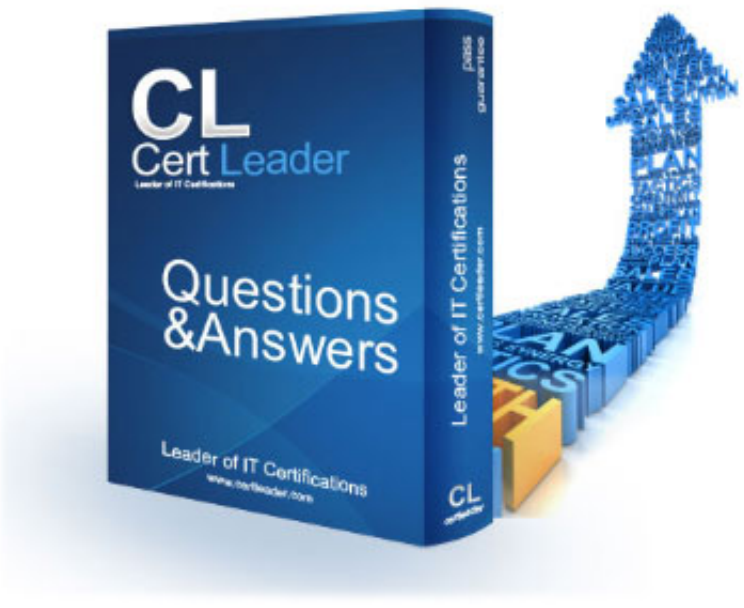
PAM-DEF Dumps

CyberArk Defender - PAM

https://www.certleader.com/PAM-DEF-dumps.html



NEW QUESTION 1
The primary purpose of exclusive accounts is to ensure non-repudiation (Individual accountability).

A. TRUE
B. FALSE

Answer: A

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

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

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

Answer: B

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

NEW QUESTION 3
Which parameters can be used to harden the Credential Files (CredFiles) while using CreateCredFile Utility? (Choose three.)

A. Operating System Username
B. Host IP Address
C. Client Hostname
D. Operating System Type (Linux/Windows/HP-UX)
E. Vault IP Address
F. Time Frame

Answer: BCE

Explanation:
When using the CreateCredFile Utility to harden Credential Files (CredFiles), it is important to include parameters that enhance security. The Host IP Address, Client Hostname, and Vault IP Address are parameters that can be used to specify the environment in which the CredFile is valid, thereby restricting its use to specific machines or networks1. This helps prevent unauthorized access to the CredFile and ensures that it is only used in the intended context.
References:
? CyberArk’s official documentation on the CreateCredFile utility provides insights into the security mechanisms used to protect credential files, including the use of environmental key materials such as application-based, machine-based, and component-based materials1.
? For a deeper understanding of how to secure Credential Files and the use of the CreateCredFile Utility, refer to the CyberArk Defender PAM course materials and study guide2.

NEW QUESTION 4
Which of the following Privileged Session Management (PSM) solutions support live monitoring of active sessions?

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

Answer: D

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

NEW QUESTION 5
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 6
A user is receiving the error message "ITATS006E Station is suspended for User jsmith" when attempting to sign into the Password Vault Web Access (PVWA). Which utility would a Vault administrator use to correct this problem?

A. createcredfile.exe
B. cavaultmanager.exe
C. PrivateArk
D. PVWA

Answer: C

Explanation:
The PrivateArk is a utility that allows the Vault administrator to access and manage the Vault data, users, groups, policies, and settings. The PrivateArk can be used to correct the problem of a user receiving the error message "ITATS006E Station is suspended for User jsmith" when attempting to sign into the PVWA. The error message means that the user has exceeded the number of invalid password attempts and has been locked out from the Vault. To unlock the user, the Vault administrator can use the PrivateArk to activate the suspended station for the user in the Trusted Net Areas1.
The other options are not utilities that can be used to correct this problem. The createcredfile.exe is a utility that creates a credential file for the CPM to connect to the target systems2. The cavaultmanager.exe is a utility that performs various Vault maintenance tasks, such as backup, restore, and encryption3. The PVWA is not a utility, but a web interface that allows the users to access and use the Vault features, such as
managing accounts, requesting passwords, and initiating sessions. References:
? Vault - ITATS006E Station is suspended for User Administrator - force.com, section "Resolution"
? Create a Credential File - CyberArk, section "Create a Credential File"
? Vault Maintenance - CyberArk, section "Vault Maintenance"
? [Password Vault Web Access - CyberArk], section "Password Vault Web Access"

NEW QUESTION 7
What is required to enable access over SSH to a Unix account through both PSM and PSMP?

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

Answer: A

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

NEW QUESTION 8
As long as you are a member of the Vault Admins group you can grant any permission on any safe.

A. TRUE
B. FALSE

Answer: B

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

? Safe member authorizations

NEW QUESTION 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
You want to give a newly-created group rights to review security events under the Security pane. You also want to be able to update the status of these events. Where must you update the group to allow this?

A. in the PTAAuthorizationGroups parameter, found in Administration > Options > PTA
B. in the PTAAuthorizationGroups parameter, found in Administration > Options > General
C. in the SecurityEventsAuthorizationGroups parameter, found in Administration > Security> Options
D. in the SecurityEventsFeedAuthorizationGroups parameter, found in Administration > Options > General

Answer: D

Explanation:
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security- Events.htm?TocPath=End%20User%7CSecurity%20Events%7C2#Permissions

NEW QUESTION 10
Which of the following statements are NOT true when enabling PSM recording for a target Windows server? (Choose all that apply)

A. The PSM software must be instated on the target server
B. PSM must be enabled in the Master Policy (either directly, or through exception)
C. PSMConnect must be added as a local user on the target server
D. RDP must be enabled on the target server

Answer: AC

Explanation:
The following statements are not true when enabling PSM recording for a target Windows server:
? A. The PSM software must be instated on the target server. This is not true, because the PSM software is installed on a dedicated server that acts as a proxy between the user and the target server. The PSM server intercepts the user’s connection request, initiates the connection to the target server, and records the privileged session. The target server does not need to have the PSM software installed on it1.
? C. PSMConnect must be added as a local user on the target server. This is not true, because PSMConnect is a predefined user that is created on the PSM server during the installation. This user is used to establish the connection between the PSM server and the target server, and to run the PSM processes. The target server does not need to have a local user named PSMConnect on it2.
The following statements are true when enabling PSM recording for a target Windows server:
? B. PSM must be enabled in the Master Policy (either directly, or through exception). This is true, because the Master Policy is a centralized overview of the security and compliance policy of privileged accounts in the organization. It allows the administrator to configure compliance driven rules that are defined as the baseline for the enterprise. One of the rules in the Master Policy is the Session Isolation rule, which determines whether or not privileged sessions are isolated and recorded by PSM. This rule can be enabled either directly in the Master Policy, or through an exception for a specific scope of accounts3.
? D. RDP must be enabled on the target server. This is true, because RDP is the protocol that is used by PSM to connect to Windows servers. The target server must have RDP enabled and configured properly to allow the PSM server to access it. The PSM server must also have the RDP client installed on it4.
References:
? 1: Privileged Session Manager
? 2: PSMConnect and PSMAdminConnect
? 3: Session Isolation
? 4: Configure RDP for PSM

NEW QUESTION 14
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 15
Which command configures email alerts within PTA if settings need to be changed post install?

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

Answer: A

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

NEW QUESTION 20
Which statement about the Master Policy best describes the differences between one-time password and exclusive access functionality?

A. Exclusive access means that only a specific group of users may use the accoun
B. After an account on a one-time password platform is used, the account is deleted from the safe automatically.
C. Exclusive access locks the account indefinitel
D. One-time password can be used replace invalid account passwords.
E. Exclusive access is enabled by default in the Master Polic
F. One-time password should only be enabled for emergencies.
G. Exclusive access allows only one person to check-out an account at a tim
H. One-time password schedules an account for a password change after the MinValidityPeriod period expires.

Answer: D

Explanation:
The Master Policy in CyberArk defines the behavior of one-time passwords and exclusive accessExclusive access ensures that only one user can check out an account at any given time, effectively locking the account during its use to prevent simultaneous access1. On the other hand, one-time password functionality is designed to change the account's password after it is used, based on a timer set by the MinValidityPeriod parameter in the policy file. This means that once the password is checked out and the timer expires, the Central Policy Manager (CPM) will change the password2. These settings are often used together to maintain accountability and security for the usage of shared privileged accounts. References:
? CyberArk Docs: One-time passwords and exclusive accounts1
? CyberArk Knowledge Article: CPM: What is the difference between "One Time" and "Exclusive" passwords?2

NEW QUESTION 21
What does the minvalidity parameter on a platform policy determine?

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

Answer: A

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

NEW QUESTION 23
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 27
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 30
It is possible to restrict the time of day, or day of week that a [b]verify[/b] process can occur

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 33
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 36
If a password is changed manually on a server, bypassing the CPM, how would you configure the account so that the CPM could resume management automatically?

A. Configure the Provider to change the password to match the Vault's Password
B. Associate a reconcile account and configure the platform to reconcile automatically
C. Associate a logon account and configure the platform to reconcile automatically
D. Run the correct auto detection process to rediscover the password

Answer: B

Explanation:
A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the account that has been changed manually, the CPM can use the reconcile account to restore the password of the account to the value that is stored in the Vault, in case it is changed or out of sync. This process is called password reconciliation and it ensures that the passwords are synchronized and available for use. To configure the account so that the CPM can resume management automatically, the platform that the account belongs to must have the following parameters set1:
? RCAutomaticReconcileWhenUnsynched: This parameter determines whether passwords will be reconciled automatically after the CPM detects a password on a remote machine that is not synchronized with its corresponding password in the Vault. The acceptable values are Yes or No.
? RCReconcileReasons: This parameter determines the codes that represent the CPM plugin errors that will launch a reconciliation process. The acceptable values are plug-in return codes separated by a comma.
? RCFromHour, RCToHour: These parameters determine the time frame in hours during which the CPM can reconcile passwords, either manually or automatically. The acceptable values are 0-23 or -1 for none.
? RCExecutionDays: This parameter determines the days of the week when the CPM will reconcile passwords. The acceptable values are days of the week, separated by commas.
References:
? 1: Password Reconciliation

NEW QUESTION 38
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 41
Which user is automatically added to all Safes and cannot be removed?

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

Answer: C

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

NEW QUESTION 46
Which combination of Safe member permissions will allow end users to log in to a remote machine transparently but NOT show or copy the password?

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

Answer: B

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

NEW QUESTION 51
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 54
How does the Vault administrator apply a new license file?

A. Upload the license.xml file to the system Safe and restart the PrivateArk Server service
B. Upload the license.xml file to the system Safe
C. Upload the license.xml file to the Vault Internal Safe and restart the PrivateArk Server service
D. Upload the license.xml file to the Vault Internal Safe

Answer: C

Explanation:
According to the CyberArk Defender PAM documentation1, the Vault administrator can apply a new license file by uploading the license.xml file to the Vault Internal Safe and restarting the PrivateArk Server service. The Vault Internal Safe is a special Safe that contains the Vault configuration files, including the license file. The Vault administrator can access this Safe from the PrivateArk Client and replace the existing license file with the new one. After that, the Vault administrator must restart the PrivateArk Server service for the changes to take effect. This procedure can be done either from the Vault machine or from a remote machine.
References:
? Manage the CyberArk License - CyberArk

NEW QUESTION 55
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 58
Which certificate type do you need to configure the vault for LDAP over SSL?

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

Answer: A

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

NEW QUESTION 59
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 64
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 67
Accounts Discovery allows secure connections to domain controllers.

A. TRUE
B. FALSE

Answer: B

NEW QUESTION 71
If a user is a member of more than one group that has authorizations on a safe, by default that user is granted .

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

Answer: D

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

NEW QUESTION 75
A password compliance audit found:
1) One-time password access of 20 domain accounts that are members of Domain Admins group in Active Directory are not being enforced.
2) All the sessions of connecting to domain controllers are not being recorded by CyberArk PSM.
What should you do to address these findings?

A. Edit the Master Policy and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
B. Edit safe properties and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
C. Edit CPM Settings and add two policy exceptions: enable "Enforce one-time password access", enable "Record and save session activity".
D. Contact the Windows Administrators and request them to add two policy exceptions at Active Directory Level: enable "Enforce one-time password access", enable "Record and save session activity".

Answer: A

Explanation:
To address the findings of the password compliance audit, you should edit the Master Policy in CyberArk Privileged Access Manager. The Master Policy is where you can enforce one-time password access and record session activity. One-time password access ensures that each password is used only once and then changed, which is a security measure to prevent unauthorized reuse of passwords1. Recording session activity is a feature of the Privileged Session Manager (PSM) that allows all activities during a session to be recorded for auditing purposes2. By enabling these settings in the Master Policy, you ensure that the domain accounts have one-time password access enforced and that all sessions connecting to domain controllers are recorded by CyberArk PSM. References:
? CyberArk Docs: One-time passwords and exclusive accounts1

NEW QUESTION 76
You have been asked to create an account group and assign three accounts which belong to a cluster. When you try to create a new group, you receive an unauthorized error; however, you are able to edit other aspects of the account properties.
Which safe permission do you need to manage account groups?

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

Answer: D

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

NEW QUESTION 77
What are the mandatory fields when onboarding from Pending Accounts? (Choose two.)

A. Address
B. Safe
C. Account Description
D. Platform
E. CPM

Answer: BD

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

NEW QUESTION 80
For a safe with Object Level Access enabled you can turn off Object Level Access Control when it no longer needed on the safe.

A. TRUE
B. FALSE

Answer: B

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

NEW QUESTION 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 88
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 92
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 93
Where can PTA be configured to send alerts? (Choose two.)

A. SIEM
B. Email
C. Google Analytics
D. EVD
E. PAReplicate

Answer: AB

Explanation:
CyberArk’s Privileged Threat Analytics (PTA) can be configured to send alerts to a Security Information and Event Management (SIEM) system and via Email. SIEM systems are used for real-time analysis of security alerts generated by applications and network hardware, while email alerts can be sent to individual or group email addresses for immediate notification1.
References:
? CyberArk Docs: Send PTA Alerts to Email1

NEW QUESTION 97
Which of the following are secure options for storing the contents of the Operator CD, while still allowing the contents to be accessible upon a planned Vault restart? (Choose three.)

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

Answer: ABD

Explanation:
? A. Store the CD in a physical safe and mount the CD every time Vault maintenance is performed. This option ensures that the CD is kept in a secure location

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

NEW QUESTION 100
If PTA is integrated with a supported SIEM solution, which detection becomes available?

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

Answer: D

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

NEW QUESTION 101
Your organization has a requirement to allow users to “check out passwords” and connect to targets with the same account through the PSM.
What needs to be configured in the Master policy to ensure this will happen?

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

Answer: A

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

NEW QUESTION 102
VAULT authorizations may be granted to .

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

Answer: AC

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

NEW QUESTION 105
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
A Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control.

A. True
B. False

Answer: A

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

NEW QUESTION 111
Which of the following components can be used to create a tape backup of the Vault?

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

Answer: C

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

NEW QUESTION 112
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 115
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 119
Which service should NOT be running on the DR Vault when the primary Production Vault is up?

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

Answer: C

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

NEW QUESTION 120
Where can a user with the appropriate permissions generate a report? (Choose two.)

A. PVWA > Reports
B. PrivateArk Client
C. Cluster Vault Manager
D. PrivateArk Server Monitor
E. PARClient

Answer: AB

Explanation:
A user with the appropriate permissions can generate a report in the PVWA (Privileged Vault Web Access) under theReports section1. Users who belong to the group specified in the ManageReportsGroup parameter in the Reports section of the Web Access Options in the System Configuration page are able to generate reports in the PVWA. By default, this group is the PVWAMonitor group1. Additionally, reports can be generated using the PrivateArk Client, which is a desktop application that provides a direct interface to manage the CyberArk Vault and its contents, including the generation of
reports2.
References:
? CyberArk Docs - Reports in PVWA1
? CyberArk Docs - Generate the Report2

NEW QUESTION 124
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 125
Which permissions are needed for the Active Directory user required by the Windows Discovery process?

A. Domain Admin
B. LDAP Admin
C. Read/Write
D. Read

Answer: D

Explanation:
The Active Directory user required by the Windows Discovery process needs to have Read permissions in the OU to scan and all sub-OUs1. This allows the Discovery process to scan predefined machines for new and modified accounts and their dependencies without requiring elevated privileges such as Domain Admin or LDAP Admin rights. The Read permission is sufficient for the Discovery process to retrieve the necessary information about the accounts that should be onboarded into the Vault. References:
? CyberArk's official documentation on managing discovery processes outlines the permissions required for the Discovery process, including the need for Read permissions for the Active Directory user performing the discovery1.
? Additional details on the required credentials for scanning and the Discovery process can be found in the supported target machines section of CyberArk's documentation2.

NEW QUESTION 130
A recently-hired colleague onboarded five new Local Accounts that are used for five standalone Windows Servers. After attempting to connect to the servers from PVWA, the colleague noticed that the "Connect" button was greyed out for all five new accounts.
What can you do to help your colleague resolve this issue? (Choose two.)

A. Verify that the address field is populated with an IP or FQDN of each server.
B. Verify that the correct PSM connection component appears within account platform settings.
C. Verify that the address field is blank and that the correct PSM connection component appears within account platform settings.
D. Notify the Windows Team that created the new accounts that the CyberArk PAM solution is not designed to manage local accounts on Windows Servers.
E. Verify that the "Disable automatic management for this account" setting for each account is not enabled.

Answer: ABE

Explanation:
? Verify Server Address: Ensure that the address field is populated with the correct IP or FQDN for each server (Option A).
? Check PSM Settings: Confirm that the correct PSM connection component is specified within the account platform settings (Option B).
? Automatic Management: Check if the "Disable automatic management for this account" setting is not enabled (Option E).
These steps should help in troubleshooting the connection issue in the CyberArk Privileged Access Management (PAM) solution.

NEW QUESTION 133
Within the Vault each password is encrypted by:

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

Answer: D

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

NEW QUESTION 136
Which built-in report from the reports page in PVWA displays the number of days until a password is due to expire?

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

Answer: A

Explanation:
ThePrivileged Accounts Inventory report in PVWA includes a column that displays the Age of the password, which indicates the number of days since the password was created1. This information can be used to determine how many days are left until a password is due to expire, based on the password policy's expiration settings.

References:
? CyberArk's official documentation on PVWA reports provides a list of available reports and their descriptions, including the Privileged Accounts Inventory report which contains details about password age and other relevant information1.

NEW QUESTION 141
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 143
Which of the following options is not set in the Master Policy?

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

Answer: C

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

NEW QUESTION 146
What is the chief benefit of PSM?

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

Answer: D

Explanation:
According to the web search results, the chief benefit of PSM is to provide both privileged session isolation and privileged session recording. Privileged session isolation means that the PSM server acts as a proxy between the user and the target machine, preventing the user from directly accessing the target machine or exposing the privileged account credentials. Privileged session recording means that the PSM server captures and stores a video and a transcript of the user's activity on the target machine, enabling auditing and monitoring of the privileged session. These benefits help to enhance the security and compliance of the privileged access management solution, as they prevent credential exposure, restrict unauthorized access, detect malicious activity, and provide evidence for forensic analysis

NEW QUESTION 151
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 155
The password upload utility must run from the CPM server

A. TRUE
B. FALSE

Answer: A

Explanation:
According to the CyberArk documentation1, the Password Upload utility must run from the Central Policy Manager (CPM) server. This utility works by uploading passwords and their properties into the Password Vault from a pre-prepared file, creating the required environment, when necessary. It is run from a command line whenever a password upload is required1.

NEW QUESTION 157
CyberArk recommends implementing object level access control on all Safes.

A. True
B. False

Answer: B

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

NEW QUESTION 160
Which type of automatic remediation can be performed by the PTA in case of a suspected credential theft security event?

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

Answer: A

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

NEW QUESTION 162
You received a notification from one of your CyberArk auditors that they are missing Vault level audit permissions. You confirmed that all auditors are missing the Audit Users Vault permission.
Where do you update this permission for all auditors?

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

Answer: B

Explanation:

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

NEW QUESTION 164
dbparm.ini is the main configuration file for the Vault.

A. True
B. False

Answer: B

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

NEW QUESTION 169
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

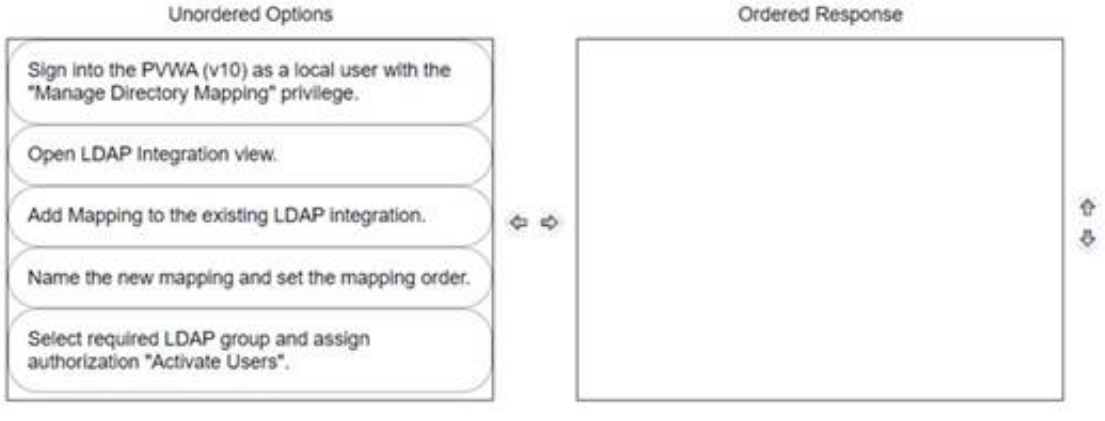
NEW QUESTION 174
Which command generates a full backup of the Vault?

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 175
DRAG DROP
You have been asked to delegate the rights to unlock users to Tier 1 support. The Tier 1 support team already has an LDAP group for its members.
Arrange the steps to do this in the correct sequence.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 178
Users are unable to launch Web Type Connection components from the PSM server. Your manager asked you to open the case with CyberArk Support.
Which logs will help the CyberArk Support Team debug the issue? (Choose three.)

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

Answer: ACD

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

NEW QUESTION 182
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 183
You notice an authentication failure entry for the DR user in the ITALog. What is the correct process to fix this error? (Choose two.)

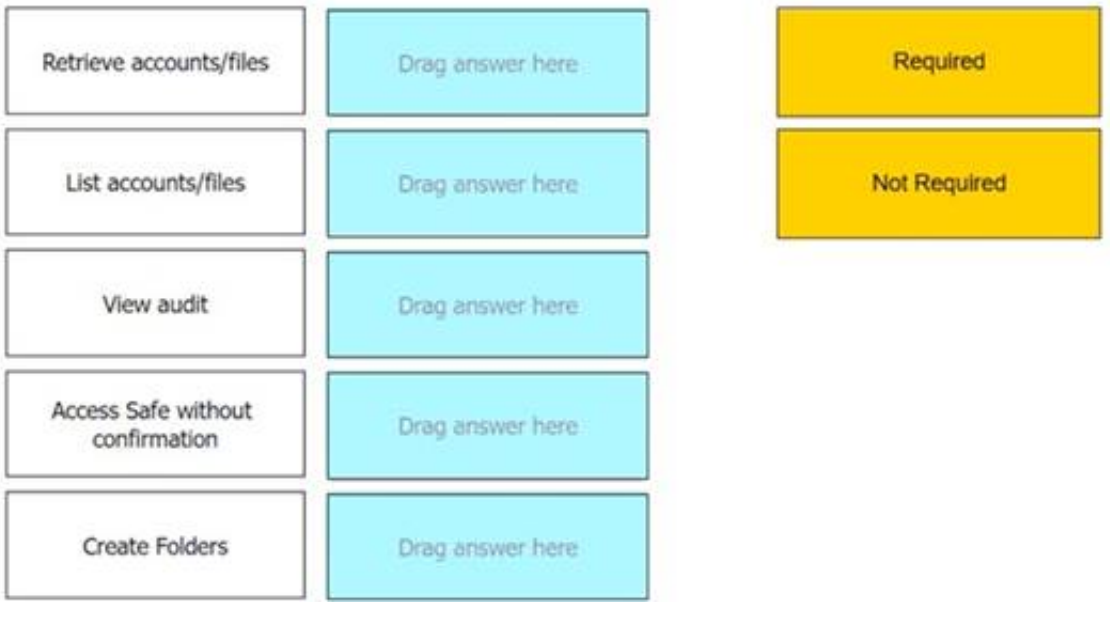
A. PrivateArk Client > Tools > Administrative Tools > Users and Groups > DR User > Update > Authentication > Update Password.
B. Create a new credential file, on the DR Vault, using the CreateCredFile utility and the newly set password.
C. Create a new credential file, on the Primary Vault, using the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

Answer: AB

Explanation:
When an authentication failure for the DR user is noticed in the ITALog, the correct process to fix this error involves two steps. First, you need to update the password for the DR user. This is done through the PrivateArk Client by navigating to Tools > Administrative Tools > Users and Groups > DR User > Update > Authentication > Update Password. After updating the password, the next step is to create a new credential file on the DR Vault using the CreateCredFile utility with the newly set password. This ensures that the DR Vault has the updated credentials necessary for the DR user to authenticate successfully12.
References:

? CyberArk's official documentation on troubleshooting authentication issues, which includes steps on updating user passwords and creating new credential files1.
? Community discussions and support articles on resolving DR user authentication failures, which provide practical insights and recommended actions2

NEW QUESTION 186
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 188
PTA can automatically suspend sessions if suspicious activities are detected in a privileged session, but only if the session is made via the CyberArk PSM.

A. True
B. False, the PTA can suspend sessions whether the session is made via the PSM or not

Answer: B

Explanation:
The PTA can automatically suspend sessions if suspicious activities are detected in a privileged session, regardless of the session method. The PTA can suspend sessions that are made via the PSM, the PVWA, or directly to the target system. The PTA can also suspend sessions that are made via SSH, RDP, or other protocols. References:
? Defender PAM Sample Items Study Guide, page 24
? PTA User Guide, page 17

NEW QUESTION 190
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 195
What is required to manage loosely connected devices?

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

Answer: B

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

NEW QUESTION 198
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 200
What is the purpose of the password change process?

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

Answer: B

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

NEW QUESTION 205

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your PAM-DEF Exam with Our Prep Materials Via below:

https://www.certleader.com/PAM-DEF-dumps.html