



CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM

NEW QUESTION 1

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

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

Answer: C

Explanation:

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

NEW QUESTION 2

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

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 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

DRAG DROP

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

According to the CyberArk documentation¹, the prerequisites for running the PSM Health Check are:

- ? PSM service installed on Windows 2016 or Windows 2019
- ? Web Server (IIS 8.5) role is installed
- ? A valid SSL certificate is installed on the Web Server

Therefore, these prerequisites are mandatory for the PSM Health Check to work properly. The PSM service installed on Windows 2008 R2 is not mandatory, as it is not supported by the PSM Health Check².

References: PSM Health Check, PSM Health Check - CyberArk

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

NEW QUESTION 6

All of your Unix root passwords are stored in the safe UnixRoot. Dual control is enabled for some of the accounts in that safe. The members of the AD group UnixAdmins need to be able to use the show, copy, and connect buttons on those passwords at any time without confirmation. The members of the AD group Operations Staff need to be able to use the show, copy and connect buttons on those passwords on an emergency basis, but only with the approval of a member of Operations Managers never need to be able to use the show, copy or connect buttons themselves.

Which safe permission do you need to grant Operations Staff? Check all that apply.

- A. Use Accounts
- B. Retrieve Accounts
- C. Authorize Password Requests
- D. Access Safe without Authorization

Answer: AB

Explanation:

To use the show, copy, and connect buttons on the accounts in the safe UnixRoot, the Operations Staff need to have the Use Accounts permission, which allows them to request access to the accounts and perform actions on them. However, since dual control is enabled for some of the accounts, they also need to have the Retrieve Accounts permission, which allows them to view the password of the account after it is authorized by another user. The Authorize Password Requests permission is not needed, as it is only required for the users who can approve the requests, not the ones who make them. The Access Safe without Authorization permission is not needed, as it would bypass the dual control mechanism and allow the Operations Staff to access the accounts without approval. References:

- ? [Defender PAM Sample Items Study Guide], page 10, question 5
- ? [CyberArk Privileged Access Security Implementation Guide], page 30, table 2-1
- ? [CyberArk Privileged Access Security Administration Guide], page 43, section 3.2.2.1

NEW QUESTION 7

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 8

DRAG DROP

Match each component to its respective Log File location.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Comprehensive explanation: The log file locations for each component in CyberArk's Privileged Access Management (PAM) are specific to the function and operation of that component. The PTA System logs are typically found in the PrivateArk Server directory, specifically in the PADR folder. The PSM for SSH, which is the Privileged Session Manager for SSH, stores its logs in the tomcat logs directory. Lastly, the logs for Disaster Recovery operations are located in the CARksymop logs directory on a Linux-based system. References: The information is based on the CyberArk documentation and best practices for managing and maintaining log files for different components within the PAM solution¹²³. The log file locations are essential for troubleshooting and auditing purposes, ensuring that all activities and changes are properly recorded and can be reviewed when necessary.

NEW QUESTION 9

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 10

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 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 12

You are logging into CyberArk as the Master user to recover an orphaned safe. Which items are required to log in as Master?

- A. Master CD, Master Password, console access to the Vault server, Private Ark Client
- B. Operator CD, Master Password, console access to the PVWA server, PVWA access
- C. Operator CD, Master Password, console access to the Vault server, Recover.exe
- D. Master CD, Master Password, console access to the PVWA server, Recover.exe

Answer: A

Explanation:

The Master user is a predefined user that has complete control over the entire system and can manage a full recovery when necessary. To log in as the Master user, you need the following items:

? Master CD: This is a physical CD that contains the Private Recovery Key, which is a file named RecPrv.key. This key is used to decrypt the Vault data and authenticate the Master user. The Master CD must be inserted into the Vault server's CD drive.

? Master Password: This is a password that is set by the Master user during the initial installation of the Vault. It is used to log in to the Vault with the Master user name. The Master password can be reset by the Master user if needed.

? Console access to the Vault server: This is a direct access to the Vault server machine, either physically or remotely. The Master user can only log in from the Vault server machine, not from any other client machine.

? Private Ark Client: This is a graphical user interface that allows the Master user to connect to the Vault and perform various tasks, such as recovering orphaned safes, activating predefined users, and managing network areas. The Private Ark Client must be installed on the Vault server machine and configured to use PrivateArk authentication method.

References: How to log in as the Master user, Predefined users and groups, Log in as Master from CyberArk PrivateArk Client

NEW QUESTION 15

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

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

Answer: C

Explanation:

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

NEW QUESTION 19

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 22

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 26

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 27

A user has successfully conducted a short PSM session and logged off. However, the user cannot access the Monitoring tab to view the recordings. What is the issue?

- A. The user must login as PSMAdminConnect
- B. The PSM service is not running
- C. The user is not a member of the PVWAMonitor group
- D. The user is not a member of the Auditors group

Answer: D

Explanation:

To access the Monitoring tab and view the recordings of the PSM sessions, the user must have membership in the Auditors group or membership in the relevant Account Safes and Recording Safes with the appropriate permissions1. The user must also use the same connection method (RDP file or HTML5 Gateway) as the end user who conducted the session1. The other options are not relevant to the issue, as the user does not need to login as PSMAdminConnect, the PSM service is running if the user was able to conduct a session, and the PVWAMonitor group is not a valid group in CyberArk. References:

? Monitor Privileged Sessions - CyberArk, section "The MONITORING page"

NEW QUESTION 30

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

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

Answer: A

Explanation:

SSH keys are a way to authenticate to a target machine with a privileged account, and are subject to the same risks and challenges as privileged passwords. CyberArk provides an out-of-the-box target platform to manage SSH keys, called UNIX Via SSH Keys, which simplifies and automates SSH keys lifecycle management. This platform works as follows:

? CyberArk stores the private keys in the Vault, where they benefit from all the security and accessibility features of the Vault, such as encryption, auditing, and backup.

? CyberArk updates the public keys on the target systems, using a parent account that has access to the file that contains the public key, such as `~/ssh/authorized_keys`. CyberArk can generate new random SSH key pairs and update the public keys on the target systems according to the organizational policy, such as after a single use, after a predefined period, or manually.

? CyberArk can also verify that the private and public keys are synchronized, and reconcile them if they are not, using a reconcile account that can reset the SSH key pairs on the target systems.

References: Manage SSH Keys, Use SSH Keys

NEW QUESTION 33

Which dependent accounts does the CPM support out-of-the-box? (Choose three.)

- A. Solaris Configuration file

- B. Windows Services
- C. Windows Scheduled
- D. Windows DCOM Applications
- E. Windows Registry
- F. Key Tab file

Answer: BCE

Explanation:

Dependent accounts are accounts that represent resources such as Windows Services, Windows Scheduled Tasks, and others, which are accessed from a target machine and require the same credentials as the target machine. The CyberArk Privileged Account Security Solution's Central Policy Manager (CPM) supports out-of-the-box dependent accounts for Windows Services, Windows Scheduled Tasks, and Windows Registry. When changing a password, the CPM synchronizes the target account password with all other occurrences of that password in any related dependent accounts. This ensures that all dependent accounts are updated simultaneously to maintain security and functionality¹². References:

- ? CyberArk Docs: Manage dependent accounts¹
- ? CyberArk Docs: Supported dependent accounts

NEW QUESTION 38

DRAG DROP

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

Cyber-Ark Hardened Windows Firewall	Drag answer here	Running
PrivateArk Database	Drag answer here	Stopped
PrivateArk Server	Drag answer here	
CyberArk Vault Disaster Recovery	Drag answer here	
Cyber-Ark Event Notification Engine	Drag answer here	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

CyberArk Hardened Windows Firewall -> Running PrivateArk Database -> Running
 PrivateArk Server -> Stopped

CyberArk Vault Disaster Recovery -> Running CyberArk Event Notification Engine -> Stopped

? Comprehensive Explanation: A DR Vault is a Vault that acts as a standby replica of the Primary Vault and is ready to take its place when the Primary Vault is unavailable. The DR Vault operates in Replication mode, which means it continuously replicates the data and metadata from the Primary Vault. In Replication mode, the following services have the following status on the DR Vault:

- ? Cyber-Ark Hardened Windows Firewall: This service provides firewall protection for the Vault server. It should be running on the DR Vault to ensure security.
- ? PrivateArk Database: This service manages the database that stores the metadata of the Vault. It should be stopped on the DR Vault, because the database is not active in Replication mode. The database is only activated when the DR Vault switches to Production mode.
- ? PrivateArk Server: This service manages the Vault server and its communication with other components. It should be stopped on the DR Vault, because the Vault server is not active in Replication mode. The Vault server is only activated when the DR Vault switches to Production mode.
- ? CyberArk Vault Disaster Recovery: This service manages the replication process between the Primary Vault and the DR Vault. It should be running on the DR Vault to ensure data synchronization and readiness for failover.
- ? Cyber-Ark Event Notification Engine: This service manages the event notifications and alerts for the Vault. It should be stopped on the DR Vault, because the event notifications are not relevant in Replication mode. The event notifications are only activated when the DR Vault switches to Production mode.

References: Primary-DR environment - CyberArk, Replicate the Primary Vault to the Satellite Vaults - CyberArk

NEW QUESTION 39

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 40

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 44

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

- A. TRUE
- B. FALSE

Answer: B

Explanation:

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

- References:
- ? 1: Manage the CyberArk License

NEW QUESTION 46

An auditor needs to login to the PSM in order to live monitor an active session. Which user ID is used to establish the RDP connection to the PSM server?

- A. PSMConnect
- B. PSMMaster
- C. PSMGwUser
- D. PSMAdminConnect

Answer: A

Explanation:

The PSMConnect user is a local user on the PSM server that is used to establish RDP connections to the PSM server. The PSMConnect user has the following permissions: Log on locally, Log on as a batch job, and Allow log on through Remote Desktop Services. The PSMConnect user is also a member of the local group PSMUsers, which has access to the PSM web console. The other user IDs are not used for RDP connections to the PSM server. The PSMMaster user is a local user on the PSM server that is used to run the PSM services. The PSMGwUser user is a local user on the PSM server that is used to run the PSM Gateway service. The PSMAdminConnect user is a local user on the PSM server that is used to connect to the PSM web console as an administrator. References: Privileged Session Manager, Defender - PAM, PSM for Web Console, Connect through PSM for SSH

NEW QUESTION 49

What is the purpose of the HeadStartInterval setting in a platform?

- A. It determines how far in advance audit data is collected for 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 53

Accounts Discovery allows secure connections to domain controllers.

- A. TRUE
- B. FALSE

Answer: B

NEW QUESTION 54

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 57

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

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

Answer: C

Explanation:

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

References:

? CyberArk Docs: Safe Settings¹

NEW QUESTION 59

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

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

Answer: A

Explanation:

Before failing back to the production infrastructure after a Disaster Recovery (DR) exercise, it is crucial to ensure that the Production Instance replicates all changes that occurred from the Disaster Recovery Instance. This includes all audit history and any other changes made during the DR event. The replication process ensures that no data is lost and that the audit history is maintained consistently across both the DR and Production environments¹.

References:

? CyberArk Docs - Reports and Audits¹

? CyberArk Docs - Vault Audit Action Codes²

? CyberArk Blog - Failover and Failback Process

NEW QUESTION 64

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 68

In the Private Ark client under the Tools menu > Administrative Tools > Users and Groups, which option do you use to update users' Vault group memberships?

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

Answer: C

Explanation:

In the PrivateArk client, to update users' Vault group memberships, you use the Member Of tab. After logging in as an administrative user and navigating to the Users and Groups window, you select a user and click Update. In the Member Of tab, you can manage the user's group memberships by adding or removing them from groups within the Vault1.

References:

? CyberArk Docs - Manage users in PrivateArk client1

NEW QUESTION 69

PSM captures a record of each command that was executed in Unix.

- A. TRUE
- 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 73

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

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

Answer: ACD

Explanation:

To run the Password Upload Utility, you need to create or configure the following files:

? A comma delimited upload file: This is a text file that contains the passwords and

their properties that will be uploaded to the Vault. The file must have a .csv extension and follow a specific format. The first line in the file defines the names of the password properties as specified in the Password Vault. Every other line represents a single password object and its property values, according to the properties specified in the first line1.

? PACli.ini: This is a configuration file that stores the parameters for the PACli, which

is a command-line interface that enables communication between the Password Upload Utility and the Vault. The PACli.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: Vault, User, Password, and LogFile2.

? conf.ini: This is a configuration file that stores the parameters for the Password

Upload Utility. The conf.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: InputFile, LogFile, and ErrorFile3.

You do not need to create or configure the following file to run the Password Upload Utility:

? Vault.ini: This is a configuration file that stores the parameters for the Vault server, such as the database name, port, and password. This file is not used by the Password Upload Utility, and it is not located in the same folder as the Password Upload Utility executable file. The Vault.ini file is located in the Vault installation folder, and it is used by the Vault service and the PrivateArk Client4. References:

? 1: Create the Password File

? 2: PACli.ini

? 3: Password Upload Utility Parameter File (conf.ini)

? 4: [CyberArk Privileged Access Security Implementation Guide], Chapter 2: Installing the Vault, Section: Configuring the Vault, Subsection: Vault.ini

NEW QUESTION 76

Ad-Hoc Access (formerly Secure Connect) provides the following features. Choose all that apply.

- A. PSM connections to target devices that are not managed by CyberArk.
- B. Session Recording.
- C. Real-time live session monitoring.
- D. PSM connections from a terminal without the need to login to the PVWA.

Answer: ABC

Explanation:

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

- ? Configure ad hoc connections
- ? Ad Hoc Connections
- ? Privileged Remote Access Management – PAM Remote Access

NEW QUESTION 79

Secure Connect provides the following. Choose all that apply.

- A. PSM connections to target devices that are not managed by CyberArk.
- B. Session Recording
- C. Real-time live session monitoring.
- D. PSM connections from a terminal without the need to login to the PVWA

Answer: ABC

Explanation:

Secure Connect provides the following features:

? A. PSM connections to target devices that are not managed by CyberArk. This is true, because Secure Connect is a feature that enables users to connect to target systems through PSM without storing the account credentials in the vault. Secure Connect allows users to provide their own credentials at the time of connection, and these credentials are not saved or managed by CyberArk. Secure Connect can be used with any connection component that supports PSM, such as RDP, SSH, WinSCP, etc¹.

? B. Session Recording. This is true, because Secure Connect sessions are recorded by PSM and stored in the Vault, just like regular PSM sessions. The recorded sessions can be viewed and audited by authorized users through the PVWA or the PSM web interface².

? C. Real-time live session monitoring. This is true, because Secure Connect sessions can be monitored in real-time by authorized users through the PSM web interface. The PSM web interface allows users to view the live session screen, send messages to the session user, pause or terminate the session, and take control of the session if needed³.

The following feature is not provided by Secure Connect:

? D. PSM connections from a terminal without the need to login to the PVWA. This is false, because Secure Connect requires users to login to the PVWA and initiate the connection from there. The PVWA provides the URL for the Secure Connect session, which contains the target system address and the connection component ID. The user then needs to copy and paste the URL into a browser or a remote connection manager to launch the session¹.

References:

- ? 1: Secure Connect
- ? 2: Recorded Sessions
- ? 3: PSM Web Interface

NEW QUESTION 82

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 85

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

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

Answer: B

Explanation:

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

NEW QUESTION 88

What is the primary purpose of One Time Passwords?

- 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: A

Explanation:

One Time Passwords (OTPs) are passwords that are valid for only one use or a limited time period. The primary purpose of OTPs is to reduce the risk of credential theft, which is a common attack vector for hackers and malicious insiders. By using OTPs, the exposure of the credentials is minimized, and the attacker cannot reuse the stolen password to access the target system. OTPs also enhance the security of the authentication process, as they add an extra layer of verification to the user's identity. OTPs can be generated by various methods, such as SMS, email, hardware tokens, software tokens, etc1.

The other options are not the primary purpose of OTPs, because:

? B. More frequent password changes. This is not the primary purpose of OTPs, but a consequence of using them. OTPs require more frequent password changes, as they expire after one use or a limited time period. However, this is not the main goal of using OTPs, but rather a means to achieve the goal of reducing the risk of credential theft.

? C. Non-repudiation (individual accountability). This is not the primary purpose of OTPs, but a benefit of using them. Non-repudiation means that the user cannot deny performing an action or accessing a resource, as there is sufficient evidence to prove their identity and activity. OTPs can help achieve non-repudiation, as they are unique and personal to each user, and can be traced back to the user's device or account. However, this is not the main goal of using OTPs, but rather an advantage of using them.

? D. To force a 'collusion to commit' fraud ensuring no single actor may use a password without authorization. This is not the primary purpose of OTPs, but a feature of using them. OTPs can help prevent unauthorized access to privileged accounts, as they require the user to have both the OTP and the regular password to access the target system. This means that no single actor can use the password without authorization, as they would need the cooperation of another actor who has the OTP. However, this is not the main goal of using OTPs, but rather a capability of using them.

References:

? 1: One-time password

NEW QUESTION 92

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 94

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

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

Answer: A

Explanation:

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

References:

? CyberArk Docs - Export Vault Data (EVD) utility1

? CyberArk Docs - Export data to files

NEW QUESTION 95

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 100

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 101

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

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

Answer: A

Explanation:

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

NEW QUESTION 103

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

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

Answer: A

Explanation:

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

NEW QUESTION 105

Which report could show all accounts that are past their expiration dates?

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

Answer: A

Explanation:

The Privileged Account Compliance Status report shows the compliance status of all privileged accounts in the Vault, based on the expiration date and password change policy. This report can help identify accounts that are past their expiration dates and need to be updated or removed. References:

? [Defender PAM Sample Items Study Guide], page 18, question 90

NEW QUESTION 110

DRAG DROP

Match the connection component to the corresponding OS/Function.

PSM-SSH	Drag answer here	Windows
PSM-RDP	Drag answer here	UNIX File Transfer
PSM-WinSCP	Drag answer here	UNIX
PSM-SQLPlus	Drag answer here	Database
PSM-OS390	Drag answer here	Mainframe

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

? A connection component is a set of parameters that defines how PSM connects to a target system using a specific protocol or application. Different connection components are suitable for different types of systems or functions. The correct matches are as follows:

? PSM-SSH: This connection component enables transparent connections to UNIX machines using the SSH protocol. It supports various UNIX flavors, such as Linux, Solaris, AIX, and HP-UX.

? PSM-RDP: This connection component enables transparent connections to Windows machines using the RDP protocol. It supports various Windows versions, such as Windows Server, Windows 10, and Windows 7.

? PSM-WinSCP: This connection component enables transparent connections to UNIX machines using the WinSCP application. It supports file transfer operations, such as upload, download, delete, and rename, between the local and remote machines.

? PSM-SQLPlus: This connection component enables transparent connections to Oracle databases using the SQL*Plus application. It supports various Oracle versions, such as Oracle 12c, Oracle 11g, and Oracle 10g.

? PSM-OS390: This connection component enables transparent connections to IBM mainframes using the OS/390 protocol. It supports various mainframe applications, such as TSO, CICS, and IMS.

References: Connection Components, Connection Component Parameters

NEW QUESTION 113

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 118

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 123

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 125

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 129

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 131

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 134

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

- A. Select Update on the CyberArk group, and then click Add > LDAP Group
- B. Select Update on the LDAP Group, and then click Add > LDAP Group
- C. Select Member Of on the CyberArk group, and then click Add > LDAP Group
- D. Select Member Of on the LDAP group, and then click Add > LDAP Group

Answer: C

Explanation:

To add an LDAP group to a CyberArk group, you need to use the Private Ark client and follow these steps1:

? In the Users and Groups tree, select the CyberArk group that you want to add the

LDAP group to.

? In the Properties pane, click Member Of.

? Click Add > LDAP Group.

? In the LDAP Group dialog box, enter the name of the LDAP group and click OK. References: Add an LDAP group to a Vault group

NEW QUESTION 135

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 138

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 142

Which onboarding method would you use to integrate CyberArk with your accounts provisioning process?

- A. Accounts Discovery
- B. Auto Detection
- C. Onboarding RestAPI functions
- D. PTA Rules

Answer: C

Explanation:

The Onboarding RestAPI functions are a set of web services that allow you to integrate CyberArk with your accounts provisioning process. You can use the Onboarding RestAPI functions to create, update, delete, or verify accounts in the CyberArk Vault, as well as to retrieve information about accounts, platforms, and safes. The Onboarding RestAPI functions are part of the Central Credential Provider component, which is installed on a dedicated server that communicates with the Vault. References:

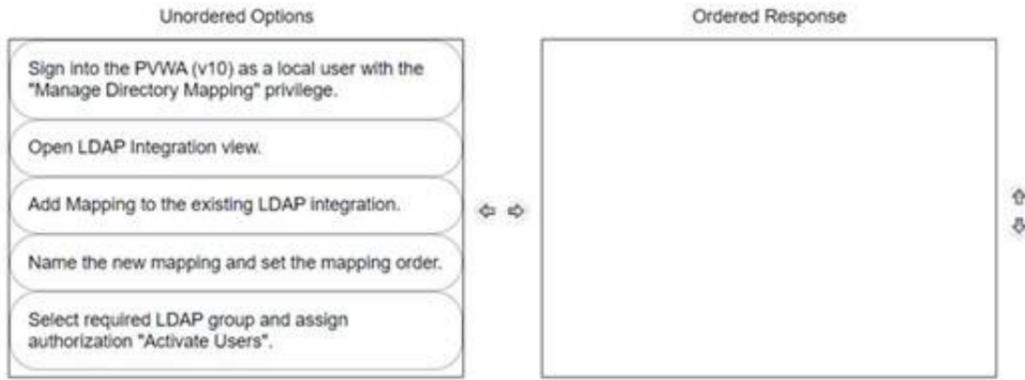
? [Defender PAM Course], Module 4: Onboarding Accounts, Lesson: Onboarding RestAPI Functions

? [Onboarding RestAPI Functions Guide], Introduction

NEW QUESTION 143

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 146

DRAG DROP

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

Retrieve accounts/files	Drag answer here	Required
List accounts/files	Drag answer here	
View audit	Drag answer here	Not Required
Access Safe without confirmation	Drag answer here	
Create Folders	Drag answer here	

- 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. The View audit authorization is necessary for users to view the audit records associated with the recordings¹.

References:

? CyberArk Docs - Monitor Privileged Sessions

NEW QUESTION 150

DRAG DROP

Arrange the steps to restore a Vault using PARestore for a Backup in the correct sequence.

Unordered Options
BackupFilesDeletion=No
CAVaultManager RestoreDB
BackupFilesDeletion=Yes,24,1,5,7d
CAVaultManager RecoverBackupFiles
PARestore vault.ini operator /FullVaultRestore

Ordered Response

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 151

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 the CPM Scanner and the list 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 155

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 156

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 159

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

PAM-DEF Practice Exam Features:

- * PAM-DEF Questions and Answers Updated Frequently
- * PAM-DEF Practice Questions Verified by Expert Senior Certified Staff
- * PAM-DEF Most Realistic Questions that Guarantee you a Pass on Your First Try
- * PAM-DEF Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The PAM-DEF Practice Test Here](#)