CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM

NEW QUESTION 1
You have been asked to turn off the time access restrictions for a safe. Where is this setting found?

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

Answer: A

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

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

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

Answer: AB

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

NEW QUESTION 3
Which one the following reports is NOT generated by using the PVWA?

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

Answer: C

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

NEW QUESTION 4
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 5
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

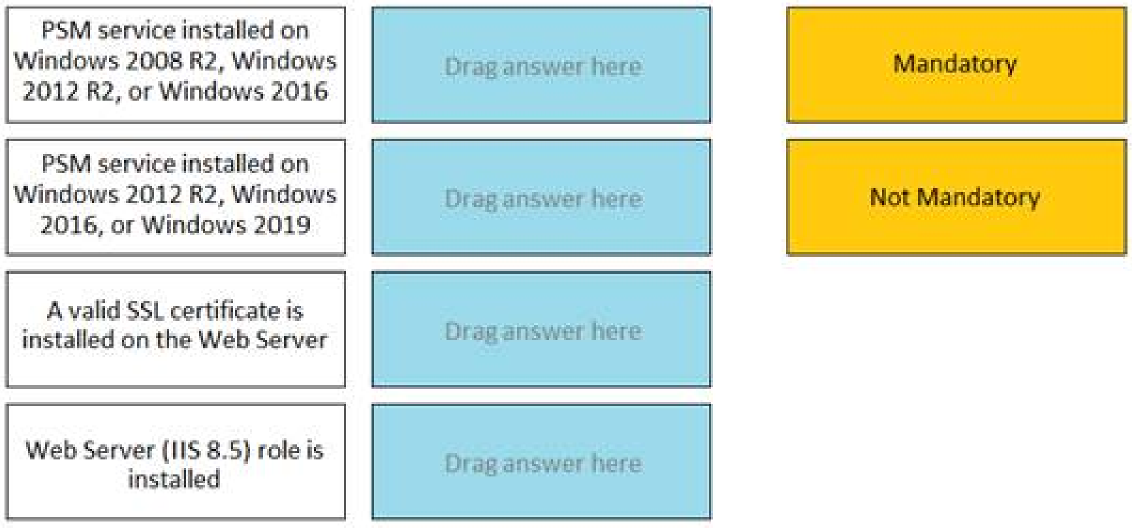
NEW QUESTION 6
Which of the following Privileged Session Management (PSM) solutions support live monitoring of active sessions?

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 7
DRAG DROP
For each listed prerequisite, identify if it is mandatory or not mandatory to run the PSM Health Check.

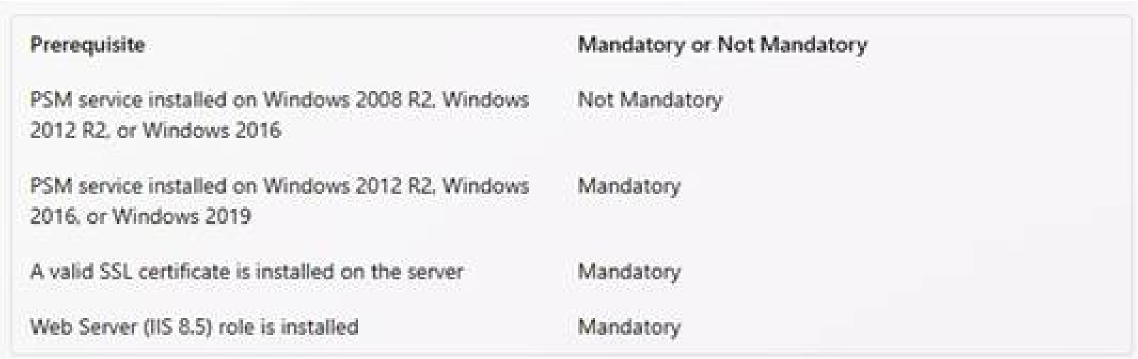


PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016	Drag answer here	Mandatory
PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019	Drag answer here	Not Mandatory
A valid SSL certificate is installed on the Web Server	Drag answer here	
Web Server (IIS 8.5) role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

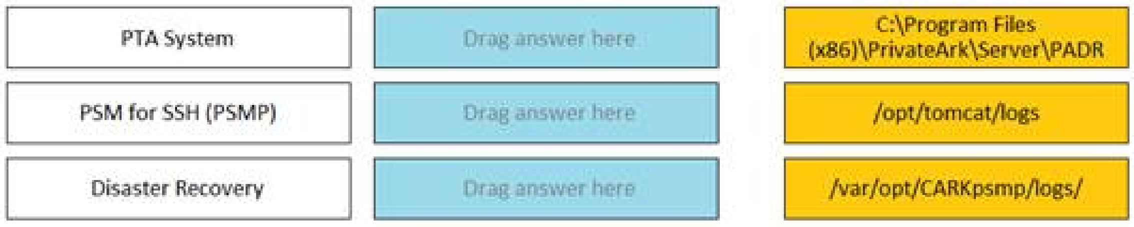
NEW QUESTION 10
Which of the following logs contains information about errors related to PTA?

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 10
DRAG DROP
Match each component to its respective Log File location.

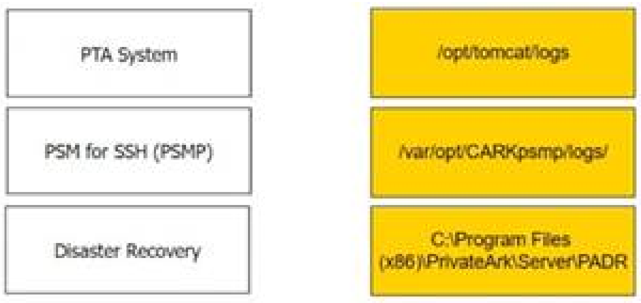


PTA System	Drag answer here	C:\Program Files (x86)\PrivateArk\Server\PADR
PSM for SSH (PSMP)	Drag answer here	/opt/tomcat/logs
Disaster Recovery	Drag answer here	/var/opt/CARKpsmp/logs/

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 12
You have been given the requirement that certain accounts cannot have their passwords updated during business hours.
How can you set up a configuration to meet this requirement?

A. Change settings on the CPM configuration safe so that access is permitted after business hours only.
B. Update the password change parameters of the platform to match the permitted time frame.
C. Disable automatic CPM management for all accounts that are assigned to this platform.
D. Add an exception to the Master Policy to allow the action for this platform during the permitted time.

Answer: B

Explanation:
To ensure that certain accounts do not have their passwords updated during business hours, you can configure the password change parameters within the platform settings to specify the permitted time frame for updates. This involves setting the FromHour andToHour parameters to define a window outside of business hours during which the CyberArk Central Policy Manager (CPM) will perform automatic password changes1. By doing so, you can control when password changes occur and ensure compliance with the specified requirement.
References:
? CyberArk Community: Discussion on configuring automatic password change parameters

NEW QUESTION 14
What is required to enable access over SSH to a Unix account through both PSM and PSMP?

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

Answer: A

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

NEW QUESTION 18
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 20
Which usage can be added as a service account platform?

A. Kerberos Tokens
B. IIS Application Pools
C. PowerShell Libraries
D. Loosely Connected Devices

Answer: B

Explanation:
A service account platform is a type of platform that defines how CyberArk manages passwords for service accounts, which are accounts that run applications or services on remote machines. A usage is a configuration that allows CyberArk to manage passwords for files, such as XML or INI files, that are stored on remote machines. A usage is associated with a parent account, which is the account that has access to the file. A usage can be added as a service account platform if the file contains the password of a service account. For example, IIS Application Pools is a usage that can be added as a service account platform, because it manages the passwords of the application pools that run on IIS servers. The other options, Kerberos Tokens, PowerShell Libraries, and Loosely Connected Devices, are not usages that can be added as service account platforms, because they do not manage passwords for service accounts. References: Usages, Service Account Platforms

NEW QUESTION 22
When are external vault users and groups synchronized by default?

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

Answer: A

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

NEW QUESTION 25
Where can you assign a Reconcile account? (Choose two.)

A. in PVWA at the account level
B. in PVWA in the platform configuration
C. in the Master policy of the PVWA
D. at the Safe level
E. in the CPM settings

Answer: AB

Explanation:
A Reconcile account can be assigned in the Privileged Vault Web Access (PVWA) at both the account level and within the platform configuration. At the account level, a Reconcile account password can be defined which will override the account specified in the platform1. In the platform configuration, you can navigate to Platform Management, select the platform, edit it, and then expand Automatic Password Management to enter the values in the ‘ReconcileAccountSafe’ and

'ReconcileAccountName' fields, which will apply to all accounts attached to that specific platform2.
References:
? CyberArk Docs - Reconcile Password1
? CyberArk Community - Associate reconcile account with a specific platform

NEW QUESTION 29
Which statement is correct concerning accounts that are discovered, but cannot be added to the Vault by an automated onboarding rule?

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

Answer: A

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

NEW QUESTION 32
You are concerned about the Windows Domain password changes occurring during business hours.
Which settings must be updated to ensure passwords are only rotated outside of business hours?

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

Answer: B

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

NEW QUESTION 36
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 38
You are onboarding 5,000 UNIX root accounts for rotation by the CPM. You discover that the CPM is unable to log in directly with the root account and will need to use a secondary account.
How should this be configured to allow for password management using least privilege?

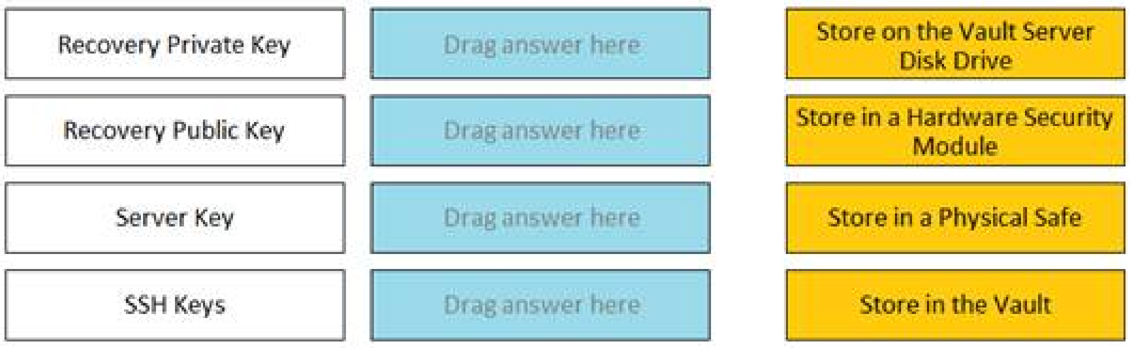
A. Configure each CPM to use the correct logon account.
B. Configure each CPM to use the correct reconcile account.
C. Configure the UNIX platform to use the correct logon account.
D. Configure the UNIX platform to use the correct reconcile account.

Answer: C

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

environments, which includes setting up the correct logon account for tasks that require elevated privileges1.
? Additional information on managing UNIX and Linux accounts, including the configuration of logon and reconcile accounts, can be found in the Unix plugin documentation for CyberArk

NEW QUESTION 39
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 43
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 47
Which user is automatically added to all Safes and cannot be removed?

A. Auditor
B. Administrator
C. Master
D. Operator

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 51

A user needs to view recorded sessions through the PVWA.
Without giving auditor access, which safes does a user need access to view PSM recordings? (Choose two.)

A. Recordings safe
B. Safe the account is in
C. System safe
D. PVWAConfiguration safe
E. VaultInternal safe

Answer: AB

Explanation:
To view recorded sessions through the PVWA without having auditor access, a user needs access to two specific safes: the Recordings safe and thesafe the account is in. The Recordings safe is where the PSM session recordings are stored, and users need permission to access this safe to view the recordings. Additionally, users need access to the safe where the account associated with the recorded session is stored, as this is where the session details and permissions are managed12.
References:
? CyberArk Docs - Configure video and text recordings3
? CyberArk Community - Viewing PSM recorded sessions1

NEW QUESTION 53
When a group is granted the 'Authorize Account Requests' permission on a safe Dual Control requests must be approved by

A. Any one person from that group
B. Every person from that group
C. The number of persons specified by the Master Policy
D. That access cannot be granted to groups

Answer: C

Explanation:
When a group is granted the ‘Authorize Account Requests' permission on a safe, dual control requests must be approved by the number of persons specified by the Master Policy. This means that the request will be sent to all the members of the group, but only a certain number of them need to confirm it for the request to be authorized. The Master Policy defines the number of required approvers for each level of confirmation, as well as the number of levels. For example, if the Master Policy requires two approvers at the first level and one approver at the second level, then the request will be sent to the group and two members of the group must confirm it before it is sent to the second level of confirmation, where one more approver is needed. References:
? Request access
? Safe Members
? CyberArk Defender - PAM Exam Practice Test

NEW QUESTION 57
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 60
How do you create a cold storage backup?

A. On the DR Vault, install PAReplicate according to the Installation guide, configure the logon ini file, and define the Schedule tasks for full and incremental backups.
B. Install the Vault Backup utility on a different machine from the Enterprise Password Vault server and trigger the full backup.
C. Configure the backup options in the PVWA.
D. On the DR Vault, configure the cold storage backup path in TSParm.ini file.

Answer: A

Explanation:
To create a cold storage backup, you would install thePAReplicate utility
on the DR Vault as per the installation guide. This utility is part of the CyberArk Vault's backup solution and is used to export the encrypted contents of your Safes securely to a computer outside the Vault environment. After installation, you would configure the logon ini file with the necessary credentials and define the scheduled tasks for both full and incremental backups. This ensures that the Safes are regularly backed up and that the data is available for recovery if needed1.
References:
? CyberArk's official documentation on using the CyberArk Backup Process, which includes details on the PAReplicate utility and how to configure it for cold storage backups1.
? Additional information on installing the Vault Backup Utility and configuring backup options, which provides context for the correct answer

NEW QUESTION 64
What do you need on the Vault to support LDAP over SSL?

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

Answer: A

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

NEW QUESTION 67
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 71
What is the name of the Platform parameters that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy?

A. Min Validity Period
B. Interval
C. Immediate Interval
D. Timeout

Answer: A

Explanation:
The name of the Platform parameter that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy is Min Validity Period. This parameter defines the number of minutes to wait from the last retrieval of the account until it is replaced. This gives the user a minimum period to be able to use the password before it is changed by the CPM. The Min Validity Period parameter can be configured in the Platform Management settings for each platform that supports One Time Passwords. The default value is 60 minutes, but it can be modified according to the organization's security policy1. The Min Validity Period parameter is also used to release exclusive accounts automatically1. References:
? 1: Privileged Account Management, Min Validity Period subsection

NEW QUESTION 74
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 75

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

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

Answer: C

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

NEW QUESTION 78
What is the maximum number of levels of authorization you can set up in Dual Control?

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

Answer: B

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

NEW QUESTION 80
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 84
Vault admins must manually add the auditors’ group to newly created safes so auditors will have sufficient access to run reports.

A. TRUE
B. FALSE

Answer: B

Explanation:
Vault admins do not need to manually add the auditors’ group to newly created safes, because the auditors’ group is automatically added to every safe in the vault by default. The auditors’ group has the View Audit authorization, which allows its members to view the safe’s activity and run reports. However, vault admins can remove the auditors’ group from specific safes if they want to restrict the access of the auditors. References: Predefined users and groups - CyberArk

NEW QUESTION 89
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 91
What is the configuration file used by the CPM scanner when scanning UNIX/Linux devices?

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

Answer: A

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

NEW QUESTION 95
Ad-Hoc Access (formerly Secure Connect) provides the following features. 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:
Ad-Hoc Access (formerly Secure Connect) is a feature that allows users to connect to target devices that are not managed by CyberArk through the PSM. Users can specify the address, username, and password of the target device, and select a client to launch the connection. Ad-Hoc Access sessions benefit from the standard PSM features, such as session recording, detailed auditing, and real-time live session monitoring. However, Ad- Hoc Access does not allow users to connect from a terminal without logging in to the PVWA, as this would bypass the authentication and authorization mechanisms of CyberArk. References:
? Configure ad hoc connections
? Ad Hoc Connections
? Privileged Remote Access Management – PAM Remote Access

NEW QUESTION 98
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 100
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 101
When creating an onboarding rule, it will be executed upon .

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

Answer: C

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

NEW QUESTION 103
Which CyberArk utility allows you to create lists of Master Policy Settings, owners and safes for output to text files or MSSQL databases?

A. Export Vault Data
B. Export Vault Information
C. PrivateArk Client
D. Privileged Threat Analytics

Answer: B

Explanation:
The Export Vault Information utility is a CyberArk tool that allows you to create lists of Master Policy settings, owners and safes for output to text files or MSSQL databases. This utility can be used to export various types of information from the Vault, such as accounts, safes, platforms, policies, users, groups, and audit records. The utility can also generate reports based on predefined templates or custom queries. The utility can be run from the command line or the graphical user interface. References: Export Vault Information, Export Vault Information Utility

NEW QUESTION 106
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 107
One can create exceptions to the Master Policy based on .

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

Answer: B

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

NEW QUESTION 109
What does the Export Vault Data (EVD) utility do?

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

Answer: A

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

NEW QUESTION 113
In order to connect to a target device through PSM, the account credentials used for the connection must be stored in the vault?

A. True.
B. Fals
C. Because the user can also enter credentials manually using Secure Connect.
D. Fals
E. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect.
F. Fals
G. Because if credentials are not stored in the vault, the PSM will prompt forcredentials.

Answer: B

Explanation:
In order to connect to a target device through PSM, the account credentials used for the connection do not necessarily have to be stored in the vault. The user can also enter credentials manually using Secure Connect, which 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, etc. To use Secure Connect, the user needs to specify the target system address and the connection component ID in the URL, and then enter the credentials in the PSM login screen1.
The other options are not correct, because:
? A. True. This is not correct, because as explained above, the user can also enter credentials manually using Secure Connect.
? C. False. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect. This is not correct, because PSM Connect is a predefined user that is created on the PSM server during the installation. This user is used to establish the connection between the PSM server and the target server, and to run the PSM processes. The PSM Connect user is not used to log into the target device as the end user2.
? D. False. Because if credentials are not stored in the vault, the PSM will prompt for credentials. This is not correct, because this option is essentially the same as Secure Connect, which is the correct answer.
References:
? 1: Secure Connect
? 2: PSMConnect and PSMAdminConnect

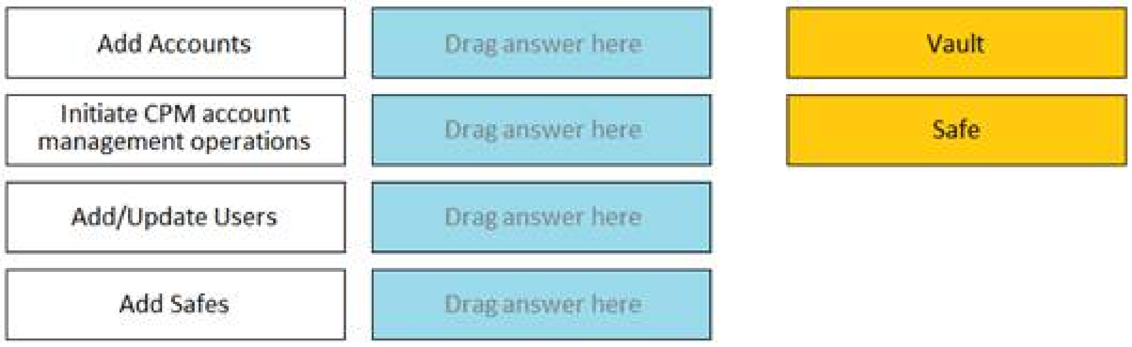
NEW QUESTION 117
Which of the following components can be used to create a tape backup of the Vault?

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

Answer: C

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

NEW QUESTION 118
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 119
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 120
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 125
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 129
It is possible to control the hours of the day during which a user may log into the vault.

A. TRUE
B. FALSE

Answer: A

Explanation:

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

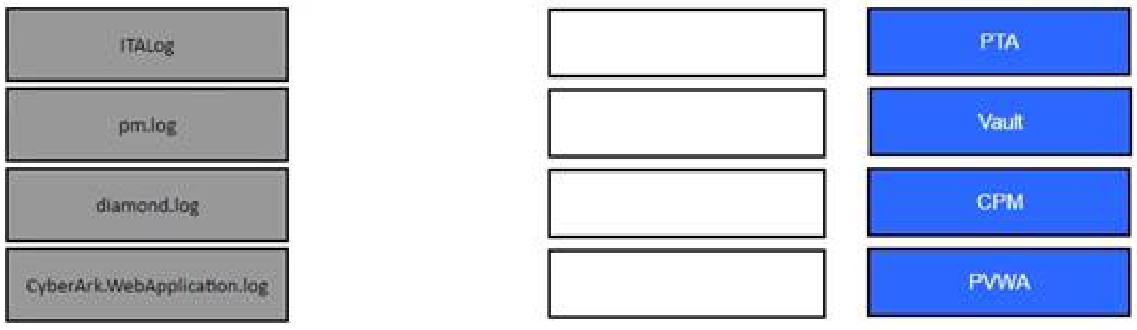
NEW QUESTION 134
Can the 'Connect' button be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied?

A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction.
B. Yes, only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component.
C. Yes, if a logon account is associated with the root account.
D. No, it is not possible.

Answer: B

Explanation:
The ‘Connect’ button is a feature of the PVWA that allows users to initiate a privileged session to a target system through PSM without revealing the account credentials. The ‘Connect’ button can be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, but only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component. A logon account is a linked account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the PSM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the PSM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account. The PSM-SSH connection component is a predefined connection component that enables users to connect to Unix systems through PSM using SSH. The PSM-SSH connection component supports the use of logon accounts to access root accounts on Unix systems1.
The other options are not correct, because:
? A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction. This is not correct, because PMTerminal.exe is a process that is used by the PSM-RDP connection component, not the PSM-SSH connection component. PMTerminal.exe is a terminal emulator that enables users to connect to Windows systems through PSM using RDP. PMTerminal.exe does not bypass the root SSH restriction, but rather uses the credentials stored in the Vault to authenticate to the target system2.
? C. Yes, if a logon account is associated with the root account. This is not correct, because a logon account alone is not sufficient to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied. The user also needs to connect through the PSM-SSH connection component, which supports the use of logon accounts to access root accounts on Unix systems1.
? D. No, it is not possible. This is not correct, because it is possible to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, as explained in option B.
References:
? 1: Logon Accounts for SSH and Telnet Connections
? 2: Connect through PSM for SSH

NEW QUESTION 137
DRAG DROP
Match the log file name with the CyberArk Component that generates the log.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 138
In addition to add accounts and update account contents, which additional permission on the safe is required to add a single account?

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

Answer: C

Explanation:
In addition to the permissions to add accounts and update account contents, the permission to Update Account Properties is required to add a single account to a

safe in CyberArk. This permission allows the user to modify the properties of an account, which is a necessary step when adding a new account to ensure that all relevant details and configurations are correctly set1. References: The information provided is based on general knowledge of CyberArk PAM best practices and the permissions required for account management as outlined in CyberArk's official documentation

NEW QUESTION 140
Your organization requires all passwords be rotated every 90 days. Where can you set this regulatory requirement?

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

Answer: D

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

NEW QUESTION 145
Which CyberArk group does a user need to be part of to view recordings or live monitor sessions?

A. Auditors
B. Vault Admin
C. DR Users
D. Operators

Answer: A

Explanation:
To view recordings or live monitor sessions, users must be part of the Auditors group or have the appropriate permissions in the relevant Account Safes and Recording Safes12. The other groups do not have the necessary permissions to access the recordings or monitor the sessions by default. References: Monitor Active Sessions, Active Session Monitoring

NEW QUESTION 150
A newly created platform allows users to access a Linux endpoint. When users click to connect, nothing happens.
Which piece of the platform is missing?

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

Answer: A

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

NEW QUESTION 155
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 156
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 159
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 160
Which report could show all accounts that are past their expiration dates?

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

Answer: A

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

NEW QUESTION 161
tsparm.ini is the main configuration file for the Vault.

A. True
B. False

Answer: B

Explanation:
tsparm.ini isnot the main configuration file for the Vault. It is one of the several configuration files that control the initial settings and method of operation of the Server. The main configuration file for the Vault is DBParm.ini, which contains the general parameters of the database, such as the Vault name, the Vault IP address, the Vault port, the encryption algorithm, the log retention, and the debug mode. References:
? Defender PAM Sample Items Study Guide, page 9, question 92
? CyberArk Privileged Access Security Implementation Guide, page 75, section "DBParm.ini"
? CyberArk Vault Server Parameter Files, page 1, section "TSParm.ini"

NEW QUESTION 162
You want to create a new onboarding rule. Where do you accomplish this?

A. In PVWA, click Reports > Unmanaged Accounts > Rules
B. In PVWA, click Options > Platform Management > Onboarding Rules
C. In PrivateArk, click Tools > Onboarding Rules
D. In PVWA, click Accounts > Onboarding Rules

Answer: D

Explanation:
To create a new onboarding rule, you accomplish this in the Privileged Vault Web Access (PVWA) by navigating to Accounts > Onboarding Rules. Once there, you can click on Create rule to start the New onboarding rule wizard and proceed with the configuration of the rule. This process allows you to set up rules that automatically onboard newly discovered accounts, minimizing manual effort and reducing the chance of human error1.
References:
? CyberArk Docs - Onboarding rules

NEW QUESTION 164
What is the purpose of the CyberArk Event Notification Engine service?

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

Answer: B

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

NEW QUESTION 167
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

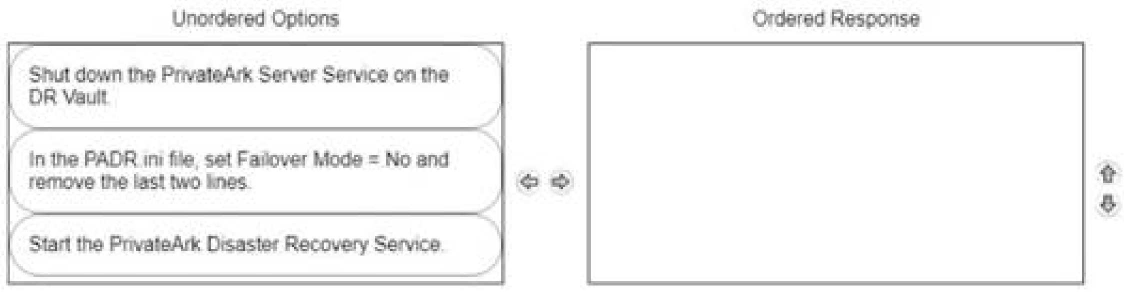
NEW QUESTION 170
You are troubleshooting a PVWA slow response. Which log files should you analyze first? (Choose two.)

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

Answer: CD

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

NEW QUESTION 175
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.



Unordered Options

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.

Ordered Response

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 179
Which utilities could you use to change debugging levels on the vault without having to restart the vault. Select all that apply.

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

Answer: AB

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

NEW QUESTION 180
You want to build a connector that connects to a website through the Web applications for PSM framework.
Which default connector do you duplicate and modify?

A. PSM-ChromeSample
B. PSM-WebForm
C. PSM-WebApp
D. PSM-WebAppSample

Answer: D

Explanation:
When building a connector to connect to a website through the Web applications for PSM framework, you would duplicate and modify the default connector PSM-WebAppSample. This sample connector serves as a template that can be customized to fit the specific requirements of the web application you are targeting. It provides a starting point with predefined settings that can be adjusted to create a new, functional connector for the desired web application12.
References:
? CyberArk Docs - Web applications for PSM2
? CyberArk Docs - Configure PSM to connect to Web applications1

NEW QUESTION 181
Which of the following options is not set in the Master Policy?

A. Password Expiration Time

B. Enabling and Disabling of the Connection Through the PSM
C. Password Complexity
D. The use of “One-Time-Passwords”

Answer: C

Explanation:
Password Complexity is not set in the Master Policy, but in the Platform Management settings for each platform. The Master Policy is a set of rules that define the security and compliance policy of privileged accounts in the organization, such as access workflows, password management, session monitoring, and auditing1. The Master Policy does not include any technical settings that determine how the system manages accounts on various platforms1. Password Complexity is a technical setting that defines the minimum requirements for the length and composition of the passwords that are generated by the CPM for the accounts associated with the platform2. Password Complexity can be configured in the Platform Management settings, which are independent of the Master Policy and can be customized according to the organization’s environment and security policies1.
The other options are set in the Master Policy, as follows:
? A. Password Expiration Time: This is a policy rule that determines how often passwords are changed. It can be set in the Master Policy under the Password Management section1.
? B. Enabling and Disabling of the Connection Through the PSM: This is a policy rule that determines whether users can connect to target systems through the PSM. It can be set in the Master Policy under the Session Management section1.
? D. The use of “One-Time-Passwords”: This is a policy rule that determines whether passwords are changed every time they are retrieved by a user. It can be set in the Master Policy under the Password Management section1. References:
? 1: The Master Policy
? 2: Platform Management, Password Complexity subsection

NEW QUESTION 185
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

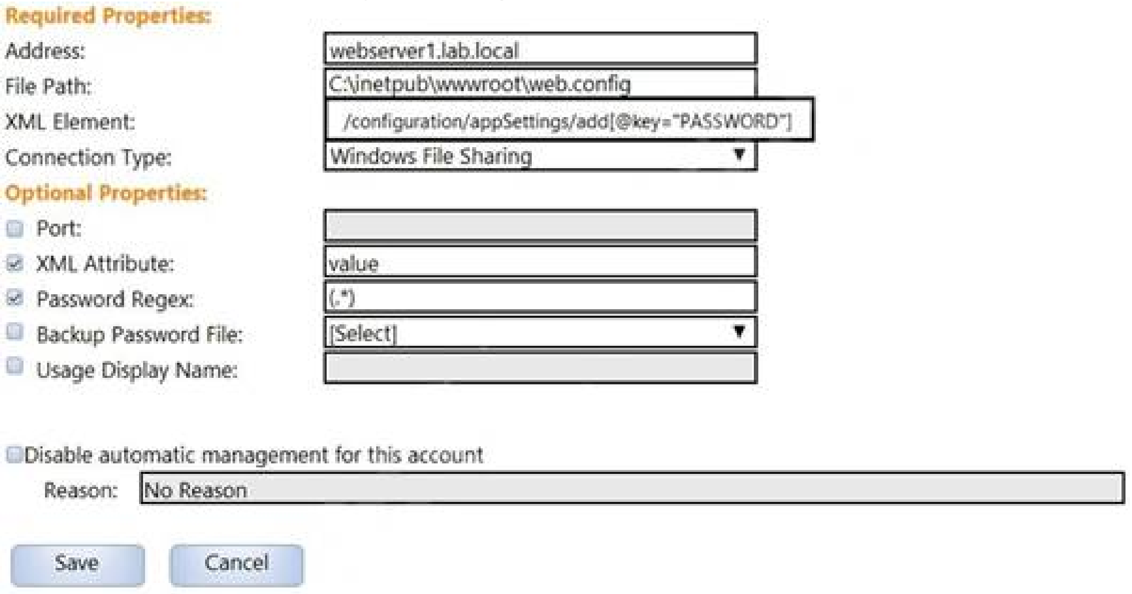
NEW QUESTION 186
In the Private Ark client, how do you add an LDAP group to a CyberArk group?

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 191
In the screenshot displayed, you just configured the usage in CyberArk and want to update its password.
What is the least intrusive way to accomplish this?



Required Properties:

Address:	webserver1.lab.local
File Path:	C:\inetpub\wwwroot\web.config
XML Element:	/configuration/appSettings/add[@key="PASSWORD"]
Connection Type:	Windows File Sharing ▼

Optional Properties:

□ Port:	
☑ XML Attribute:	value
☑ Password Regex:	(.*)
□ Backup Password File:	[Select] ▼
□ Usage Display Name:	

□ Disable automatic management for this account
Reason: No Reason

A. Use the “change” button on the usage’s details page.
B. Use the “change” button on the parent account’s details page.
C. Use the “sync” button on the usage’s details page.
D. Use the “reconcile” button on the parent account’s details page.

Answer: C

Explanation:
A usage is a configuration that allows CyberArk to manage passwords for files, such as XML or INI files, that are stored on remote machines. A usage is associated with a parent account, which is the account that has access to the file. To update the password of a usage, the least intrusive way is to use the “sync” button on the usage’s details page. This will synchronize the password value between the Vault and the file, without changing the actual password. The “change” button will initiate a password change process by the CPM, which will generate a new random password for the usage and the file. The “reconcile” button will initiate a password reconcile process by the CPM, which will use a reconcile account to reset the password of the usage and the file to the value stored in the Vault. References: Usages, Manage passwords for usages

NEW QUESTION 192
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 193
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 195
CyberArk recommends implementing object level access control on all Safes.

A. True
B. False

Answer: B

Explanation:
CyberArk does not recommend implementing object level access control on all Safes. According to the CyberArk documentation1, enabling object level access control impacts Vault performance. Therefore, it should be used only when necessary and with caution. Object level access control is useful when you need to give granular permissions to specific passwords or files in a Safe, regardless of the Safe level member authorizations. For example, you can use it to grant access to an external vendor or technician for a specific password only, without exposing any other passwords or files in the Safe. However, if you do not need this level of granularity, you can use the regular Safe member authorizations to control user access to the Safe and its contents.

NEW QUESTION 198
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 201
A Reconcile Account can be specified in the Master Policy.

A. TRUE
B. FALSE

Answer: B

Explanation:
A Reconcile Account is not specified in the Master Policy, but in the Platform settings. The Master Policy defines the general password management settings for all the accounts in the Vault, such as the frequency of password rotation and verification. The Platform settings define the specific password management settings for each type of target system, such as the password complexity and the Reconcile Account. References:
? Defender PAM course, Module 2: Password Management, Lesson 2: Master Policy and Platforms, slide 8
? Defender PAM course, Module 2: Password Management, Lesson 3: Reconcile and Logon Accounts, slide 2
? Defender PAM Sample Items Study Guide, Question 37
? CyberArk Privileged Access Security Documentation, Password Management - Master Policy
? CyberArk Privileged Access Security Documentation, Password Management - Platforms

NEW QUESTION 202
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 206
What is the purpose of the 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 long 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: A

Explanation:
The Interval setting in a CPM policy is used to control how often the CPM looks for System Initiated CPM work, such as password changes, verifications, and reconciliations. The Interval setting defines the frequency, in minutes, that the CPM will check the accounts that are associated with the policy and perform the required actions. For example, if the Interval is set to 60, the CPM will check the accounts every hour and change, verify, or reconcile the passwords according to the policy settings. The Interval setting does not affect User Initiated CPM work, such as manual password changes or retrievals, which are performed immediately upon request. The Interval setting also does not control how long 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 4: CPM Policy Settings
? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 5: Managing Passwords, Section: CPM Policy Settings, Subsection: Interval

NEW QUESTION 211
Which values are acceptable in the address field of an Account?

A. It must be a Fully Qualified Domain Name (FQDN)
B. It must be an IP address
C. It must be NetBIOS name
D. Any name that is resolvable on the Central Policy Manager (CPM) server is acceptable

Answer: D

Explanation:
The address field of an Account is used to identify the target system where the Account is located. The CPM uses this address to connect to the target system and perform password management operations. Therefore, the address field can be any name that is resolvable on the CPM server, such as a FQDN, an IP address, a NetBIOS name, or a custom name defined in the hosts file of the CPM server. References:
? Defender PAM Sample Items Study Guide, page 9, question 91
? CyberArk Privileged Access Security Implementation Guide, page 75, section “Address”

NEW QUESTION 212
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 214
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.

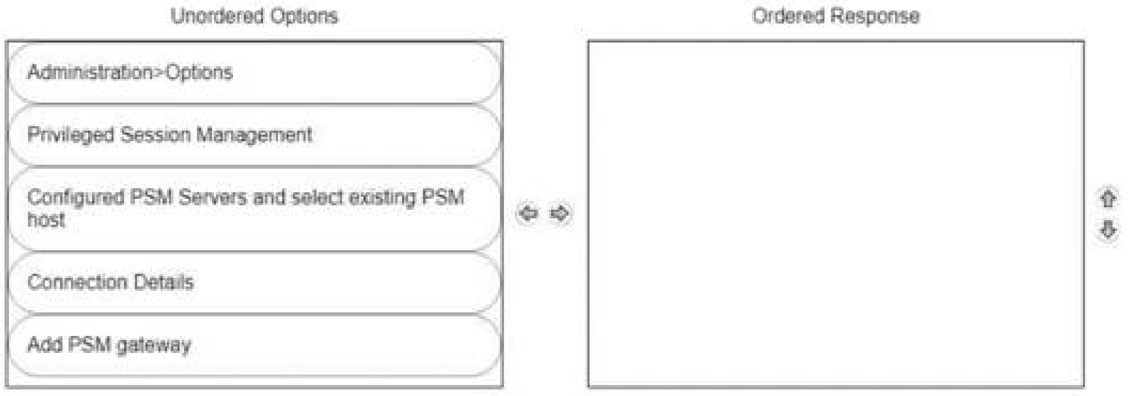
NEW QUESTION 219
How much disk space do you need on the server for a PAReplicate?

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

Answer: D

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

NEW QUESTION 222
DRAG DROP
A new HTML5 Gateway has been deployed in your organization.
From the PVWA, arrange the steps to configure a PSM host to use the HTML5 Gateway in the correct sequence.


Unordered Options
Administration>Options
Privileged Session Management
Configured PSM Servers and select existing PSM host
Connection Details
Add PSM gateway
Ordered Response

A. Mastered
B. Not Mastered

Answer: A

Explanation:
To configure a PSM host to use the HTML5 Gateway from the PVWA, you would typically follow these steps:
? Log into the PVWA with an administrative user.
? Navigate to Administration > Options.
? Right-click on Privileged Session Management and select Add Configured PSM Gateway Servers.
? Right-click Configured PSM Gateway Servers, then Add PSM Gateway Server.
? Select the newly added gateway server and enter a unique ID for the PSM HTML5 Gateway.

? Expand the newly created gateway server and enter the necessary configuration details.
Please note that these steps are based on general procedures for configuring a PSM host with an HTML5 Gateway and should be verified against the official CyberArk documentation or by a qualified CyberArk professional. For detailed instructions and best practices, refer to the CyberArk documentation123.

NEW QUESTION 224
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 229
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 231
In accordance with best practice, SSH access is denied for root accounts on UNIX/LINUX system. What is the BEST way to allow CPM to manage root accounts.

A. Create a privileged account on the target serve
B. Allow this account the ability to SSH directly from the CPM machin
C. Configure this account as the Reconcile account of the target server's root account.
D. Create a non-privileged account on the target serve
E. Allow this account the ability to SSH directly from the CPM machin
F. Configure this account as the Logon account of the target server's root account.
G. Configure the Unix system to allow SSH logins.
H. Configure the CPM to allow SSH logins.

Answer: B

Explanation:
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Using-Logon-Accounts-for-SSH-and- Telnet-Connections.htm?Highlight=logon%20account

NEW QUESTION 234
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 239
What is required to manage loosely connected devices?

A. PSM for SSH
B. EPM
C. PSM
D. PTA

Answer: B

Explanation:
To manage loosely connected devices, which are not always connected to the network, CyberArk uses the Endpoint Privilege Manager (EPM). EPM is capable of rotating credentials of accounts on Windows and macOS devices that are loosely connected to the enterprise network. It operates over the internet and can communicate with the corporate PVWA to retrieve the new password and change it on the device1. References: The information provided is based on general knowledge of CyberArk PAM
best practices and the management of loosely connected devices as outlined in CyberArk’s official documentation1.

NEW QUESTION 241
What is the purpose of the password change process?

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

Answer: B

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

NEW QUESTION 243
......