CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM

NEW QUESTION 1
Which parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests.

A. HeadStartInterval
B. Interval
C. ImmediateInterval
D. The CPM does not change the password under this circumstance

Answer: B

Explanation:
This parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests. It is set in the Master Policy under the Dual Control section. The value of this parameter determines the frequency of the CPM's verification process for accounts that have been accessed by users who have received confirmation from authorized Safe owners. The CPM will change the password of these accounts according to the value of this parameter. References:
? Dual Control - CyberArk
? Dual control in V10 Interface - docs.cyberark.com
? PAM-DEF CyberArk Defender – PAM

NEW QUESTION 2
A Vault Administrator team member can log in to CyberArk, but for some reason, is not given Vault Admin rights.
Where can you check to verify that the Vault Admins directory mapping points to the correct AD group?

A. PVWA > User Provisioning > LDAP Integration > Mapping Criteria
B. PVWA > User Provisioning > LDAP Integration > Map Name
C. PVWA > Administration > LDAP Integration > Mappings
D. PVWA > Administration > LDAP Integration > AD Groups

Answer: C

Explanation:
The directory mappings are the rules that define how users and groups from an external directory, such as Active Directory (AD), are mapped to roles and authorizations in CyberArk. To verify that the Vault Admins directory mapping points to the correct AD group, you need to check the Mappings page in the PVWA. This page displays the list of existing directory mappings in the Vault and their properties, such as mapping name, LDAP branch, domain groups, and mapping authorizations. You can edit or delete a directory mapping from this page, or create a new one using the Create Directory Mapping button. References: Directory Maps, Create directory mapping, Get directory mapping list

NEW QUESTION 3
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 4
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 5
The primary purpose of exclusive accounts is to ensure non-repudiation (Individual accountability).

A. TRUE
B. FALSE

Answer:

A

Explanation:
The primary purpose of exclusive accounts is to ensure non-repudiation (individual accountability). Exclusive accounts are accounts that can only be used by one user at a time, and are locked during usage. This means that no other user can access the same account until the current user releases it or the session expires. By using exclusive accounts, the organization can enforce individual accountability and traceability for the actions performed on the target systems. Exclusive accounts also reduce the risk of credential theft and unauthorized access, as the passwords are changed every time they
are retrieved by a user1. Exclusive accounts can be configured in the Master Policy under the Password Management section, by enabling the Exclusive Access rule2. References:
? 1: The Master Policy, One Time Password subsection
? 2: The Master Policy, Exclusive Access subsection

NEW QUESTION 6
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 7
Which of the Following can be configured in the Master Poky? Choose all that apply.

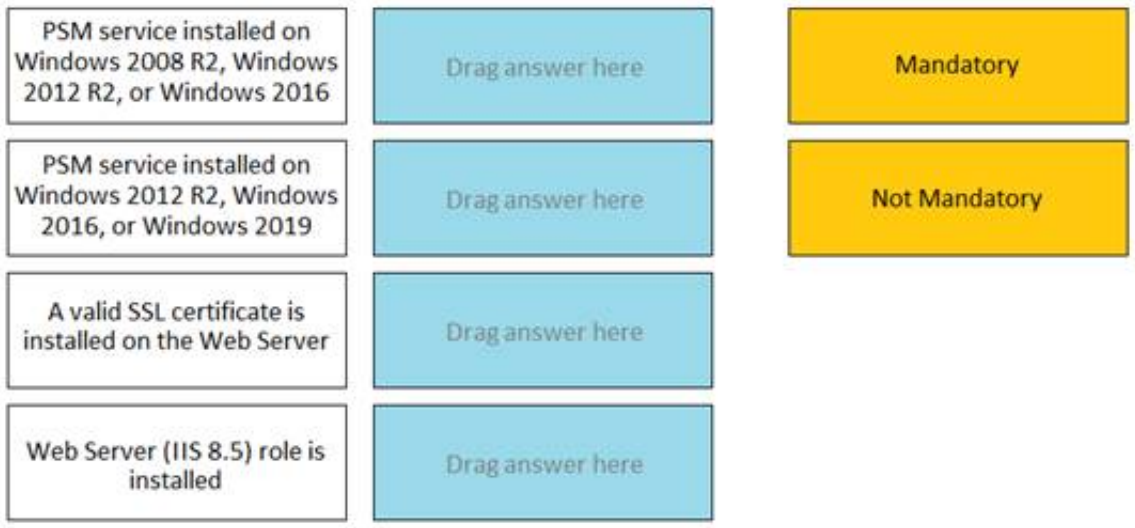
A. Dual Control
B. One Time Passwords
C. Exclusive Passwords
D. Password Reconciliation
E. Ticketing Integration
F. Required Properties
G. Custom Connection Components
H. Password Aging Rules

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 8
DRAG DROP
For each listed prerequisite, identify if it is mandatory or not mandatory to run the PSM Health Check.



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 9
The vault supports Role Based Access Control.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 10
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 10
Which Cyber Are components or products can be used to discover Windows Services or Scheduled Tasks that use privileged accounts? Select all that apply.

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

Answer: ABE

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

NEW QUESTION 15
To use PSM connections while in the PVWA, what are the minimum safe permissions a user or group will need?

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

Answer: B

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

NEW QUESTION 16
What does the minvalidity parameter on a platform policy determine?

A. time between a password retrieval and the account becoming eligible for a password change
B. timeout for users signed into the PVWA as configured in the global settings
C. minimum amount of time that Just in Time access is valid
D. time in minutes before an empty safe will be automatically deleted

Answer: A

Explanation:
The minvalidity parameter on a platform policy in CyberArk determines the minimum amount of time that must pass between the retrieval of a password and when the account becomes eligible for a password change. This parameter ensures that a user has a guaranteed period to use the password before it is changed again, providing stability and predictability in password management1. References: The information provided is based on general knowledge of CyberArk PAM best practices and the functionality of the minvalidity parameter as outlined in CyberArk's official documentation

NEW QUESTION 18
DRAG DROP
Match each key to its recommended storage location.

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 20
It is possible to restrict the time of day, or day of week that a [b]verify[/b] process can occur

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 21
You need to recover an account localadmin02 for target server 10.0.123.73 stored in Safe Team1.
What do you need to recover and decrypt the object? (Choose three.)

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

Answer: ABC

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

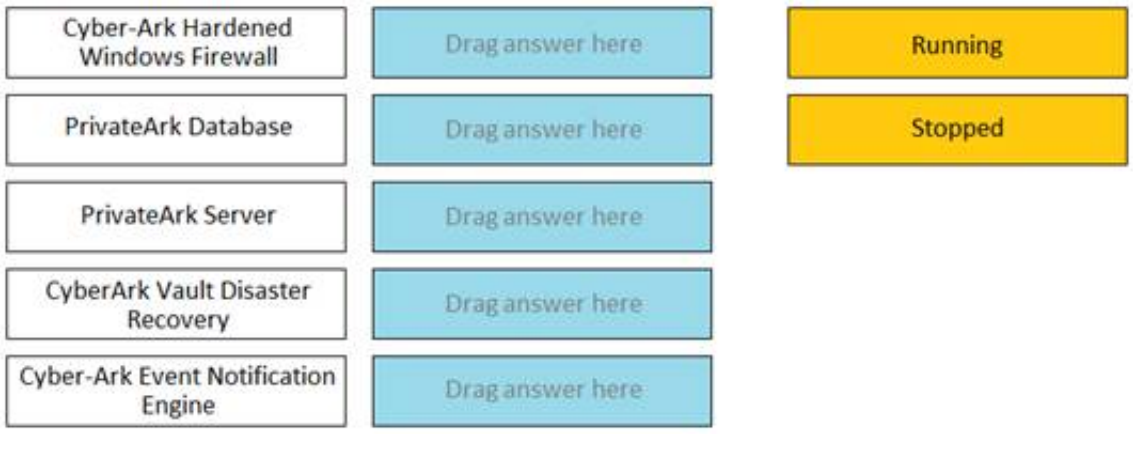
NEW QUESTION 22
Which master policy settings ensure non-repudiation?

A. Require password verification every X days and enforce one-time password access.
B. Enforce check-in/check-out exclusive access and enforce one-time password access.
C. Allow EPV transparent connections ('Click to connect') and enforce check-in/check-out exclusive access.
D. Allow EPV transparent connections ('Click to connect') and enforce one-time password access.

Answer: B

Explanation:
Non-repudiation in the context of CyberArk Master Policy settings refers to the assurance that a user cannot deny the validity of their actions. The settings that ensure non-repudiation are those that enforce accountability and traceability of actions. Enforcing check-in/check-out exclusive access ensures that only one user can access an account at a time, and their actions can be traced back to themEnforcing one-time password access means that passwords are used only once and then changed, which prevents the reuse of credentials and ties actions to specific instances of access12.
References:
? CyberArk Docs: Master Policy Rules2
? CyberArk Docs: The Master Policy1

NEW QUESTION 23
DRAG DROP
Match the Status of Service on a DR Vault to what is displayed when it is operating normally in Replication mode.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 25
Due to network activity, ACME Corp's PrivateArk Server became active on the OR Vault while the Primary Vault was also running normally. All the components continued to point to the Primary Vault.
Which steps should you perform to restore DR replication to normal?
A. Replicate data from DR Vault to Primary Vault > Shutdown PrivateArk Server on DR Vault > Start replication on DR vault
B. Shutdown PrivateArk Server on DR Vault > Start replication on DR vault
C. Shutdown PrivateArk Server on Primary Vault > Replicate data from DR Vault to Primary Vault > Shutdown PrivateArk Server on DR Vault > Start replication on DR vault
D. Shutdown PrivateArk Server on DR Vault > Replicate data from DR Vault to Primary Vault > Shutdown PrivateArk Server on DR Vault > Start replication on DR vault

Answer: B

Explanation:
To restore DR replication to normal after network activity caused the PrivateArk Server on the DR Vault to become active while the Primary Vault was also running, you should first shut down the PrivateArk Server on the DR Vault. This ensures that the DR Vault is no longer active and can be prepared for replication. After shutting down the server, you should then start the replication process on the DR Vault to synchronize the data from the Primary Vault1.
References:
? CyberArk's official documentation on initiating a DR failback to the Production
Vault provides a detailed procedure for restoring DR replication to normal1.
? Additional information on monitoring backup and DR replications can be found in CyberArk's documentation2.
? For further study and understanding of the CyberArk Defender PAM course objectives and documents, the official CyberArk training resources and study guides are recommended3.

NEW QUESTION 27
When a DR Vault Server becomes an active vault, it will automatically revert back to DR mode once the Primary Vault comes back online.

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

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

Answer: B

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

NEW QUESTION 31
CyberArk implements license limits by controlling the number and types of users that can be provisioned in the vault.

A. TRUE
B. FALSE

Answer: B

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

NEW QUESTION 33
Which certificate type do you need to configure the vault for LDAP over SSL?

A. the CA Certificate that signed the certificate used by the External Directory
B. a CA signed Certificate for the Vault server
C. a CA signed Certificate for the PVWA server
D. a self-signed Certificate for the Vault

Answer: A

Explanation:
To enable SSL-based encryption for LDAP integration, the Vault machine and the PVWA machine need to trust the certificate used by the External Directory. This can be achieved by importing the CA Certificate that signed the certificate used by the External Directory into the Windows certificate store on both the Vault and PVWA machines. This will facilitate an SSL connection between the Vault and the External Directory. References: Configure the Vault for LDAP, Configure LDAPS in CyberArk. What certificate I need to use?

NEW QUESTION 34
It is possible to leverage DNA to provide discovery functions that are not available with auto-detection.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 37
You have been asked to turn off the time access restrictions for a safe. Where is this setting found?

A. PrivateArk Client
B. RestAPI
C. PVWA
D. Vault

Answer: C

Explanation:
The setting to turn off the time access restrictions for a safe is found in the Password Vault Web Access (PVWA). The PVWA provides a web interface through which users can manage safes, including setting and modifying various safe properties such as access restrictions. By accessing the safe settings in the PVWA, you can adjust the time access restrictions as required1.
References:
? CyberArk Docs: Safe Settings1

NEW QUESTION 39
You have been asked to create an account group and assign three accounts which belong to a cluster. When you try to create a new group, you receive an unauthorized error; however, you are able to edit other aspects of the account properties.
Which safe permission do you need to manage account groups?

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

Answer: D

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

NEW QUESTION 44
A Logon Account can be specified in the Master Policy.

A. TRUE
B. FALSE

Answer: B

Explanation:
A Logon Account cannot be specified in the Master Policy. 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. A Logon Account is a technical setting that defines the account that the CPM uses to log on to a target system and perform password management tasks, such as changing, verifying, or reconciling passwords2. A Logon Account can be specified in the Platform Management settings, which are configured by the IT administrator for each platform2. The Platform Management settings are independent of the Master Policy and can be customized according to the organization's environment and security policies1. References:
? The Master Policy
? [Platform Management]

NEW QUESTION 49
You are creating a shared safe for the help desk.
What must be considered regarding the naming convention?

A. Ensure your naming convention is no longer than 20 characters.
B. Combine environments, owners and platforms to minimize the total number of safes created.
C. Safe owners should determine the safe name to enable them to easily remember it.
D. The use of these characters V:*<>".| is not allowed.

Answer: D

Explanation:
When creating a shared safe for the help desk in CyberArk's Privileged Access Management (PAM), it is important to adhere to the naming conventions set forth by CyberArk. One of the key considerations is that certain characters are not permitted in the safe name. Specifically, the characters V:*<>".| are not allowed in the naming of safes. This is to ensure compatibility and prevent issues with the file system or the CyberArk application itself, as these characters may interfere with normal operations or be reserved for specific functions within the operating system or the application.
References: The information regarding safe naming conventions is based on CyberArk's best practices and guidelines, which are detailed in the official CyberArk documentation and study guides. It is important to consult the CyberArk Defender PAM resources and documents to ensure compliance with these standards

NEW QUESTION 51
An auditor initiates a live monitoring session to PSM server to view an ongoing live session. When the auditor's machine makes an RDP connection the PSM server, which user will be used?

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

Answer: A

Explanation:
According to the web search results, when an auditor initiates a live monitoring session to PSM server to view an ongoing live session, the auditor's machine makes an RDP connection to the PSM server using the PSMAdminConnect user. The PSMAdminConnect user is a local or domain user that starts PSM sessions

on the PSM machine for authorized users who want to monitor or terminate active sessions1. The PSMAdminConnect user has limited permissions and access rights on the PSM server, and its credentials are managed by the CPM. The PSMAdminConnect user retrieves the credentials of the target account from the vault and uses them to establish a secure connection to the target machine. The auditor can then view the live session through the PSM session, while the PSM server records and audits the session activity.

NEW QUESTION 55
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 58
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 62
What is the easiest way to duplicate an existing platform?

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

Answer: B

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

NEW QUESTION 67
Which of the following files must be created or configured m order to run Password Upload Utility? Select all that apply.

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

Answer: ACD

Explanation:
To run the Password Upload Utility, you need to create or configure the following files:
? A comma delimited upload file: This is a text file that contains the passwords and
their properties that will be uploaded to the Vault. The file must have a .csv extension and follow a specific format. The first line in the file defines the names of the password properties as specified in the Password Vault. Every other line represents a single password object and its property values, according to the properties specified in the first line1.
? PACli.ini: This is a configuration file that stores the parameters for the PACli, which
is a command-line interface that enables communication between the Password Upload Utility and the Vault. The PACli.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: Vault, User, Password, and LogFile2.

? conf.ini: This is a configuration file that stores the parameters for the Password
Upload Utility. The conf.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: InputFile, LogFile, and ErrorFile3.
You do not need to create or configure the following file to run the Password Upload Utility:
? Vault.ini: This is a configuration file that stores the parameters for the Vault server, such as the database name, port, and password. This file is not used by the Password Upload Utility, and it is not located in the same folder as the Password Upload Utility executable file. The Vault.ini file is located in the Vault installation folder, and it is used by the Vault service and the PrivateArk Client4. References:
? 1: Create the Password File
? 2: PACli.ini
? 3: Password Upload Utility Parameter File (conf.ini)
? 4: [CyberArk Privileged Access Security Implementation Guide], Chapter 2: Installing the Vault, Section: Configuring the Vault, Subsection: Vault.ini

NEW QUESTION 72
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 77
If PTA is integrated with a supported SIEM solution, which detection becomes available?

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

Answer: D

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

NEW QUESTION 82
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 87
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 91
The vault supports Subnet Based Access Control.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 93
Where can you check that the LDAP binding is using TCP/636?

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

Answer: D

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

NEW QUESTION 97
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 100
DRAG DROP
Match each permission to where it can be found.

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 104
You created a new safe and need to ensure the user group cannot see the password, but can connect through the PSM.
Which safe permissions must you grant to the group? (Choose two.)

A. List Accounts Most Voted
B. Use Accounts Most Voted
C. Access Safe without Confirmation
D. Retrieve Files
E. Confirm Request

Answer: BD

Explanation:
To ensure that a user group can connect through the Privileged Session Manager (PSM) without seeing the password, you must grant the Use Accounts and Retrieve Files permissions to the group for the safe. TheUse Accounts permission allows users to initiate sessions using accounts without viewing the account details or
passwords. TheRetrieve Files permission enables users to retrieve files during PSM sessions without having access to the passwords1.
References:
? CyberArk Docs - Safe Permissions

NEW QUESTION 108
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 112
Which parameter controls how often the CPM looks for Soon-to-be-expired Passwords that need to be changed.

A. HeadStartInterval
B. Interval
C. ImmediateInterval
D. The CPM does not change the password under this circumstance

Answer: A

NEW QUESTION 116
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 118
Which change could CyberArk make to the REST API that could cause existing scripts to fail?

A. adding optional parameters in the request
B. adding additional REST methods
C. removing parameters
D. returning additional values in the response

Answer: C

Explanation:
Changes to the REST API that could cause existing scripts to fail include removing parameters. When parameters are removed from an API, scripts that rely on those parameters being present may no longer function correctly because they expect certain data to be available. This can lead to errors or unexpected behavior in the scripts that use the API1.
References:
? CyberArk Docs: REST APIs1

NEW QUESTION 120
In PVWA, you are attempting to play a recording made of a session by user jsmith, but there is no option to “Fast Forward” within the video. It plays and only allows you to skip between commands instead. You are also unable to download the video.
What could be the cause?

A. Recording is of a PSM for SSH session.
B. The browser you are using is out of date and needs an update to be supported.
C. You do not have the “View Audit” permission on the safe where the account is stored.
D. You need to update the recorder settings in the platform to enable screen capture every 10000 ms or less.

Answer: A

Explanation:
The inability to “Fast Forward” within a video recording in the PVWA and the restriction to only skip between commands suggests that the recording is of a PSM for SSH session. PSM for SSH sessions are typically recorded as text-based logs that capture command-level activities, which allows for skipping between commands but not fast- forwarding through a video timeline. Additionally, the lack of an option to download the video is consistent with the behavior of text-based session recordings, which do not provide a video file for download1.
References:
? CyberArk’s official documentation on Recorded Sessions, which explains the playback functionalities and limitations of different types of session recordings1.
? Information on configuring video and text recordings in PSM, which details how recordings are managed and the options available for different session types2.

NEW QUESTION 122
Within the Vault each password is encrypted by:

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

Answer: D

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

NEW QUESTION 124
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 127
Which is the primary purpose of exclusive accounts?

A. Reduced risk of credential theft
B. More frequent password changes
C. Non-repudiation (individual accountability)
D. To force a ‘collusion to commit’ fraud ensuring no single actor may use a password without authorization

Answer: D

Explanation:
According to the web search results, exclusive accounts are a feature of CyberArk Defender PAM that enables organizations to permit users to check out a ‘one-time’ password and lock it so that no other users can retrieve it at the same time1. After the user has used the password, the user checks the password back into the Vault. This ensures exclusive usage of the privileged account, enabling full control and tracking for the password. The duration of the check-out period can be configured in the platform settings for each account1.
The primary purpose of exclusive accounts is to prevent a single user from accessing a sensitive account without authorization, which could lead to fraud or misuse of privileges. By requiring a check-out and check-in process, exclusive accounts ensure that there is a ‘collusion to commit’ fraud, meaning that at least two users are involved in the malicious activity and are accountable for it. One user must check out the password and use it, while another user must approve the check-in and verify the password change. This way, exclusive accounts add an additional measure of protection and accountability for accessing sensitive accounts.

NEW QUESTION 129
Your customer, ACME Corp, wants to store the Safes Data in Drive D instead of Drive C. Which file should you edit?

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

Answer: A

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

NEW QUESTION 130
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 132
When should vault keys be rotated?

A. when it is copied to file systems outside the vault
B. annually
C. whenever a CyberArk user leaves the organization
D. when migrating to a new data center

Answer: D

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

NEW QUESTION 134
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?

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 136
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 137
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

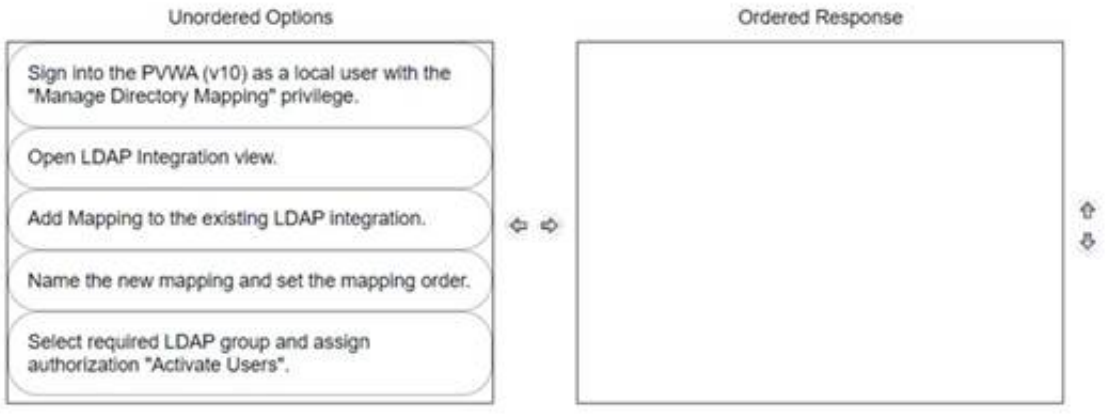
NEW QUESTION 138
To enable the Automatic response “Add to Pending” within PTA when unmanaged credentials are found, what are the minimum permissions required by PTAUser for the PasswordManager_pending safe?

A. List Accounts, View Safe members, Add accounts (includes update properties), Update Account content, Update Account properties
B. List Accounts, Add accounts (includes update properties), Delete Accounts, Manage Safe
C. Add accounts (includes update properties), Update Account content, Update Account properties, View Audit
D. View Accounts, Update Account content, Update Account properties, Access Safe without confirmation, Manage Safe, View Audit

Answer: A

Explanation:
To enable the automatic response “Add to Pending” within PTA when unmanaged credentials are found, the PTAUser needs to have the minimum permissions for the PasswordManager_pending safe as follows:
? List Accounts: This permission allows the PTAUser to view the accounts in the safe and their properties.
? View Safe members: This permission allows the PTAUser to view the members of the safe and their authorizations.
? Add accounts (includes update properties): This permission allows the PTAUser to add new accounts to the safe and update their properties, such as name, address, platform, and policy.
? Update Account content: This permission allows the PTAUser to update the password of the accounts in the safe.
? Update Account properties: This permission allows the PTAUser to update the properties of the existing accounts in the safe, such as name, address, platform, and policy.
These permissions are required for the PTAUser to be able to detect unmanaged privileged accounts and add them to the pending accounts queue in the PasswordManager_pending safe. The PTAUser also needs to have the same permissions for the PasswordManager_reconcile safe to enable the automatic response “Reconcile credentials” for suspicious password change events. References: Configure PTA Remediations, Safe Member Authorizations

NEW QUESTION 141
DRAG DROP
You have been asked to delegate the rights to unlock users to Tier 1 support. The Tier 1 support team already has an LDAP group for its members.
Arrange the steps to do this in the correct sequence.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 142
DRAG DROP
Match each PTA alert category with the PTA sensors that collect the data for it.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 143
Assuming a safe has been configured to be accessible during certain hours of the day, a Vault Admin may still access that safe outside of those hours.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 147
You notice an authentication failure entry for the DR user in the ITALog. What is the correct process to fix this error? (Choose two.)

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

Answer: AB

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

NEW QUESTION 148
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?

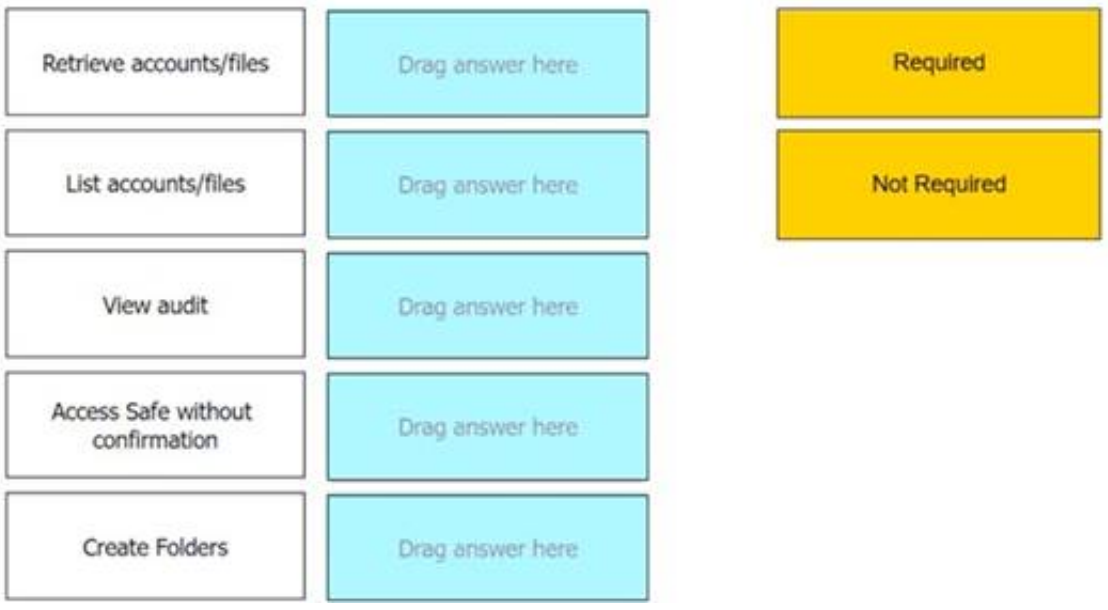
A. The account does not have sufficient permissions to change its own password.
B. The domain controller is unreachable.
C. The password has been changed recently and minimum password age is preventing the change.
D. The CPM service is disabled and will need to be restarted.

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 149
DRAG DROP
Which authorizations are required in a recording safe to allow a group to view recordings?

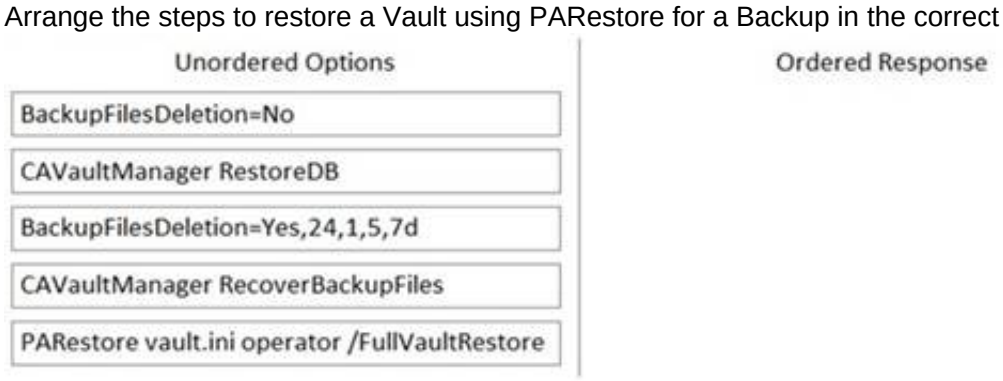


A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Retrieve accounts/files: Required
? List accounts/files: Required
? View audit: Required
? Access Safe without confirmation: Not Required
? Create Folders: Not Required
Comprehensive Explanation: To allow a group to view recordings in a recording safe, the required authorizations are Retrieve accounts/files, List accounts/files, and View audit.
These authorizations enable the group members to access and view the session recordings stored within the safe. The Retrieve accounts/files permission allows users to retrieve files during PSM sessions. The List accounts/files permission enables users to see the list of accounts and files within the safe. TheView audit authorization is necessary for users to view the audit records associated with the recordings1.
References:
? CyberArk Docs - Monitor Privileged Sessions

NEW QUESTION 152
DRAG DROP
Arrange the steps to restore a Vault using PARestore for a Backup in the correct sequence.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
BackupFilesDeletion=No
PARestore vault.ini operator /FullVaultRestore CAVaultManager RecoverBackupFiles CAVaultManager RestoreDB BackupFilesDeletion=Yes,24,1,5,7d
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Restoring-Safes-or-the-Vault.htm

NEW QUESTION 154
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 159
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

PAM-DEF Practice Exam Features:

* PAM-DEF Questions and Answers Updated Frequently

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

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

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