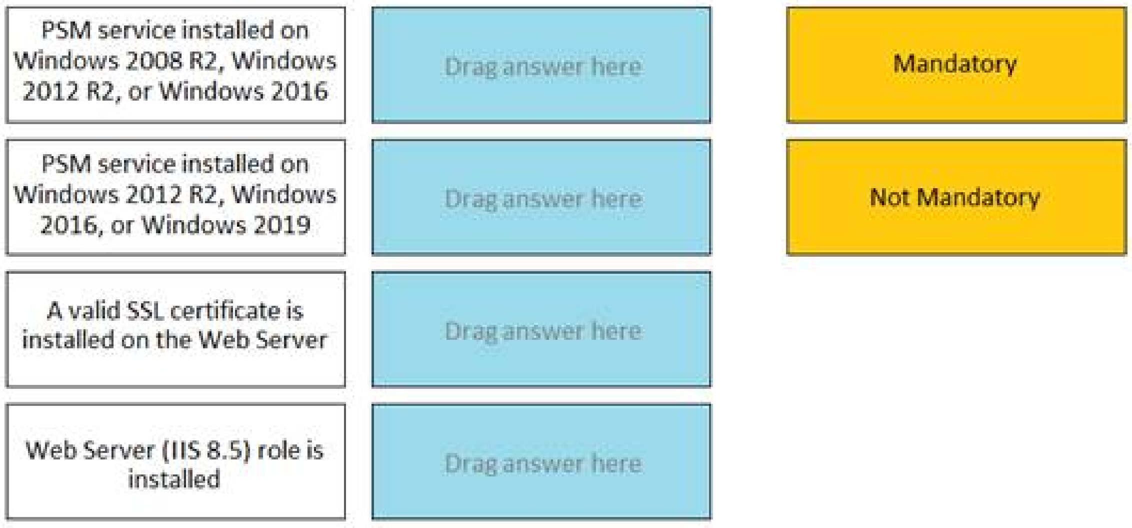
NEW QUESTION 5
Which of the following Privileged Session Management (PSM) solutions support live monitoring of active sessions?

A. PSM (i.e., launching connections by clicking on the connect button in the Password Vault Web Access (PVWA)
B. PSM for Windows (previously known as RDP Proxy)
C. PSM for SSH (previously known as PSM-SSH Proxy)
D. All of the above

Answer: D

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

NEW QUESTION 6
DRAG DROP
For each listed prerequisite, identify if it is mandatory or not mandatory to run the PSM Health Check.



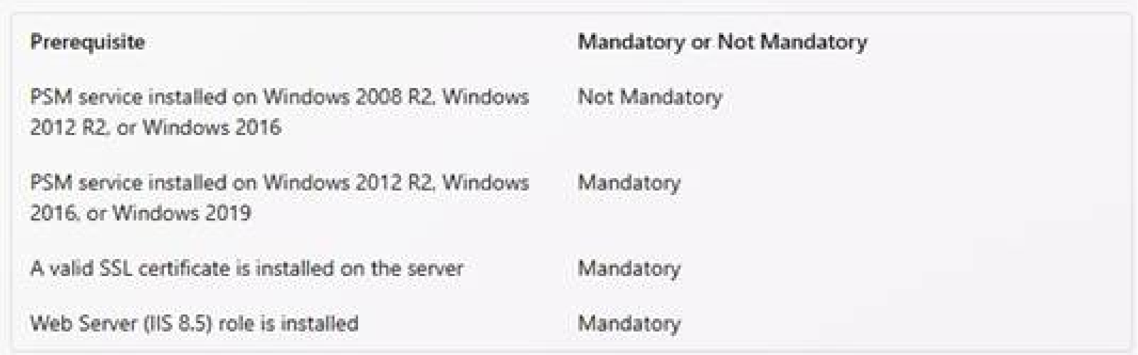
PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016	Drag answer here	Mandatory
PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019	Drag answer here	Not Mandatory
A valid SSL certificate is installed on the Web Server	Drag answer here	
Web Server (IIS 8.5) role 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 7
A new domain controller has been added to your domain. You need to ensure the CyberArk infrastructure can use the new domain controller for authentication. Which locations must you update?

A. on the Vault server in Windows\System32\Etc\Hosts and in the PVWA Application under Administration > LDAP Integration > Directories > Hosts
B. on the Vault server in Windows\System32\Etc\Hosts and on the PVWA server in Windows\System32\Etc\Hosts
C. in the Private Ark client under Tools > Administrative Tools > Directory Mapping
D. on the Vault server in the certificate store and on the PVWA server in the certificate store

Answer: A

Explanation:
When a new domain controller is added to a domain, it is necessary to update the CyberArk infrastructure to ensure it can use the new domain controller for authentication. This involves updating the hosts file on theVault server located
at Windows\System32\Etc\Hosts to include the new domain controller's details. Additionally, within the PVWA Application, you need to navigate to Administration > LDAP Integration > Directories > Hosts and update the information there as well. This ensures that both the Vault server and the PVWA Application are aware of the new domain controller and can authenticate against it1.
References:
? CyberArk's official documentation on configuring Active Directory integration, which includes details on setting up domain controllers for authentication2.
? Information on adding Active Directory as a directory service in CyberArk Identity, which discusses the integration of domain controllers3.

NEW QUESTION 8
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 9
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 10
A new HTML5 Gateway has been deployed in your organization. Where do you configure the PSM to use the HTML5 Gateway?

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

D. Administration > Options > Privileged Session Management > Configured PSM Servers> Connection Details

Answer: C

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

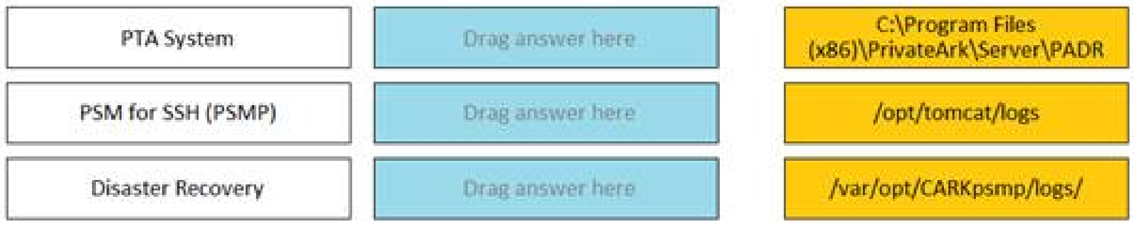
NEW QUESTION 10
Which of the following logs contains information about errors related to PTA?

A. ITAlog.log
B. diamond.log
C. pm_error.log
D. WebApplication.log

Answer: B

Explanation:
According to the web search results, the diamond.log is the main log file that records the PTA system activities, such as receiving and processing events, generating alerts, and sending notifications1. The diamond.log also contains information about errors related to PTA, such as connection failures, configuration issues, parsing problems, or internal exceptions2. The diamond.log can be found in the /opt/tomcat/logs directory on the PTA machine1. The debug level of the diamond.log can be changed using the changeLogLevel.sh utility or manually editing the log4j.properties file1. The diamond.log can be used for troubleshooting PTA issues and viewing statistics

NEW QUESTION 11
DRAG DROP
Match each component to its respective Log File location.

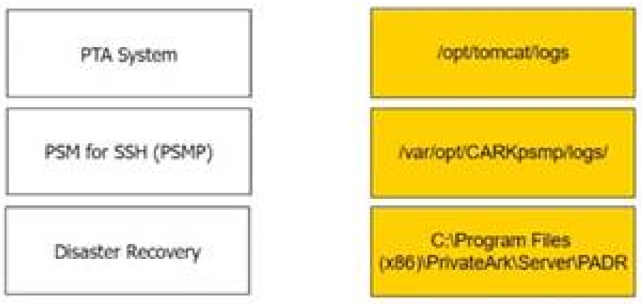


PTA System	Drag answer here	C:\Program Files (x86)\PrivateArk\Server\PADR
PSM for SSH (PSMP)	Drag answer here	/opt/tomcat/logs
Disaster Recovery	Drag answer here	/var/opt/CARKpsmp/logs/

A. Mastered
B. Not Mastered

Answer: A

Explanation:



PTA System	/opt/tomcat/logs
PSM for SSH (PSMP)	/var/opt/CARKpsmp/logs/
Disaster Recovery	C:\Program Files (x86)\PrivateArk\Server\PADR

Comprehensive explanation: The log file locations for each component in CyberArk's Privileged Access Management (PAM) are specific to the function and operation of that component. The PTA System logs are typically found in the PrivateArk Server directory, specifically in the PADR folder. The PSM for SSH, which is the Privileged Session Manager for SSH, stores its logs in the tomcat logs directory. Lastly, the logs for Disaster Recovery operations are located in the CARKsymop logs directory on a Linux-based system. References: The information is based on the CyberArk documentation and best practices for managing and maintaining log files for different components within the PAM solution123. The log file locations are essential for troubleshooting and auditing purposes, ensuring that all activities and changes are properly recorded and can be reviewed when necessary.

NEW QUESTION 14
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 19
Which Cyber Are components or products can be used to discover Windows Services or Scheduled Tasks that use privileged accounts? Select all that apply.

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

Answer: ABE

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

NEW QUESTION 20
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 22
As long as you are a member of the Vault Admins group you can grant any permission on any safe.

A. TRUE
B. FALSE

Answer: B

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

NEW QUESTION 27
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 32
To use PSM connections while in the PVWA, what are the minimum safe permissions a user or group will need?

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

Answer: B

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

NEW QUESTION 36
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 37
Which of the following Privileged Session Management solutions provide a detailed audit log of session activities?

A. PSM (i.e., launching connections by clicking on the "Connect" button in the PVWA)
B. PSM for Windows (previously known as RDP Proxy)
C. PSM for SSH (previously known as PSM SSH Proxy)
D. All of the above

Answer: D

Explanation:
All of the Privileged Session Management solutions provide a detailed audit log of session activities. PSM, PSM for Windows, and PSM for SSH enable organizations to secure, control and monitor privileged access to network devices by using Vaulting technology to manage privileged accounts and create detailed session audits and video recordings of all IT administrator privileged sessions on remote machines1. PSM also provides additional audit features such as SQL Command Level Audit, Windows Events Audit, and Universal Keystrokes Audit1. PSM for Web captures a detailed transcript of cloud application user activity to enable a security manager or auditor the ability to monitor sessions for suspicious or restricted operations2. References:
? Monitor Privileged Sessions - CyberArk
? Privileged Session Manager for Web - CyberArk

NEW QUESTION 41
Target account platforms can be restricted to accounts that are stored m specific Safes using the Allowed Safes property.

A. TRUE
B. FALSE

Answer: A

Explanation:
Target account platforms can be restricted to accounts that are stored in specific Safes using the Allowed Safes property. This property is a parameter that can be configured in the Platform Management settings for each platform. The Allowed Safes property specifies the name or names of the Safes where the platform can be applied. The default value is .*, which means that the platform can be used in any Safe. However, if you want to limit the platform to certain Safes, you can enter the name or names of the Safes, separated by a pipe (|) character. For example, if you want to restrict the platform to Safes called WindowsPasswords and LinuxPasswords, you can enter AllowedSafes=(WindowsPasswords)|(LinuxPasswords). This feature is useful for preventing unauthorized users from accessing passwords, especially if you implement the reconciliation functionality. It also helps the CPM to focus its search operations on specific Safes, instead of scanning all Safes it can see in the Vault1. References:
? 1: Limit Platforms to Specific Safes

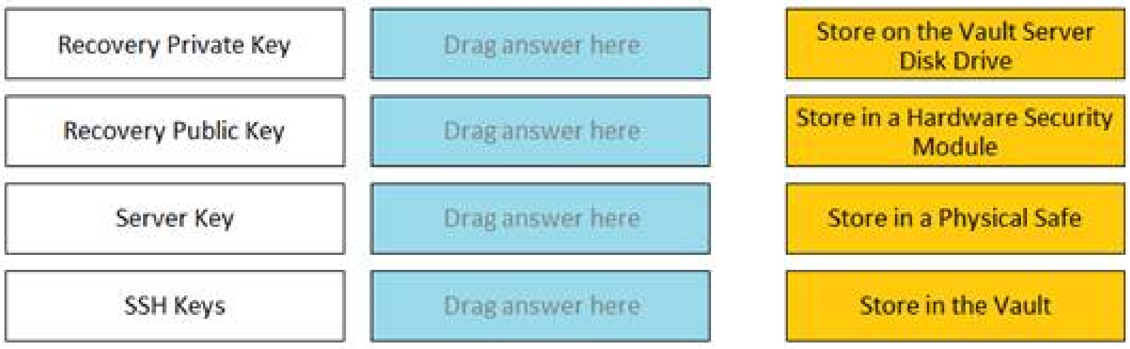
NEW QUESTION 46
A user has successfully conducted a short PSM session and logged off. However, the user cannot access the Monitoring tab to view the recordings.
What is the issue?

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 51
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 52
It is possible to restrict the time of day, or day of week that a [b]verify[/b] process can occur

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 57
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 58
When a DR Vault Server becomes an active vault, it will automatically fail back to the original state once the Primary Vault comes back online.

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

Answer: C

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

NEW QUESTION 60
To ensure all sessions are being recorded, a CyberArk administrator goes to the master policy and makes configuration changes.
Which configuration is correct?

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

Answer: C

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

NEW QUESTION 63
Which user(s) can access all passwords in the Vault?

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

Answer: D

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

they are explicitly added as a member of a Safe that contains the passwords2.
The auditors group is a predefined group that is created during the initial installation of the Vault and has the Audit Users authorization. The members of the auditors group can view
and generate reports on the Vault activity, but they cannot access any passwords in the Vault unless they are explicitly added as a member of a Safe that contains the passwords2. References:
? Master User - CyberArk
? Predefined users and groups - CyberArk

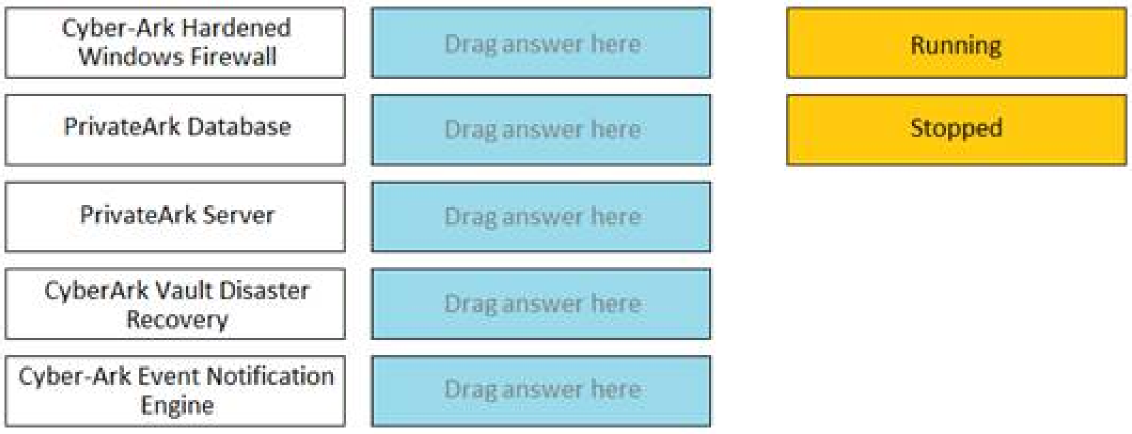
NEW QUESTION 68
How much disk space do you need on a server to run a full replication with PAReplicate?

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

Answer: D

Explanation:
When running a full replication with PAReplicate, it is essential to have at least the same amount of disk space on the server as the disk size of the Primary Vault. This ensures that there is sufficient space to replicate all the data from the Primary Vault without any issues. The disk space should be equal to or larger than the total size of the data being replicated to accommodate the full backup1.
References:
? CyberArk Docs: Install the Vault Backup Utility

NEW QUESTION 69
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 73
When a DR Vault Server becomes an active vault, it will automatically revert back to DR mode once the Primary Vault comes back online.

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

Answer: B

Explanation:
According to the web search results, when a DR Vault Server becomes an active vault, it will not automatically revert back to DR mode once the Primary Vault comes back online. The Vault administrator must manually set the DR Vault to DR mode by setting “FailoverMode=no” in the padr.ini file1. This file is located in the /opt/CARKaim/conf directory on the DR Vault machine2. The Vault administrator must also stop the replication process on the DR Vault and restart the

PrivateArk Server service1. This procedure is known as a DR failback, which restores the original roles of the Primary Vault and the DR Vault after a failover1. The AllowFailback setting in the padr.ini file does not affect the DR failback process, as it only determines whether the DR Vault can be used as a backup for another DR Vault in a cascading DR scenario3. The dbparm.ini file is not relevant for the DR failback process, as it contains the database parameters for the Vault server.
References:
? Initiate a DR failback to the Production Vault - CyberArk
? Install the Disaster Recovery application - CyberArk
? Cascading DR - CyberArk
? [dbparm.ini file - CyberArk]

NEW QUESTION 77
Which combination of Safe member permissions will allow end users to log in to a remote machine transparently but NOT show or copy the password?

A. Use Accounts, Retrieve Accounts, List Accounts
B. Use Accounts, List Accounts
C. Use Accounts
D. List Accounts, Retrieve Accounts

Answer: B

Explanation:
The Use Accounts permission enables Safe members to log in to a remote machine through a PSM connection from the Accounts List or the Account Details page. The List Accounts permission enables Safe members to view the Accounts list. However, to show or copy the password, the Safe members also need the Retrieve Accounts permission, which allows them to view and copy the account value in the Account Details
page or the Accounts list. Therefore, the combination of Use Accounts and List Accounts will allow end users to log in to a remote machine transparently but not show or copy the password. References:
? Safe Members - CyberArk1, section “Permissions”
? Safes and Safe members - CyberArk2, section “Safe members overview”

NEW QUESTION 79
CyberArk implements license limits by controlling the number and types of users that can be provisioned in the vault.

A. TRUE
B. FALSE

Answer: B

Explanation:
CyberArk does not implement license limits by controlling the number and types of users that can be provisioned in the vault. CyberArk implements license limits by controlling the number and types of users that can authenticate to the vault and use its features. The license limits are based on the user types and objects that are defined in the vault, such as Vault Users, LDAP Users, LDAP Groups, Safes, Accounts, etc. The license limits are enforced by the License Manager, which is a service that runs on the Vault server and monitors the license usage. The License Manager can send notifications and alerts when the license usage reaches certain thresholds, and can also block or allow access to the vault based on the license status1.
References:
? 1: Manage the CyberArk License

NEW QUESTION 82
What is the purpose of the HeadStartlnterval 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 83

The Vault administrator can change the Vault license by uploading the new license to the system Safe.

A. True
B. False

Answer: A

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

NEW QUESTION 86
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 91
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 92
If a user is a member of more than one group that has authorizations on a safe, by default that user is granted .

A. the vault will not allow this situation to occur.
B. only those permissions that exist on the group added to the safe first.
C. only those permissions that exist in all groups to which the user belongs.
D. the cumulative permissions of all groups to which that user belongs.

Answer: D

Explanation:
When a user is a member of more than one group that has authorizations on a safe, by default that user is granted the cumulative permissions of all groups to which that user belongs. This means that the user will have the highest level of access that any of the groups have on the safe. For example, if one group has View and Retrieve permissions, and another group has Add and Delete permissions, the user will have View, Retrieve, Add, and Delete permissions on the safe. This is the default behavior of the vault, unless the Exclusive option is enabled on the safe. The Exclusive option restricts the user’s permissions to only those of the group added to the safe first. References:
? [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.2:
Safe Permissions, Slide 8: Cumulative Permissions
? [Defender PAM Sample Items Study Guide], Question 1: Safe Permissions
? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section: Safe Properties, Subsection: Exclusive

NEW QUESTION 96
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 97
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 99
Before failing back to the production infrastructure after a DR exercise, what must you do to maintain audit history during the DR event?

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

Answer: A

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

NEW QUESTION 103
You have been asked to create an account group and assign three accounts which belong to a cluster. When you try to create a new group, you receive an unauthorized error; however, you are able to edit other aspects of the account properties.
Which safe permission do you need to manage account groups?

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

Answer: D

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

NEW QUESTION 107
What are the mandatory fields when onboarding from Pending Accounts? (Choose two.)

A. Address
B. Safe
C. Account Description

D. Platform
E. CPM

Answer: BD

Explanation:
When onboarding accounts from the Pending Accounts list, the mandatory fields that must be specified are the Safe where the account will be stored and the Platform that the account will be associated with. The Safe is crucial as it determines the secure location within the CyberArk Vault where the account's credentials will be kept. The Platform is essential because it defines the set of policies and behaviors that will be applied to the account, such as password rotation and session monitoring12.
References:
? CyberArk Docs - Pending accounts1
? CyberArk Docs - Onboarding rules

NEW QUESTION 110
When running a "Privileged Accounts Inventory" Report through the Reports page in PVWA on a specific safe, which permission/s are required on that safe to show complete account inventory information?

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

Answer: A

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

NEW QUESTION 113
For a safe with Object Level Access enabled you can turn off Object Level Access Control when it no longer needed on the safe.

A. TRUE
B. FALSE

Answer: B

Explanation:
According to the CyberArk documentation1, once Object Level Access Control is enabled for a Safe, it cannot be disabled. This feature allows granular control over user access to passwords and files in the Safe, regardless of their Safe level member authorizations2. To enable Object Level Access Control, users need to have the Manage Safe authorization in the Vault1.

NEW QUESTION 117
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 119
A Vault administrator have associated a logon account to one of their Unix root accounts in
the vault. When attempting to verify the root account's password the Central Policy Manager (CPM) will:

A. ignore the logon account and attempt to log in as root
B. prompt the end user with a dialog box asking for the login account to use
C. log in first with the logon account, then run the SU command to log in as root using the password in the Vault
D. none of these

Answer: C

Explanation:
According to the web search results, when a Vault administrator has associated a logon account to one of their Unix root accounts in the vault, the CPM will log in

first with the logon account, then run the SU command to log in as root using the password in the Vault1. This is a common use case for using a logon account, as the best practice for Unix systems is to disallow the root user from logging in using SSH, which is what the CPM uses to sign in to a system to manage the password2. The logon account can be defined on the target account level or on the platform level, making it available to all
accounts associated with the platform2. The CPM can also use the logon account to initiate PSM sessions to the target machine3.

NEW QUESTION 121
In the Private Ark client under the Tools menu > Administrative Tools > Users and Groups, which option do you use to update users' Vault group memberships?

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

Answer: C

Explanation:
In the PrivateArk client, to update users' Vault group memberships, you use the Member Of tab. After logging in as an administrative user and navigating to the Users and Groups window, you select a user and click Update. In theMember Of tab, you can manage the user's group memberships by adding or removing them from groups within the Vault1.
References:
? CyberArk Docs - Manage users in PrivateArk client1

NEW QUESTION 122
Secure Connect provides the following. Choose all that apply.

A. PSM connections to target devices that are not managed by CyberArk.
B. Session Recording
C. Real-time live session monitoring.
D. PSM connections from a terminal without the need to login to the PVWA

Answer: ABC

Explanation:
Secure Connect provides the following features:
? A. PSM connections to target devices that are not managed by CyberArk. This is true, because Secure Connect is a feature that enables users to connect to target systems through PSM without storing the account credentials in the vault. Secure Connect allows users to provide their own credentials at the time of connection, and these credentials are not saved or managed by CyberArk. Secure Connect can be used with any connection component that supports PSM, such as RDP, SSH, WinSCP, etc1.
? B. Session Recording. This is true, because Secure Connect sessions are recorded by PSM and stored in the Vault, just like regular PSM sessions. The recorded sessions can be viewed and audited by authorized users through the PVWA or the PSM web interface2.
? C. Real-time live session monitoring. This is true, because Secure Connect sessions can be monitored in real-time by authorized users through the PSM web interface. The PSM web interface allows users to view the live session screen, send messages to the session user, pause or terminate the session, and take control of the session if needed3.
The following feature is not provided by Secure Connect:
? D. PSM connections from a terminal without the need to login to the PVWA. This is false, because Secure Connect requires users to login to the PVWA and initiate the connection from there. The PVWA provides the URL for the Secure Connect session, which contains the target system address and the connection component ID. The user then needs to copy and paste the URL into a browser or a remote connection manager to launch the session1.
References:
? 1: Secure Connect
? 2: Recorded Sessions
? 3: PSM Web Interface

NEW QUESTION 127
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 132
Which of the following are secure options for storing the contents of the Operator CD, while still allowing the contents to be accessible upon a planned Vault restart? (Choose three.)

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

Answer: ABD

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

NEW QUESTION 137
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 141
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 145
VAULT authorizations may be granted to .

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

Answer: AC

Explanation:
Vault Authorizations
• Can be assigned only to users (not groups).
• Cannot be inherited via group membership.
• Defined only via the Private Ark Client. Safe Auth
• Assigned to users and/or groups.
• Can be inherited via group membership.

- Can be defined in the Private Ark Client or PVWA

NEW QUESTION 146
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

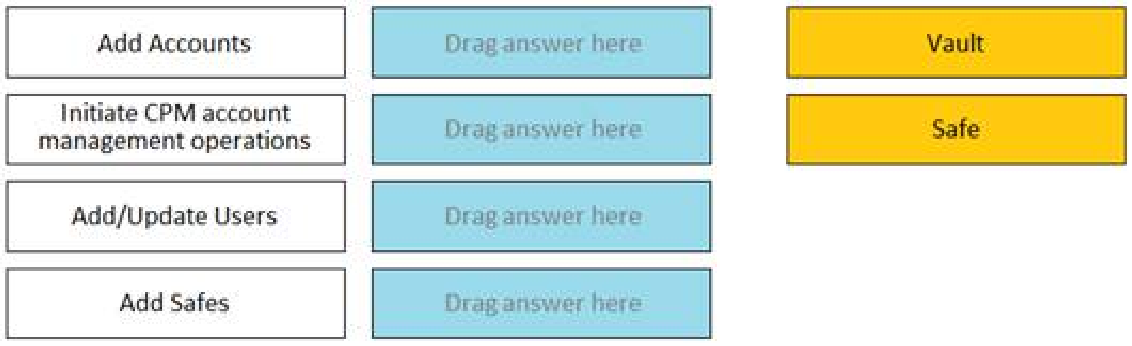
NEW QUESTION 150
A Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control.

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 155
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 156
Which service should NOT be running on the DR Vault when the primary Production Vault is up?

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

Answer: C

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

NEW QUESTION 161
What is the correct process to install a custom platform from the CyberArk Marketplace?

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

Answer: B

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

NEW QUESTION 162
What can you do to ensure each component server is operational?

A. Logon to PVWA with v10 UI, navigate to Healthcheck, and validate each component server is connected to the Vault.
B. Ping each component server to ensure connectivity.
C. Use the PrivateArk client to connect to the Vault server and validate all the services are running.
D. Install the Vault Server interface on a remote machine to avoid interactive logon to the Vault OS and review the ITALog.log through the Vault Server interface.

Answer: A

Explanation:
To ensure that each component server is operational, you can log on to the Privileged Vault Web Access (PVWA) with the version 10 user interface, navigate to the Healthcheck section, and validate that each component server is connected to the Vault. The System Health dashboard in PVWA provides a high-level visual representation of the health status of the different CyberArk components, including whether the Vault service is up and whether the component servers are connected1.
References:
? CyberArk Docs - Monitor system health

NEW QUESTION 164
In a default CyberArk installation, which group must a user be a member of to view the “reports” page in PVWA?

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

Answer: A

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

NEW QUESTION 167
Where can reconcile and/or logon accounts be linked to an account? (Choose two.)

A. account settings
B. platform settings
C. master policy
D. safe settings
E. service account settings

Answer: BD

Explanation:
Reconcile and logon accounts can be linked to an account within the platform settings and safe settings. The platform settings define the parameters for its linked accounts in either the Target Account or Service Account that requires them. When linked accounts are specified in the Target Account platform, they appear in the CPM pane of the Account Details page. Similarly, when they are specified in the Service Account platform, they appear in the CPM pane of the Service Account Details page1. Safe settings are also involved in the process of linking accounts, as they determine where the accounts are stored and managed within the CyberArk Vault.
References:
? CyberArk Docs - Linked Accounts1
? CyberArk REST API documentation on adding Reconcile and Login Accounts to an Account

NEW QUESTION 168
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 172
The Accounts Feed contains:

A. Accounts that were discovered by CyberArk in the last 30 days
B. Accounts that were discovered by CyberArk that have not yet been onboarded
C. All accounts added to the vault in the last 30 days
D. All users added to CyberArk in the last 30 days

Answer: B

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

NEW QUESTION 177
For Digital Vault Cluster in a high availability configuration, how does the cluster determine if a node is down?

A. The heartbeat s no longer detected on the private network.
B. The shared storage array is offline.
C. An alert is generated in the Windows Event log.
D. The Digital Vault Cluster does not detect a node failure.

Answer: A

Explanation:
In a Digital Vault Cluster environment, each node has a Cluster Vault Manager (CVM) service that monitors the local resources and the status of the other node via a private network1. The CVM service sends a heartbeat signal to the other node every few seconds to check its availability2. If the heartbeat is not detected for a certain period of time, the CVM service assumes that the other node is down and triggers a failover process3. The failover process involves shutting down the resources on the failed node and starting them on the available node4. References: Digital Vault Cluster environment, CyberArk High-Availability Vault Cluster, Manage the CyberArk Digital Cluster Vault Server, Local resources failover process

NEW QUESTION 179
Which item is an option for PSM recording customization?

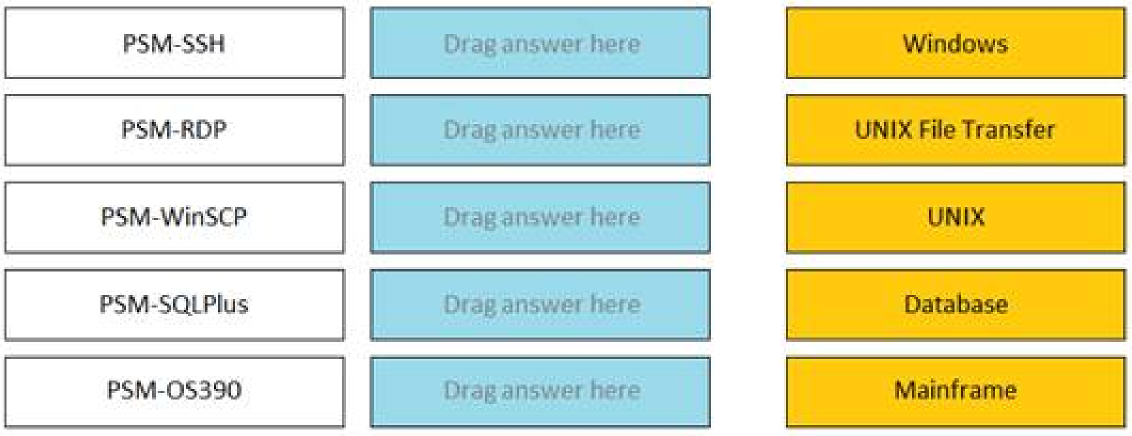
A. Windows events text recorder with automatic play-back

B. Windows events text recorder and universal keystrokes recording simultaneously
C. Universal keystrokes text recorder with windows events text recorder disabled
D. Custom audio recording for windows events

Answer: C

Explanation:
For PSM recording customization, one of the options is to use the Universal keystrokes text recorder with theWindows events text recorder disabled. This configuration allows for the recording of all keystrokes that are typed during privileged sessions on all supported connections. However, it is important to note that Universal keystroke recording andWindows events recordings cannot be configured for the same PSM-RDP connection. By default, Windows events text recording is enabled for PSM-RDP connections, so to enable universal keystrokes text recording, the Windows events text recording must first be disabled1.
References:
? CyberArk's official documentation on configuring recordings and audits in PSM, which includes details on how to customize text recorders and the limitations of configuring multiple recorders for the same connection1

NEW QUESTION 182
DRAG DROP
Match the connection component to the corresponding OS/Function.



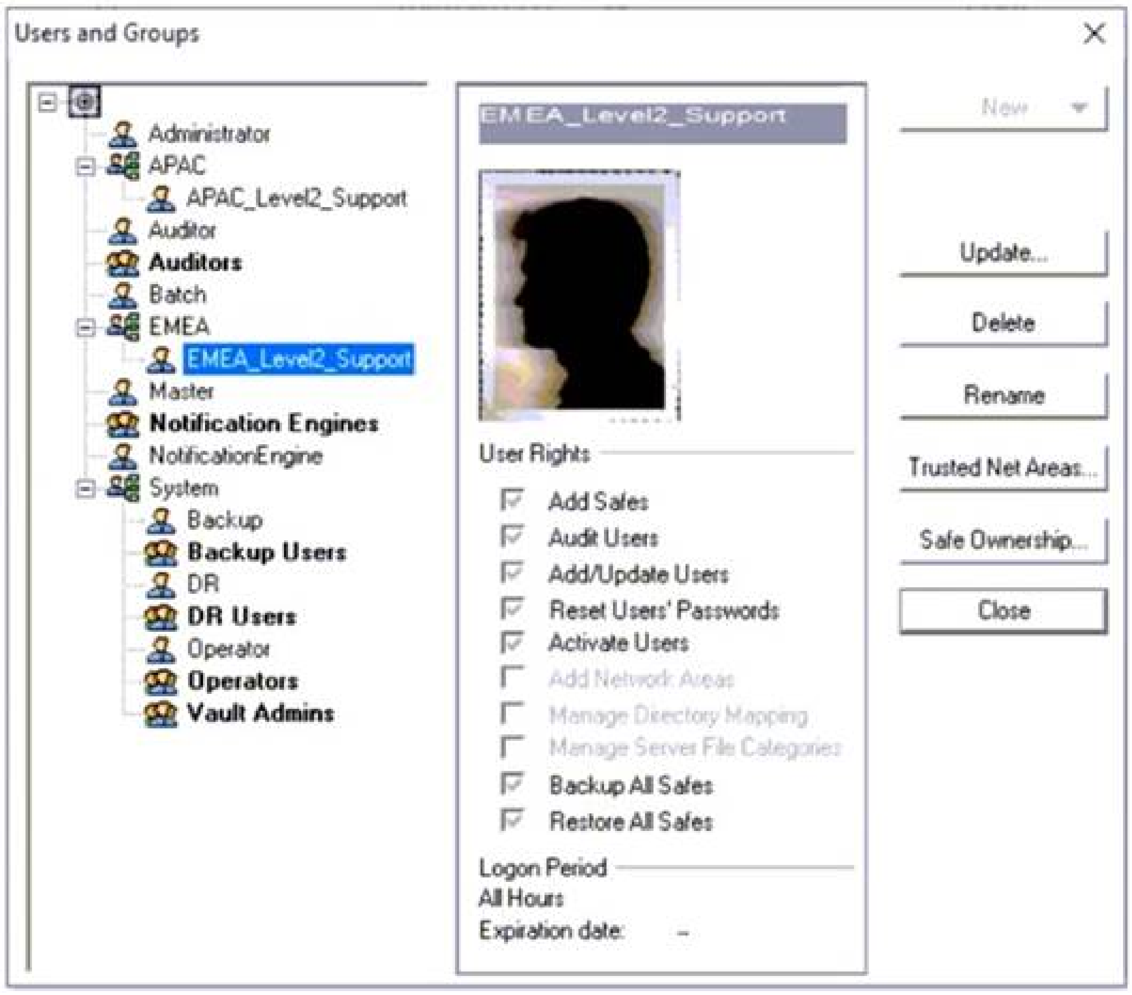
PSM-SSH	Drag answer here	Windows
PSM-RDP	Drag answer here	UNIX File Transfer
PSM-WinSCP	Drag answer here	UNIX
PSM-SQLPlus	Drag answer here	Database
PSM-OS390	Drag answer here	Mainframe

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? A connection component is a set of parameters that defines how PSM connects to a target system using a specific protocol or application. Different connection components are suitable for different types of systems or functions. The correct matches are as follows:
? PSM-SSH: This connection component enables transparent connections to UNIX machines using the SSH protocol. It supports various UNIX flavors, such as Linux, Solaris, AIX, and HP-UX.
? PSM-RDP: This connection component enables transparent connections to Windows machines using the RDP protocol. It supports various Windows versions, such as Windows Server, Windows 10, and Windows 7.
? PSM-WinSCP: This connection component enables transparent connections to UNIX machines using the WinSCP application. It supports file transfer operations, such as upload, download, delete, and rename, between the local and remote machines.
? PSM-SQLPlus: This connection component enables transparent connections to Oracle databases using the SQL*Plus application. It supports various Oracle versions, such as Oracle 12c, Oracle 11g, and Oracle 10g.
? PSM-OS390: This connection component enables transparent connections to IBM mainframes using the OS/390 protocol. It supports various mainframe applications, such as TSO, CICS, and IMS.
References: Connection Components, Connection Component Parameters

NEW QUESTION 183
Refer to the exhibit.



EMEA_Level2_Support

User Rights

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

Logon Period
All Hours
Expiration date: -

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

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

Answer: D

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

NEW QUESTION 186
When managing SSH keys, the CPM stored the Private Key

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

Answer: A

Explanation:
When managing SSH keys, the CPM stores the private key in the Vault. The CPM generates a new random SSH key pair and updates the public SSH key on the target server. The new private SSH key is then stored in the Digital Vault where it benefits from all the accessibility and security features of the Vault. The private SSH key is never stored on the target server, as this would expose it to unauthorized access or theft. The private SSH key cannot be generated from the public key, as this would defeat the purpose of
asymmetric encryption. References:
? Manage SSH Keys
? SSH Key Manager
? Use SSH Keys

NEW QUESTION 188
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?

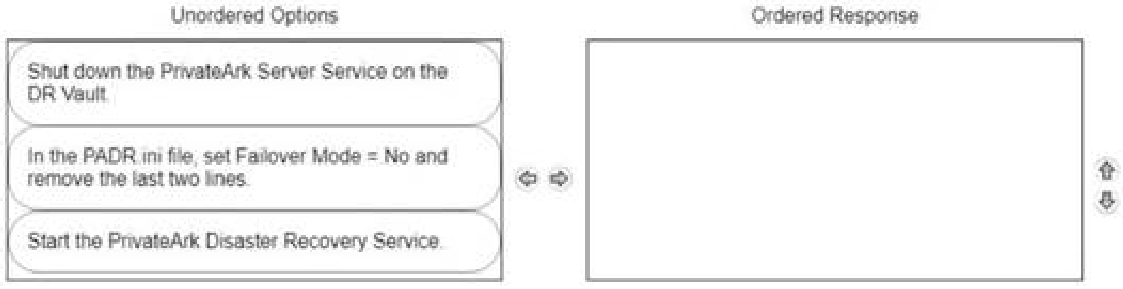
A. KeyPath
B. KeyFile
C. ObjectName
D. Address

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 193
DRAG DROP
ADR Vault became active due to a failure of the primary Vault. Service on the primary Vault has now been restored. Arrange the steps to return the DR vault to its normal standby mode in the correct sequence.



Shut down the PrivateArk Server Service on the DR Vault.

In the PADR.ini file, set Failover Mode = No and remove the last two lines.

Start the PrivateArk Disaster Recovery Service.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Shut down the PrivateArk Server Service on the DR Vault.
? In the PADR.ini file, set Failover Mode = No and remove the last two lines.
? Start the PrivateArk Disaster Recovery Service.
Comprehensive Explanation: When the primary Vault service has been restored and you need to return the DR Vault to its normal standby mode, the steps are as follows:
? Shut down the PrivateArk Server Service on the DR Vault to stop the Vault from being active.
? Modify the PADR.ini file by setting Failover Mode to No and removing the last two lines that were added during the failover process. This reconfigures the DR Vault to standby mode.
? Start the PrivateArk Disaster Recovery Service to complete the transition back to standby mode1.
References:
? CyberArk Docs - Initiate a DR Failback to the Production Vault1

NEW QUESTION 195
Which is the primary purpose of exclusive accounts?

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: D

Explanation:
According to the web search results, exclusive accounts are a feature of CyberArk Defender PAM that enables 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 time1. After the user has used the password, the user checks the password back into the Vault. This ensures exclusive usage of the privileged account, enabling full control and tracking for the password. The duration of the check-out period can be configured in the platform settings for each account1.
The primary purpose of exclusive accounts is to prevent a single user from accessing a sensitive account without authorization, which could lead to fraud or misuse of privileges. By requiring a check-out and check-in process, exclusive accounts ensure that there is a 'collusion to commit' fraud, meaning that at least two users are involved in the malicious activity and are accountable for it. One user must check out the password and use it, while another user must approve the check-in and verify the password change. This way, exclusive accounts add an additional measure of protection and accountability for accessing sensitive accounts.

NEW QUESTION 200
Your customer, ACME Corp, wants to store the Safes Data in Drive D instead of Drive C. Which file should you edit?

A. TSparm.ini
B. Vault.ini
C. DBparm.ini
D. user.ini

Answer: A

Explanation:
To store the Safes Data in a different drive, such as moving from Drive C to Drive D, you need to edit the TSparm.ini file. This file contains various parameters that configure the behavior of the Vault, including the location of the Safes Data. By editing the SafesDirectory parameter in theTSparm.ini file, you can specify a new path for the Safes Data, effectively changing the storage location to the desired drive1.
References:
? CyberArk's official documentation on managing files and documents, which includes information on how to store files in different locations within the Vault2.
? Knowledge articles on how to move the PSMRecordings safe or other Vault data to a different drive, which provide step-by-step instructions and mention the TSparm.ini file1

NEW QUESTION 202
When should vault keys be rotated?

A. when it is copied to file systems outside the vault

B. annually
C. whenever a CyberArk user leaves the organization
D. when migrating to a new data center

Answer: D

Explanation:
Vault keys should be rotated when there is a significant event that could potentially compromise the security of the keys, such as when migrating to a new data center. This is because the keys may be exposed to new environments and systems, and rotating them ensures that any potential exposure does not result in a security breach. Additionally, periodic rotation of encryption keys is recommended to maintain the integrity of the encryption and to adhere to best practices for security1. References:
? CyberArk Docs: Credentials Rotation Policy2
? HashiCorp Developer: Key Rotation

NEW QUESTION 207
What is the purpose of the PrivateArk Server service?

A. Executes password changes
B. Maintains Vault metadata
C. Makes Vault data accessible to components
D. Sends email alerts from the Vault

Answer: C

Explanation:
The purpose of the PrivateArk Server service is to make Vault data accessible to components, such as the PVWA, the CPM, the PSM, and the PTA, and handle the requests from the clients and components. The PrivateArk Server service is a Windows service that runs the Vault and communicates with the PrivateArk Database service, which maintains the Vault metadata. The PrivateArk Server service can start automatically or manually depending on the Server's key configuration. The PrivateArk Server service can also be run in "console" mode for troubleshooting purposes1.
The other options are not the purpose of the PrivateArk Server service, although they may be related to other services or components of the Vault. The Central Policy Manager component is the component that executes password changes, verifications, and reconciliations for the accounts that are managed by the Vault. The Event Notification Engine service is the service that sends email alerts from the Vault, based on predefined events and recipients. The PrivateArk Client is a utility that allows the Vault administrator to access and manage the Vault data, users, groups, policies, and settings. References:
? Server Components - CyberArk, section "The PrivateArk Server process (Dbmain)"

NEW QUESTION 212
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 217
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 220
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 221
SAFE Authorizations may be granted to . Select all that apply.

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

Answer: ABCD

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

NEW QUESTION 223
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 227
You need to enable the PSM for all platforms. Where do you perform this task?

A. Platform Management > (Platform) > UI & Workflows
B. Master Policy > Session Management
C. Master Policy > Privileged Access Workflows
D. Administration > Options > Connection Components

Answer: A

Explanation:
To enable PSM for specific platforms, you need to go to Platform Management, select the platform you want to configure, click Edit, expand UI & Workflows, and select Privileged Session Management. There you can customize the PSM settings for that platform, such as the PSM server ID, the connection components, the PSM connection method, and the PSM recording options. You can also disable dual control for PSM connections if needed. References: Configure PSM for Specific Platforms

NEW QUESTION 231
The password upload utility must run from the CPM server

A. TRUE
B. FALSE

Answer: A

Explanation:
According to the CyberArk documentation1, the Password Upload utility must run from the Central Policy Manager (CPM) server. This utility works by uploading passwords and their properties into the Password Vault from a pre-prepared file, creating the required environment, when necessary. It is run from a command line

whenever a password upload is required1.

NEW QUESTION 233
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

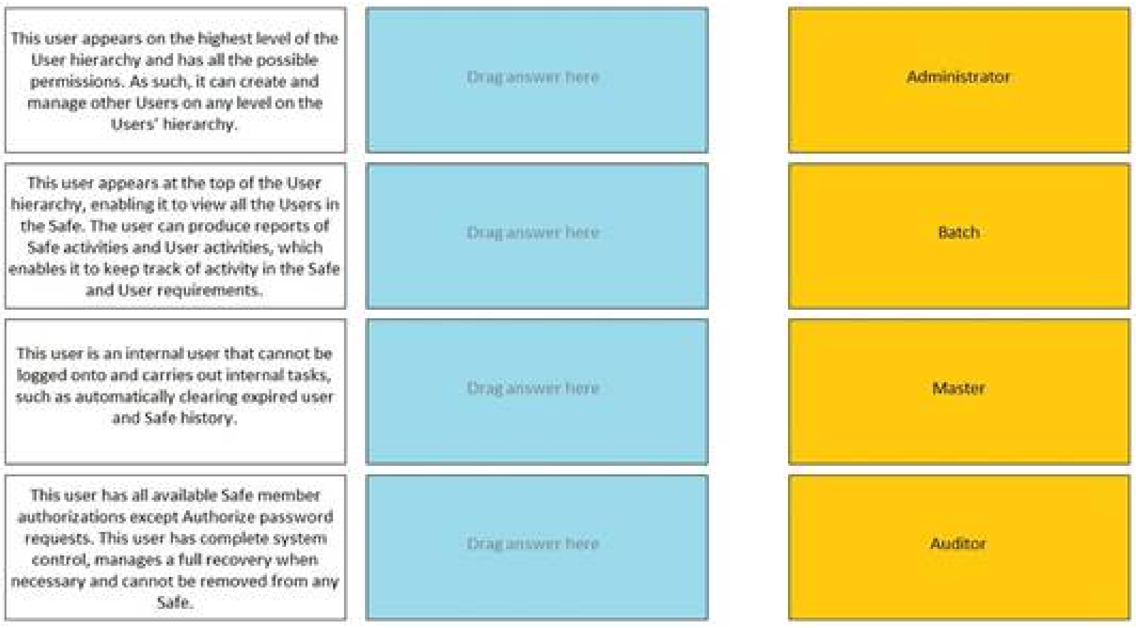
NEW QUESTION 234
Which type of automatic remediation can be performed by the PTA in case of a suspected credential theft security event?

A. Password change
B. Password reconciliation
C. Session suspension
D. Session termination

Answer: A

Explanation:
The PTA can perform automatic password change as a type of remediation in case of a suspected credential theft security event. According to the CyberArk documentation1, "Rotate credentials - for OverPass the Hash attack and Suspected credentials theft events."1 This means that the PTA can initiate a password change request to the CPM for the affected account, which will generate a new random password and update it on the target system and the Vault. This way, the PTA can prevent the attacker from using the stolen credentials to access the target system or launch further attacks. References:
? Configure PTA Remediations - CyberArk, section “Remediation Initiation”

NEW QUESTION 239
DRAG DROP
Match the built-in Vault User with the correct definition.

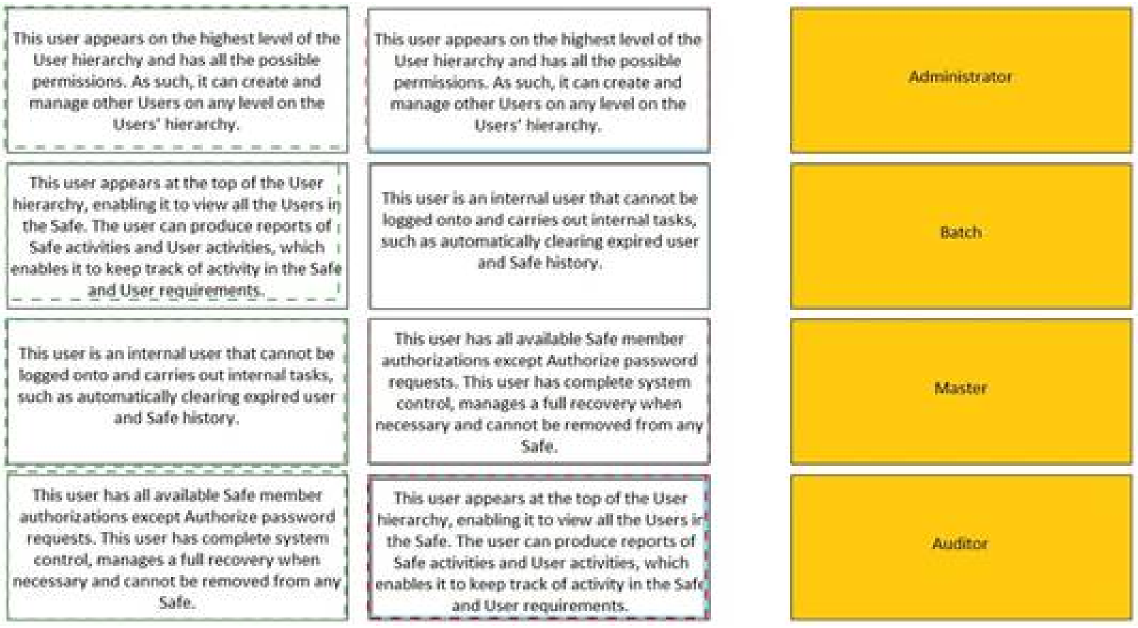


This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.	Drag answer here	Administrator
This user appears at the top of the User hierarchy, enabling it to view all the Users in 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

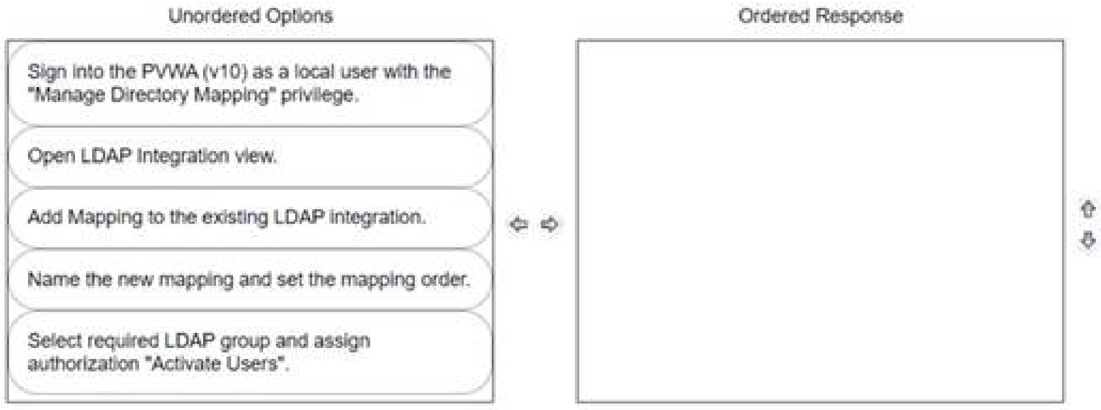
NEW QUESTION 243
Which statement is true about setting the reconcile account at the platform level?

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

Answer: C

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

NEW QUESTION 247
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".

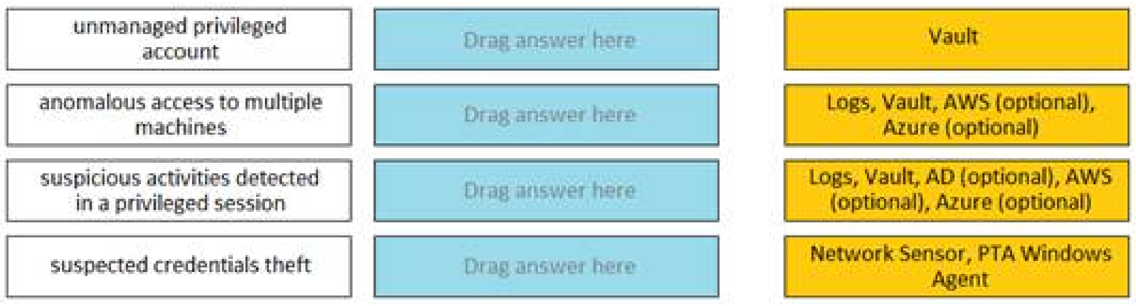
Ordered Response

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 251
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 256
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 257
You are creating a new Rest API user that utilizes CyberArk Authentication.
What is a correct process to provision this user?

A. Private Ark Client > Tools > Administrative Tools > Users and Groups > New > User
B. Private Ark Client > Tools > Administrative Tools > Directory Mapping > Add
C. PVWA > User Provisioning > LDAP Integration > Add Mapping
D. PVWA > User Provisioning > Users and Groups > New > User

Answer: D

Explanation:
To provision a new Rest API user that utilizes CyberArk Authentication, the correct process involves using the PVWA (Password Vault Web Access). You would navigate to the User Provisioning section, then to Users and Groups, and select New > User. This allows you to create a new user that can be configured for Rest API access with the appropriate authentication method1.
References:
? CyberArk's official documentation on implementing Privileged Account Security Web Services provides information on using REST APIs to create, list, modify, and delete entities in PAM - Self-Hosted from within programs and scripts, which includes user provisioning1.
? Additional details on the process and best practices for creating Rest API users can be found in the CyberArk Privileged Access Manager documentation and training resources

NEW QUESTION 260
A user requested access to view a password secured by dual-control and is unsure who to contact to expedite the approval process. The Vault Admin has been asked to look at the account and identify who can approve their request.
What is the correct location to identify users or groups who can approve?

A. PVWA> Administration > Platform Configuration > Edit Platform > UI & Workflow > Dual Control> Approvers
B. PVWA> Policies > Access Control (Safes) > Safe Members > Workflow > Authorize Password Requests
C. PVWA> Account List > Edit > Show Advanced Settings > Dual Control > Direct Managers
D. PrivateArk > Admin Tools > Users and Groups > Auditors (Group Membership)

Answer: B

Explanation:
In CyberArk's Privileged Access Management (PAM), the correct location to identify users or groups who can approve a dual-control request is within the

Password Vault Web Access (PVWA). Specifically, you would navigate to the 'Policies' section, then to 'Access Control (Safes)', and within a safe, you would go to 'Safe Members'. Here, under the 'Workflow' tab, there is an option to 'Authorize Password Requests'. This is where the Vault Admin can identify which users or groups are authorized to approve requests for viewing passwords secured by dual-control.
References: The information is based on the best practices and guidelines provided in the CyberArk Defender PAM course and learning resources, which include the official CyberArk documentation and study guides.

NEW QUESTION 263
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 266
Which processes reduce the risk of credential theft? (Choose two.)

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

Answer: BD

NEW QUESTION 270
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 274
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 275
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 277
......