Exam Questions PAM-DEF

CyberArk Defender - PAM

https://www.2passeasy.com/dumps/PAM-DEF/

NEW QUESTION 1
A new domain controller has been added to your domain. You need to ensure the CyberArk infrastructure can use the new domain controller for authentication. Which locations must you update?

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

Answer: A

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

NEW QUESTION 2
Which keys are required to be present in order to start the PrivateArk Server service?

A. Recovery public key
B. Recovery private key
C. Server key
D. Safe key

Answer: AC

Explanation:
The server key and the public recovery key are required to be present in order to start the PrivateArk Server service. The server key opens the Vault, much like the key of a physical Vault. The public recovery key is part of the asymmetric recovery key that enables the Master User to log on to the Vault in case of a disaster. The server key and the public recovery key are usually stored on a removable media, such as a disk or CD, so that they can be safely secured in a physical safe. The recovery private key and the safe key are not needed to start the PrivateArk Server service. The recovery private key is only used for recovery purposes and the safe key is only used to access a specific safe that is defined with an external key. References: Server keys, Server Components

NEW QUESTION 3
Which option in the Private Ark client is used to update users' Vault group memberships?

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

Answer: C

Explanation:
In the Private Ark client, to update users' Vault group memberships, you use the Update > Member Of tab. This tab allows administrators to manage which groups a user is a member of. By adding or removing groups in this tab, you can effectively update the user's group memberships and, consequently, their access permissions within the Vault1.
References:
? CyberArk's official documentation on managing users in the Private Ark client, which includes instructions on how to update users' group memberships

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

A. Kerberos
B. ODBC
C. VBScript
D. Sybase

Answer: B

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

NEW QUESTION 5
Which of the following logs contains information about errors related to PTA?

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

D. WebApplication.log

Answer: B

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

NEW QUESTION 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
As long as you are a member of the Vault Admins group, you can grant any permission on any safe that you have access to.

A. TRUE
B. FALSE

Answer: B

Explanation:
Being a member of the Vault Admins group does not automatically grant you any permission on any safe that you have access to. The Vault Admins group is a predefined group that is created during the installation or upgrade of the vault. This group has the Vault Admin authorization, which allows its members to perform administrative tasks on the vault, such as managing users, groups, platforms, policies, and safes1. However, this authorization does not include any safe member authorizations, such as View, Retrieve, Use, or Manage Safe2. Therefore, to grant any permission on a safe, you need to be added as a safe member with the appropriate authorizations, either directly or through another group. The Vault Admins group can be added to safes with all safe member authorizations, but this is not done automatically for all safes. By default, this group is only added to a number of system safes, such as the Password Manager Safe, the PVWAConfig Safe, and the Notification Methods Safe3. For other safes, the Vault Admins group can be added manually by the safe owner or another user with the Manage Safe authorization4. References:
? 1: Predefined users and groups, Predefined groups subsection
? 2: [CyberArk Privileged Access Security Implementation Guide], Chapter 3: Managing Safes, Section: Safe Authorizations, Table 2-1: Safe Authorizations
? 3: What default groups can be automatically added to Safes when they are created?
? 4: [CyberArk Privileged Access Security Administration Guide], Chapter 3: Managing Safes, Section: Adding Safe Members

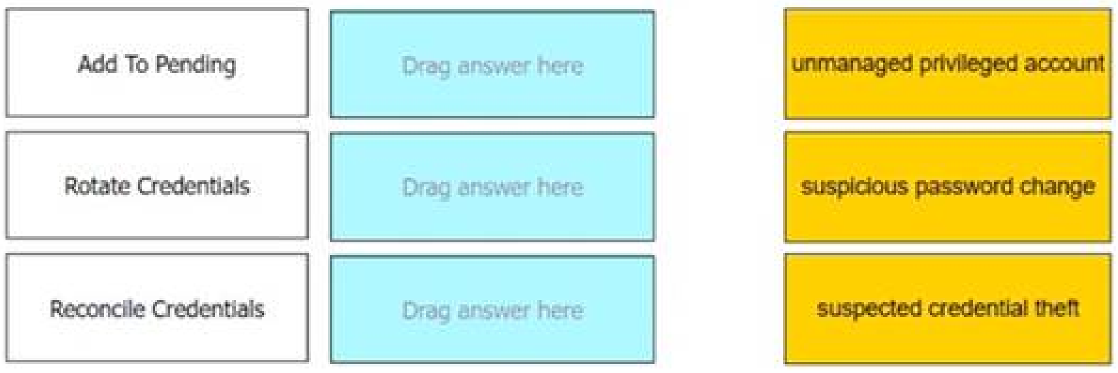
NEW QUESTION 8
You want to give a newly-created group rights to review security events under the Security pane. You also want to be able to update the status of these events. Where must you update the group to allow this?

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%7C 2#Permissions

NEW QUESTION 9
DRAG DROP
Match each automatic remediation to the correct PTA security event.



Add To Pending	Drag answer here	unmanaged privileged account
Rotate Credentials	Drag answer here	suspicious password change
Reconcile Credentials	Drag answer here	suspected credential theft

A. Mastered
B. Not Mastered

Answer: A

Explanation:
In CyberArk's Privileged Threat Analytics (PTA), automatic remediations are actions that can be configured to respond to specific security events. For the event of an unmanaged privileged account, the remediation "Add To Pending" is used to add the account to the pending accounts queue. When there is a suspected credential theft, "Rotate Credentials" is the remediation that initiates a password change. Lastly, for a suspicious password change event, "Reconcile Credentials" is the remediation that ensures the credentials are correct and valid1.
References:
? CyberArk Docs: Configure security events

NEW QUESTION 10
A logon account can be specified in the platform settings.

A. True
B. False

Answer: A

Explanation:
A logon account can be specified in the platform settings of CyberArk, a security software that manages privileged accounts and credentials. According to the CyberArk documentation1, "In the Account Details window, in the CPM pane, in the accounts section, you can associate either a logon account or a reconciliation account. If a default logon account has been configured for the platform that manages this account, that account is listed. You can associate another logon account or leave the default account as it is."1 A logon account is an account that is used to log on to a target system and perform password management operations on other accounts. A reconciliation account is an account that is used to restore access to a target system when the logon account fails.

NEW QUESTION 10
Which usage can be added as a service account platform?

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

Answer: B

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

NEW QUESTION 13
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 15
What is the primary purpose of Dual Control?

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

Answer: D

Explanation:
Dual control is a feature of CyberArk Defender PAM 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 Control. The primary purpose of dual control is to prevent a single user from accessing a sensitive account without authorization, which could lead to fraud or misuse of privileges.
By requiring confirmation from another authorized user, dual control ensures that there is a 'collusion to commit' fraud, meaning that at least two users are involved in the malicious activity and are accountable for it. References:
? Dual Control - CyberArk
? Dual Control - CyberArk
? Dual control in V10 Interface - docs.cyberark.com

NEW QUESTION 20
Where can you assign a Reconcile account? (Choose two.)

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

Answer: AB

Explanation:
A Reconcile account can be assigned in the Privileged Vault Web Access (PVWA) at both the account level and within the platform configuration. At the account level, a Reconcile account password can be defined which will override the account specified in the platform1. In the platform configuration, you can navigate to Platform Management, select the platform, edit it, and then expand Automatic Password Management to enter the values in the 'ReconcileAccountSafe' and 'ReconcileAccountName' fields, which will apply to all accounts attached to that specific platform2.
References:
? CyberArk Docs - Reconcile Password1
? CyberArk Community - Associate reconcile account with a specific platform

NEW QUESTION 21
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 22
You are concerned about the Windows Domain password changes occurring during business hours.
Which settings must be updated to ensure passwords are only rotated outside of business hours?

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

Answer: B

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

NEW QUESTION 23
Which user(s) can access all passwords in the Vault?

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

Answer: D

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

NEW QUESTION 25
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 29
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 31
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 32
A user needs to view recorded sessions through the PVWA.
Without giving auditor access, which safes does a user need access to view PSM recordings? (Choose two.)

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

Answer: AB

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

NEW QUESTION 35
Accounts Discovery allows secure connections to domain controllers.

A. TRUE
B. FALSE

Answer: B

NEW QUESTION 38
What do you need on the Vault to support LDAP over SSL?

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

Answer: A

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

NEW QUESTION 43
It is possible to leverage DNA to provide discovery functions that are not available with auto-detection.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 45
What is the name of the Platform parameters that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy?

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

Answer: A

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

NEW QUESTION 49
A Logon Account can be specified in the Master Policy.

A. TRUE
B. FALSE

Answer: B

Explanation:
A Logon Account cannot be specified in the Master Policy. The Master Policy is a set of rules that define the security and compliance policy of privileged accounts in the organization, such as access workflows, password management, session monitoring, and auditing1. The Master Policy does not include any technical settings that determine how the system manages accounts on various platforms1. A Logon Account is a technical setting that defines the account that the CPM uses to log on to a target system and perform password management tasks, such as changing, verifying, or reconciling passwords2. A Logon Account can be specified in the Platform Management settings, which are configured by the IT administrator for each platform2. The Platform Management settings are independent of the Master Policy and can be customized according to the organization's environment and security policies1. References:
? The Master Policy
? [Platform Management]

NEW QUESTION 51
What is the easiest way to duplicate an existing platform?

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

Answer: B

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

NEW QUESTION 53
You are configuring CyberArk to use HTML5 gateways exclusively for PSM connections. In the PVWA, where do you set DefaultConnectionMethod to HTML5?

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

Answer: A

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

NEW QUESTION 56
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 57
When creating an onboarding rule, it will be executed upon .

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

Answer: C

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

NEW QUESTION 60
One can create exceptions to the Master Policy based on .

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

Answer: B

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

NEW QUESTION 64
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 67
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 70
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 75
What is the correct process to install a custom platform from the CyberArk Marketplace?

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

Answer: B

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

NEW QUESTION 78
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 80
In addition to add accounts and update account contents, which additional permission on the safe is required to add a single account?

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

Answer: C

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

NEW QUESTION 81
You want to create a new onboarding rule. Where do you accomplish this?

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

Answer: D

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

NEW QUESTION 83
Via Password Vault Web Access (PVWA), a user initiates a PSM connection to the target Linux machine using RemoteApp. When the client's machine makes an RDP connection to the PSM server, which user will be utilized?

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

Answer: C

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

NEW QUESTION 86
Users who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.

A. TRUE
B. FALSE

Answer: B

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

NEW QUESTION 88
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 89
According to CyberArk, which issues most commonly cause installed components to display as disconnected in the System Health Dashboard? (Choose two.)

A. network instabilities/outages
B. vault license expiry
C. credential de-sync
D. browser compatibility issues
E. installed location file corruption

Answer: AC

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

NEW QUESTION 91
You want to build a connector that connects to a website through the Web applications for PSM framework.
Which default connector do you duplicate and modify?

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

Answer: D

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

NEW QUESTION 96
Your customer, ACME Corp, wants to store the Safes Data in Drive D instead of Drive C. Which file should you edit?

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

Answer: A

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

NEW QUESTION 101
When should vault keys be rotated?

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

Answer: D

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

NEW QUESTION 106
During a High Availability node switch you notice an error and the Cluster Vault Manager Utility fails back to the original node.
Which log files should you check to investigate the cause of the issue? (Choose three.)

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

Answer: BCE

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

NEW QUESTION 109
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 113
Which statement is true about setting the reconcile account at the platform level?

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

Answer: C

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

NEW QUESTION 118
Which command generates a full backup of the Vault?

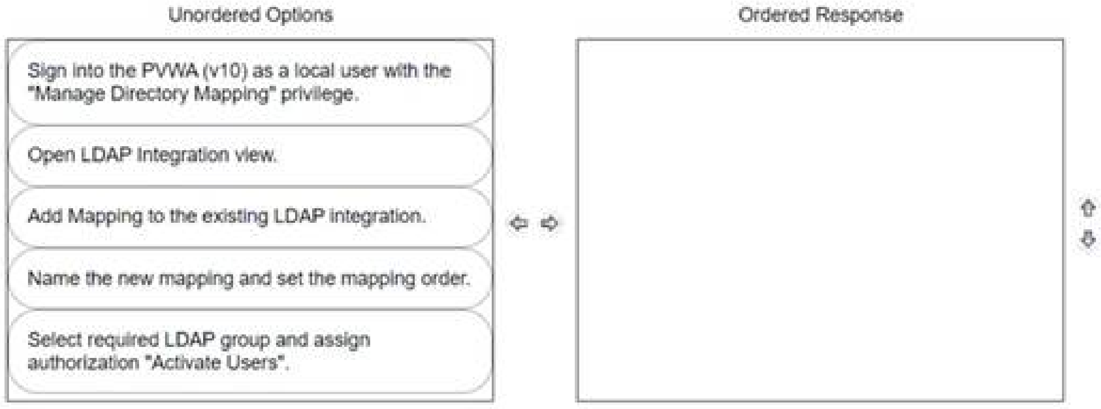
A. PAReplicate.exe Vault.ini /LogonFromFile user.ini /FullBackup
B. PAPreBackup.exe C:\PrivateArk\Server\Conf\Vault.ini Backup/Asdf1234 /full
C. PARestore.exe PADR ini /LogonFromFile vault.ini /FullBackup
D. CAVaultManager.exe RecoverBackupFiles /BackupPoolName BkpSvr1

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 122
DRAG DROP
You have been asked to delegate the rights to unlock users to Tier 1 support. The Tier 1 support team already has an LDAP group for its members.
Arrange the steps to do this in the correct sequence.



Unordered Options

Sign into the PVWA (v10) as a local user with the "Manage Directory Mapping" privilege.

Open LDAP Integration view.

Add Mapping to the existing LDAP integration.

Name the new mapping and set the mapping order.

Select required LDAP group and assign authorization "Activate Users".

Ordered Response

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 124
You are creating a new Rest API user that utilizes CyberArk Authentication.
What is a correct process to provision this user?

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

Answer: D

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

NEW QUESTION 127
What must you specify when configuring a discovery scan for UNIX? (Choose two.)

A. Vault Administrator
B. CPM Scanner
C. root password for each machine
D. list of machines to scan
E. safe for discovered accounts

Answer: BD

Explanation:
When configuring a discovery scan for UNIX, you must specify theCPM Scanner and thelist of machines to scan. The CPM Scanner is the component responsible for executing the discovery process, and it requires a list of target machines to scan for new and modified accounts and their dependencies. This list can be provided in the form of a CSV file for UNIX machines1. The discovery process will then scan the predefined machines to identify privileged accounts that should be

onboarded into the Vault for secure and automated management according to enterprise compliance policies2. References:
? CyberArk Docs - Manage discovery processes1
? CyberArk Docs - Scan for accounts using Account Discovery

NEW QUESTION 128
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 131
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 134
......