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

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 4
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
When the CPM connects to a database, which interface is most commonly used?

A. Kerberos

B. ODBC
C. VBScript
D. Sybase

Answer: B

Explanation:
The Central Policy Manager (CPM) in CyberArk most commonly uses the ODBC (Open Database Connectivity) interface when connecting to a database. ODBC is a standard API for accessing database management systems (DBMS). The CPM supports remote password management on all databases that support ODBC connections, and the machine running the CPM must support ODBC, version 2.7 and higher1. References:
? CyberArk Docs: Databases that support ODBC connections1

NEW QUESTION 6
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 7
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 8
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 9
In a rule using "Privileged Session Analysis and Response" in PTA, which session options are available to configure as responses to activities?

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

Answer: A

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

NEW QUESTION 10
When an account is unable to change its own password, how can you ensure that password reset with the reconcile account is performed each time instead of a change?

A. Set the parameter RCAllowManualReconciliation to Yes.
B. Set the parameter ChangePasswordinResetMade to Yes.
C. Set the parameter IgnoreReconcileOnMissingAccount to No.
D. Set the UnlockUserOnReconcile to Yes.

Answer: C

Explanation:
In CyberArk's Privileged Access Management (PAM), when an account cannot change its own password, setting the parameter IgnoreReconcileOnMissingAccount to No ensures that the reconcile account is used for password reset. This is because the reconcile account has the necessary permissions to reset the password when the primary account cannot do so. References: The information provided is based on general knowledge of CyberArk PAM best practices and is not taken from any specific CyberArk Defender PAM course or learning resources.

NEW QUESTION 10
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 13
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 16
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 17
Platform settings are applied to .

A. The entire vault.
B. Network Areas
C. Safes
D. Individual Accounts

Answer: D

Explanation:
Platform settings are applied to individual accounts. A platform is a set of parameters that defines how the Vault manages the passwords of accounts that belong to a certain operating system or application. Each account in the Vault is attached to a platform that determines how the account password is changed, verified, reconciled, and accessed. Platform settings can be customized to meet the specific requirements of each account type. For example, you can define the password complexity, rotation frequency, verification method, and access policy for each platform. References: [Defender PAM Sample Items Study Guide], page 15; [CyberArk Privileged Access Security Documentation], Platforms Overview.

NEW QUESTION 22
The Privileged Access Management solution provides an out-of-the-box target platform to manage SSH keys, called UNIX Via SSH Keys.
How are these keys managed?

A. CyberArk stores Private keys in the Vault and updates Public keys on target systems.
B. CyberArk stores Public keys in the Vault and updates Private keys on target systems.
C. CyberArk does not store Public or Private keys and instead uses a reconcile account to create keys on demand.
D. CyberArk stores both Private and Public keys and can update target systems with either key.

Answer: A

Explanation:
SSH keys are a way to authenticate to a target machine with a privileged account, and are subject to the same risks and challenges as privileged passwords. CyberArk provides an out-of-the-box target platform to manage SSH keys, called UNIX Via SSH Keys, which simplifies and automates SSH keys lifecycle management. This platform works as follows:
? CyberArk stores the private keys in the Vault, where they benefit from all the security and accessibility features of the Vault, such as encryption, auditing, and backup.
? CyberArk updates the public keys on the target systems, using a parent account that has access to the file that contains the public key, such as ~/.ssh/authorized_keys. CyberArk can generate new random SSH key pairs and update the public keys on the target systems according to the organizational policy, such as after a single use, after a predefined period, or manually.
? CyberArk can also verify that the private and public keys are synchronized, and reconcile them if they are not, using a reconcile account that can reset the SSH key pairs on the target systems.
References: Manage SSH Keys, Use SSH Keys

NEW QUESTION 25
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 28
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 29
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 34
Which of these accounts onboarding methods is considered proactive?

A. Accounts Discovery
B. Detecting accounts with PTA
C. A Rest API integration with account provisioning software
D. A DNA scan

Answer: C

Explanation:
A Rest API integration with account provisioning software is considered a proactive account onboarding method, because it enables the automatic creation and management of accounts in the Vault as soon as they are provisioned in the target systems. This way, the accounts are secured from the start and do not need to be discovered or onboarded manually later. A Rest API integration with account provisioning software can be achieved by using the CyberArk Accounts Feed REST API, which allows external applications to send account information to the Vault1.
The other options are not proactive account onboarding methods, because they rely on the discovery of existing accounts that may have been exposed or compromised before being onboarded to the Vault. Accounts Discovery is a feature that enables the Vault to scan target systems and identify privileged accounts that are not managed by the Vault2. Detecting accounts with PTA is a feature that enables the Privileged Threat Analytics (PTA) component to detect and alert on suspicious account activities and credential thefts3. A DNA scan is a feature that enables the Discovery and Audit (DNA) tool to scan Windows and Unix machines and generate a report on the privileged accounts and vulnerabilities found4.
References:
? CyberArk Accounts Feed REST API - CyberArk, section "CyberArk Accounts Feed REST API"
? Accounts Discovery - CyberArk, section "Accounts Discovery"
? Detect and Respond to Privileged Account Threats - CyberArk, section "Detect and Respond to Privileged Account Threats"
? CyberArk DNA - CyberArk, section "CyberArk DNA"

NEW QUESTION 36
To ensure all sessions are being recorded, a CyberArk administrator goes to the master policy and makes configuration changes.
Which configuration is correct?

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

Answer: C

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

NEW QUESTION 39
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 41
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 46
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 51
Users can be resulted to using certain CyberArk interfaces (e.g.PVWA or PACLI).

A. TRUE
B. FALSE

Answer: A

Explanation:
Users can be restricted to using certain CyberArk interfaces (e.g. PVWA or PACLI) by using the User Type property. The User Type property is a parameter that can be configured in the User Management settings for each user. The User Type property defines which interfaces the user can access the Vault through, such as PVWA, PrivateArk Client, PACLI, PSM, etc. The User Type property is determined by the CyberArk license and can be assigned to users when they are added to the Vault or when their properties are updated. For example, if a user is assigned the User Type of EPVUser, they can access the Vault through PVWA, PrivateArk Client, PrivateArk Webclient, PACLI, and
PIMSU. However, if a user is assigned the User Type of BizUser, they can only access the Vault through PVWA1. Therefore, by using the User Type property, administrators can control and restrict which CyberArk interfaces the users can use. References:
? 1: Manage users, Types of users subsection

NEW QUESTION 56
What are the minimum permissions to add multiple accounts from a file when using PVWA bulk-upload? (Choose three.)

A. add accounts
B. rename accounts
C. update account content
D. update account properties
E. view safe members
F. add safes

Answer: ACD

Explanation:
When using PVWA bulk-upload to add multiple accounts from a file, the minimum permissions required are to add accounts, update account content, and update account properties. These permissions ensure that the user has the ability to create new accounts in the Vault, modify the content of the accounts, and change their properties as necessary during the bulk-upload process1.
References:
? CyberArk Docs - Add multiple accounts from a file in V10 Interface

NEW QUESTION 58
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 60
What is the purpose of the HeadStartInterval setting m a platform?

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

Answer: B

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

NEW QUESTION 64
The Vault administrator can change the Vault license by uploading the new license to the system Safe.

A. True
B. False

Answer: A

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

NEW QUESTION 68
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 69
Which methods can you use to add a user directly to the Vault Admin Group? (Choose three.)

A. REST API
B. PrivateArk Client
C. PACLI
D. PVWA
E. Active Directory
F. Sailpoint

Answer: ABC

Explanation:
To add a user directly to the Vault Admin Group in CyberArk, you can use the following methods:
? REST API: The REST API allows for programmatic management of users and groups within the Vault, including adding users to the Vault Admin Group1.
? PrivateArk Client: The PrivateArk Client provides a graphical interface for managing users and groups, and it can be used to add users directly to the Vault

Admin Group2.
? PACLI: The PACLI (Privileged Access Command Line Interface) is a command- line tool that enables administrators to manage the Vault, including adding users to groups2.
These methods provide different ways to manage users and their group memberships within the CyberArk Vault, offering flexibility for administrators to choose the most suitable approach for their needs.
References:
? CyberArk's official documentation on using the REST API to manage users and groups1.
? Information on managing users and groups through the PrivateArk Client and PACLI2.

NEW QUESTION 72
Accounts Discovery allows secure connections to domain controllers.

A. TRUE
B. FALSE

Answer: B

NEW QUESTION 76
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 77
Before failing back to the production infrastructure after a DR exercise, what must you do to maintain audit history during the DR event?

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

Answer: A

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

NEW QUESTION 78
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 83
When running a "Privileged Accounts Inventory" Report through the Reports page in PVWA on a specific safe, which permission/s are required on that safe to show complete account inventory information?

A. List Accounts, View Safe Members

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

Answer: A

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

NEW QUESTION 84
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 85
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 90
PSM captures a record of each command that was executed in Unix.

A. TRIE
B. FALSE

Answer: A

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

NEW QUESTION 93
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 96
You are configuring CyberArk to use HTML5 gateways exclusively for PSM connections. In the PVWA, where do you set DefaultConnectionMethod to HTML5?

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

Answer: A

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

NEW QUESTION 99
For an account attached to a platform that requires Dual Control based on a Master Policy exception, how would you configure a group of users to access a password without approval.

A. Create an exception to the Master Policy to exclude the group from the workflow process.
B. Edith the master policy rule and modify the advanced' Access safe without approval' rule to include the group.
C. On the safe in which the account is stored grant the group the' Access safe without audit' authorization.
D. On the safe in which the account is stored grant the group the' Access safe without confirmation' authorization.

Answer: D

Explanation:
Dual Control is a feature that requires the approval of another user before accessing a password. It is based on a Master Policy rule that applies to all accounts attached to platforms that have this rule enabled. However, there may be situations where a group of users needs to access a password without approval, such as in an emergency or for troubleshooting purposes. In this case, an exception can be made by granting the group the 'Access safe without confirmation' authorization on the safe in which the account is stored. This authorization bypasses the Dual Control workflow and allows the group to retrieve the password without waiting for approval. However, the password retrieval will still be audited and recorded in the Vault.

NEW QUESTION 102
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
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 110
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 114
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 118
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 123
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 125
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 127
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 129
When onboarding multiple accounts from the Pending Accounts list, which associated setting must be the same across the selected accounts?

A. Platform
B. Connection Component
C. CPM
D. Vault

Answer: A

Explanation:
When onboarding multiple accounts from the Pending Accounts list, all the selected accounts must be associated with the same platform. This is necessary because the platform setting determines how the accounts will be managed within CyberArk, including the policies and behaviors that apply to those accounts. If

an account contains dependencies, those dependencies are automatically onboarded with the account. This ensures that all accounts and their dependencies are managed consistently and according to the correct policies1.
References:
? CyberArk's official documentation on Onboarding Accounts and SSH Keys1.

NEW QUESTION 132
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 137
In a default CyberArk installation, which group must a user be a member of to view the "reports" page in PVWA?

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

Answer: A

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

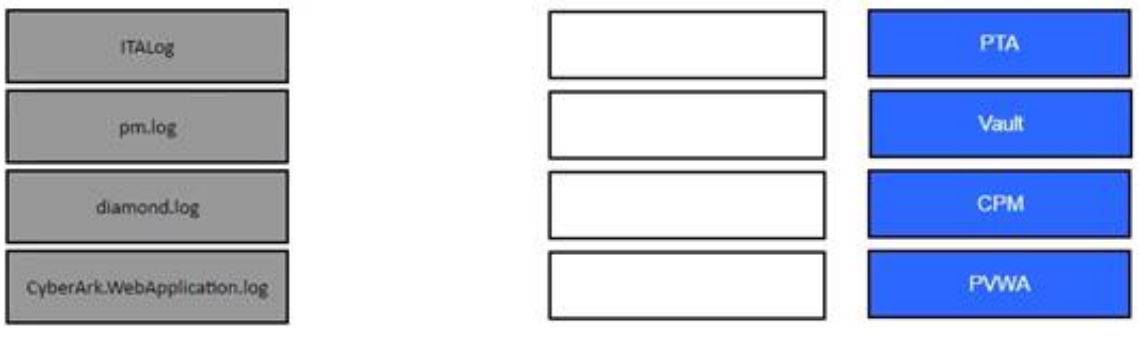
NEW QUESTION 141
Can the 'Connect' button be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied?

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 142
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 143
Customers who have the ‘Access Safe without confirmation’ safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.

A. TRUE
B. FALSE

Answer: B

Explanation:
Customers who have the ‘Access Safe without confirmation’ safe permission on a safe where accounts are configured for Dual control, do not need to request approval to use the account. The ‘Access Safe without confirmation’ safe permission allows users to access accounts without confirmation from authorized users, even if the Master Policy or an exception enforces Dual Control1. This means that users who have this permission can bypass the workflow process and access the account password or connect to the target system immediately. This permission can be granted to users or groups on a safe level by the safe owner or another user with the Manage Safe authorization2. References:
? 1: Dual Control, Advanced Settings subsection
? 2: CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section: Safe Authorizations, Table 2-1: Safe Authorizations

NEW QUESTION 148
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 152
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 155
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”

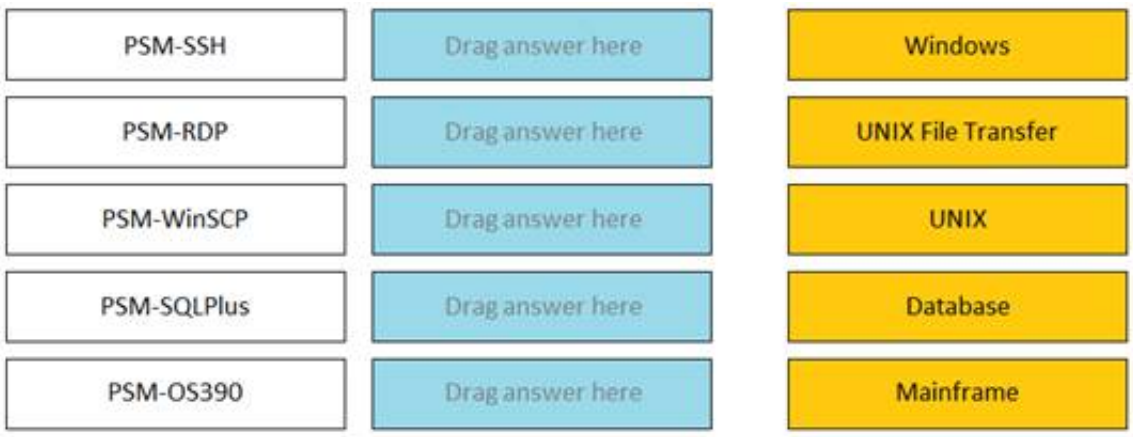
NEW QUESTION 159
You want to create a new onboarding rule. Where do you accomplish this?

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 163
DRAG DROP
Match the connection component to the corresponding OS/Function.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 166
Via Password Vault Web Access (PVWA), a user initiates a PSM connection to the target Linux machine using RemoteApp. When the client’s machine makes an RDP connection to the PSM server, which user will be utilized?

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

Answer: C

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

NEW QUESTION 171
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 173
Refer to the exhibit.

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

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

Answer: D

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

NEW QUESTION 178
Users who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.

A. TRUE
B. FALSE

Answer: B

Explanation:
Users who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, do not need to request approval to use the account. The 'Access Safe without confirmation' safe permission is a special permission that allows a user to bypass the Dual control mechanism and access the accounts in the safe without requiring confirmation from other authorized users. This permission can be useful for emergency situations or trusted users who need immediate access to the accounts. However, this permission also increases the risk of unauthorized or malicious access, so it should be granted with caution and monitored closely1.
References:
? 1: Access without confirmation

NEW QUESTION 183
Due to corporate storage constraints, you have been asked to disable session monitoring and recording for 500 testing accounts used for your lab environment. How do you accomplish this?

A. Master Policy>select Session Management>add Exceptions to the platform(s)>disable Session Monitoring and Recording policies
B. Administration>Platform Management>select the platform(s)>disable Session Monitoring and Recording Most Voted
C. Polices>Access Control (Safes)>select the safe(s)>disable Session Monitoring and Recording policies
D. Administration>Configuration Options>Options>select Privilege Session Management>disable Session Monitoring and Recording policies

Answer: D

Explanation:
To disable session monitoring and recording for a large number of accounts due to storage constraints, you would navigate to the Administration section of the CyberArk Privileged Access Security (PAS) solution, specifically to the Configuration Options. From there, you would select the Privilege Session Management (PSM) options and disable the Session Monitoring and Recording policies. This action would apply the changes to the specified accounts, thus disabling the session monitoring and recording features for them1. References: The answer is based on general knowledge of CyberArk PAS and best practices for managing session policies within the system. For specific steps and detailed procedures, please refer to the official CyberArk Defender PAM course materials and documentation

NEW QUESTION 187
Which file must be edited on the Vault to configure it to send data to PTA?

A. dbparm.ini
B. PARAgent.ini
C. my.ini
D. padr.ini

Answer: A

Explanation:
To configure the CyberArk Vault to send data to Privileged Threat Analytics (PTA), you must edit the dbparm.ini file on the Vault. This file contains parameters that specify how the Vault should forward syslog events to PTA, ensuring that the Vault can send secured syslog data to PTA for analysis and threat detection1.
References:
? CyberArk Docs: Configure Vault Trusted Connection to PTA2
? Netenrich: CyberArk Vault via Syslog1

NEW QUESTION 191
A user with administrative privileges to the vault can only grant other users privileges that he himself has.

A. TRUE
B. FALSE

Answer: B

Explanation:
A user with administrative privileges to the vault can grant other users privileges that he himself does not have, as long as he has the Authorize Users authorization on the Vault. The Authorize Users authorization enables a user to add or remove other users or groups as Vault members, and assign or revoke their authorizations. A user with this authorization can grant any privilege to any other user or group, regardless of his own privileges. However, this authorization does not allow a user to change his own privileges or the privileges of other users who have the same authorization1.
References:
? 1: Vault Member Authorizations

NEW QUESTION 194
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 196
If the AccountUploader Utility is used to create accounts with SSH keys, which parameter do you use to set the full or relative path of the SSH private key file that will be attached to the account?

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

Answer: B

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

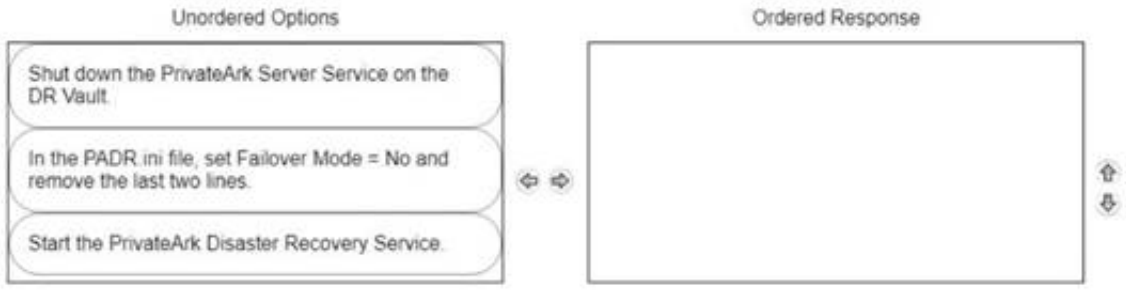
NEW QUESTION 198
To manage automated onboarding rules, a CyberArk user must be a member of which group?

A. Vault Admins
B. CPM User
C. Auditors
D. Administrators

Answer: A

Explanation:
To manage automated onboarding rules in CyberArk, a user must be a member of the Vault Admins group. This group has the necessary permissions to create and manage predefined rules that automatically onboard newly discovered accounts, which helps minimize the time it takes to onboard and securely manage accounts, reduces the time spent on reviewing pending accounts, and prevents human errors that may occur during manual onboarding1.
References:
? CyberArk's official documentation on onboarding rules provides detailed information on the groups required to manage these rules, including the Vault Admins group1.

NEW QUESTION 202
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.



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 206
According to CyberArk, which issues most commonly cause installed components to display as disconnected in the System Health Dashboard? (Choose two.)

A. network instabilities/outages
B. vault license expiry

C. credential de-sync
D. browser compatibility issues
E. installed location file corruption

Answer: AC

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

NEW QUESTION 209
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 214
What is the purpose of the PrivateArk Server service?

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

Answer: C

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

NEW QUESTION 217
What is the purpose of the Immediate Interval setting in a CPM policy?

A. To control how often the CPM looks for System Initiated CPM work.
B. To control how often the CPM looks for User Initiated CPM work.
C. To control how often the CPM rests between password changes.
D. To Control the maximum amount of time the CPM will wait for a password change to complete.

Answer: B

Explanation:
The Immediate Interval setting in a CPM policy is used to control how often the CPM looks for User Initiated CPM work, such as manual password changes, retrievals, or requests. The Immediate Interval setting defines the frequency, in minutes, that the CPM will check the accounts that are associated with the policy and perform the actions that were initiated by the users. For example, if the Immediate Interval is set to 2, the CPM will check the accounts every 2 minutes and change, retrieve, or authorize the passwords according to the user requests. The Immediate Interval setting does not affect System Initiated CPM work, such as password changes, verifications, or reconciliations that are triggered by the policy settings, such as Expiration Period or One Time Password. These actions are controlled by the Interval setting in the CPM policy. The Immediate Interval setting also does not control how often the CPM rests between password changes or

the maximum amount of time the CPM will wait for a password change to complete. These parameters are configured in the CPM.ini file, which is stored in the root folder of the <CPM username> Safe. References:
? [Defender PAM eLearning Course], Module 5: Password Management, Lesson 5.1: CPM Policies, Slide 9: CPM Policy Settings
? [Defender PAM Sample Items Study Guide], Question 6: CPM Policy Settings
? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 5: Managing Passwords, Section: CPM Policy Settings, Subsection: Immediate Interval

NEW QUESTION 220
During a High Availability node switch you notice an error and the Cluster Vault Manager Utility fails back to the original node.
Which log files should you check to investigate the cause of the issue? (Choose three.)

A. CyberArk Webconsole.log
B. VaultDB.log
C. PM_Error.log
D. ITALog.log
E. ClusterVault.console.log
F. logiccontainer.log

Answer: BCE

Explanation:
During a High Availability (HA) node switch, if an error occurs and the Cluster Vault Manager Utility fails back to the original node, you should check the following log files to investigate the cause of the issue:
? VaultDB.log: This log file contains information related to the database operations within the CyberArk Vault. It can provide insights into any issues that may have occurred during the database transactions at the time of the node switch1.
? PM_Error.log: The PM_Error.log file records errors encountered by the Password Manager (PM) during its operations. This log can help identify any issues related to password management that might have contributed to the failure of the node switch1.
? ClusterVault.console.log: The ClusterVault.console.log file includes error, warning, and information messages from the CyberArk Digital Cluster Vault. It is used for advanced troubleshooting and can reveal details about the error that caused the failback to the original node2.
References:
? CyberArk Docs - Troubleshooting High Availability issues1
? CyberArk Docs - Monitoring the CyberArk Digital Cluster Vault Server2

NEW QUESTION 223
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 224
Which Master Policy Setting must be active in order to have an account checked-out by one user for a pre-determined amount of time?

A. Require dual control password access Approval
B. Enforce check-in/check-out exclusive access
C. Enforce one-time password access
D. Enforce check-in/check-out exclusive access & enforce one-time password access

Answer: B

Explanation:
According to the CyberArk Defender PAM documentation, the Master Policy setting that must be active in order to have an account checked-out by one user for a pre- determined amount of time is Enforce check-in/check-out exclusive access. This setting 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 time. 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 account. References:
? Account check-out and check-in - CyberArk
? Master Policy - CyberArk

NEW QUESTION 228
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 229
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 234
A new colleague created a directory mapping between the Active Directory groups and the Vault.
Where can the newly Configured directory mapping be tested?

A. Connect to the Active Directory and ensure the organizational unit exists.
B. Connect to Sailpoint (or similar tool) to ensure the organizational unit is correctly named; log in to the PVWA with "Administrator" and confirm authentication succeeds.
C. Search for members that exist only in the mapping group to grant them safe permissions through the PVWA.
D. Connect to the PrivateArk Client with the Administrator Account to see if there is a user in the Vault Admin Group.

Answer: C

Explanation:
The newly configured directory mapping can be tested by searching for members that exist only in the mapping group to grant them safe permissions through the PVWA (Privileged Vault Web Access). This process allows you to verify that the directory mapping is functioning correctly by ensuring that only the intended users, who are part of the specific Active Directory group, are granted access to the safes in the CyberArk Vault12.
References:
? CyberArk Docs - Create directory mapping1
? CyberArk Docs - Edit directory mapping3
? CyberArk Docs - LDAP Integration in PVWA

NEW QUESTION 239
Which statement is true about setting the reconcile account at the platform level?

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

Answer: C

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

NEW QUESTION 244
You are onboarding an account that is not supported out of the box. What should you do first to obtain a platform to import?

A. Create a service ticket in the customer portal explaining the requirements of the custom platform.
B. Search common community portals like stackoverflow, reddit, github for an existing platform.
C. From the platforms page, uncheck the “Hide non-supported platforms” checkbox and see if a platform meeting your needs appears.
D. Visit the CyberArk marketplace and search for a platform that meets your needs.

Answer: D

Explanation:
The CyberArk marketplace is a platform that simplifies delivery of privileged access security solutions, such as CyberArk Privileged Account Security Solution. It features the industry's broadest and deepest portfolio of technology integrations, including platforms for various types of accounts. Customers can find and deploy integrations with CyberArk Marketplace in as little as four clicks. If there is no platform that meets the customer's needs, they can request a custom platform from CyberArk or create their own using the Platform Development Kit (PDK). References: CyberArk Marketplace, Platform Development Kit

NEW QUESTION 249
Which command generates a full backup of the Vault?

A. PAReplicate.exe Vault.ini /LogonFromFile user.ini /FullBackup
B. PAPreBackup.exe C:\PrivateArk\Server\Conf\Vault.ini Backup/Asdf1234 /full
C. PARestore.exe PADR ini /LogonFromFile vault.ini /FullBackup
D. CAVaultManager.exe RecoverBackupFiles /BackupPoolName BkpSvr1

Answer: A

Explanation:
The command PAReplicate.exe with the /FullBackup option is used to generate a full backup of the CyberArk Vault. This command requires the Vault configuration file (typically Vault.ini) and a credential file (specified with /LogonFromFile) that contains the user's encrypted logon credentials. The /FullBackup option indicates that a full backup of the Vault is to be performed, as opposed to an incremental backup1. References:
? CyberArk Docs: Install the Vault Backup Utility2
? CyberArk Knowledge Article: PAReplicate Configuration and Usage

NEW QUESTION 253
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 258
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 259
Time of day or day of week restrictions on when password verifications can occur configured in .

A. The Master Policy
B. The Platform settings
C. The Safe settings
D. The Account Details

Answer: C

Explanation:
Time of day or day of week restrictions on when password verifications can occur are configured in the Safe settings. This is a security feature that prevents Safes from being opened except at certain times (e.g., 8 a.m. to 5 p.m.). If a user tries to enter at a time that has not been designated for access, they will receive a message that informs them that the Safe is unavailable. References: Advanced Safe Management

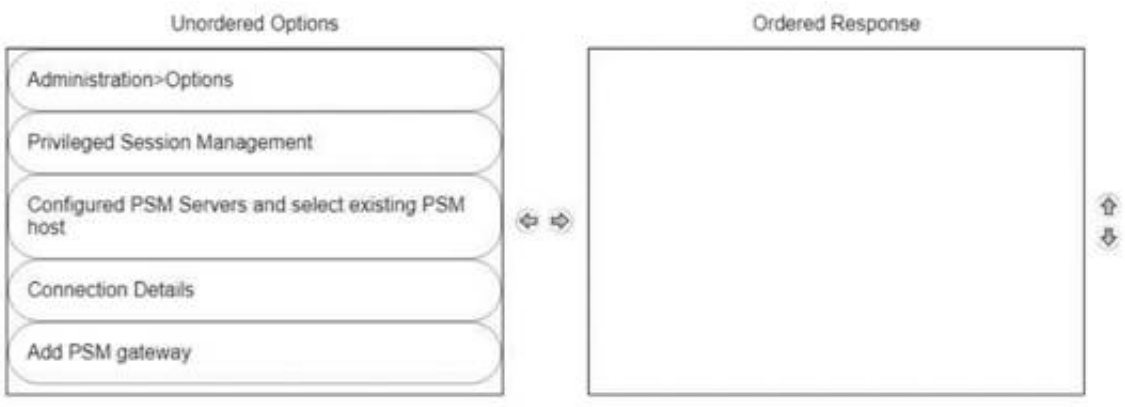
NEW QUESTION 260
How much disk space do you need on the server for a PAReplicate?

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 265
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.



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 269
You have been asked to identify the up or down status of Vault services. Which CyberArk utility can you use to accomplish this task?

A. Vault Replicator
B. PAS Reporter
C. Remote Control Agent
D. Syslog

Answer: C

Explanation:
The Remote Control Agent (PARAgent) is a CyberArk utility that can be used to monitor the status of Vault services remotely. It can also perform other tasks, such as starting and stopping the Vault, backing up and restoring the Vault, and running other utilities. The PARAgent communicates with the Remote Control Client (PARClient), which is a graphical user interface that displays the Vault status and allows the user to execute commands on the Vault. The PARAgent can also send SNMP traps to a remote terminal if the Vault service is down. References: How do I monitor the Vault status remotely?, Monitor system health

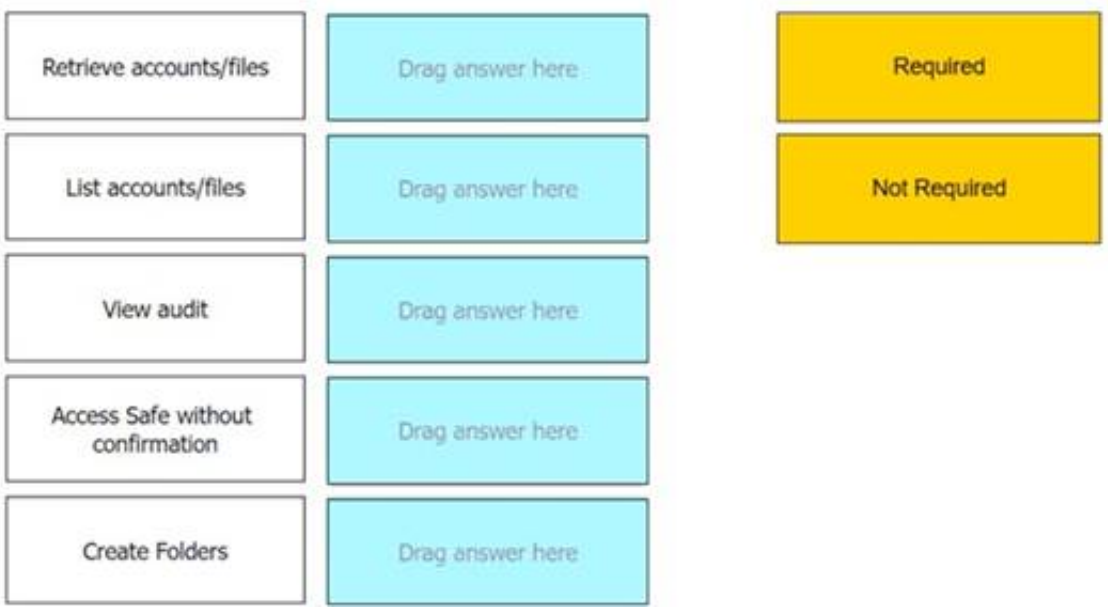
NEW QUESTION 273
When Dual Control is enabled a user must first submit a request in the Password Vault Web Access (PVWA) and receive approval before being able to launch a secure connection via PSM for Windows (previously known as RDP Proxy).

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 275
DRAG DROP
Which authorizations are required in a recording safe to allow a group to view recordings?

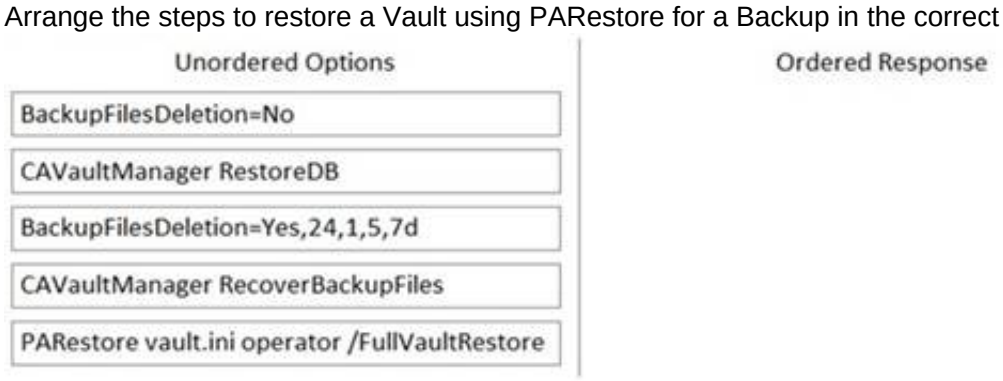


A. Mastered
B. Not Mastered

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 280
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 281
You have associated a logon account to one your UNIX cool accounts in the vault. When attempting to [b]change [/b] the root account's password the CPM will…..

A. Log in to the system as root, then change root's password

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

Answer: C

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

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

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

NEW QUESTION 286
Which report provides a list of account stored in the vault.

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

Answer: A

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

NEW QUESTION 290
.....

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