

CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM



NEW QUESTION 1

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

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

Answer: BCE

Explanation:

When using the CreateCredFile Utility to harden Credential Files (CredFiles), it is important to include parameters that enhance security. The Host IP Address, Client Hostname, and Vault IP Address are parameters that can be used to specify the environment in which the CredFile is valid, thereby restricting its use to specific machines or networks¹. This helps prevent unauthorized access to the CredFile and ensures that it is only used in the intended context.

References:

? CyberArk's official documentation on the CreateCredFile utility provides insights into the security mechanisms used to protect credential files, including the use of environmental key materials such as application-based, machine-based, and component-based materials¹.

? For a deeper understanding of how to secure Credential Files and the use of the CreateCredFile Utility, refer to the CyberArk Defender PAM course materials and study guide².

NEW QUESTION 2

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 3

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 4

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 5

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 6

You have been given the requirement that certain accounts cannot have their passwords updated during business hours. How can you set up a configuration to meet this requirement?

- A. Change settings on the CPM configuration safe so that access is permitted after business hours only.
- B. Update the password change parameters of the platform to match the permitted time frame.
- C. Disable automatic CPM management for all accounts that are assigned to this platform.
- D. Add an exception to the Master Policy to allow the action for this platform during the permitted time.

Answer: B

Explanation:

To ensure that certain accounts do not have their passwords updated during business hours, you can configure the password change parameters within the platform settings to specify the permitted time frame for updates. This involves setting the FromHour andToHour parameters to define a window outside of business hours during which the CyberArk Central Policy Manager (CPM) will perform automatic password changes1. By doing so, you can control when password changes occur and ensure compliance with the specified requirement.

References:

? CyberArk Community: Discussion on configuring automatic password change parameters

NEW QUESTION 7

Which Vault authorization does a user need to have assigned to able to generate the "Entitlement Report" from the reports page in PVWA? (Choose two.)

- A. Manage Users
- B. Audit Users
- C. Read Activity
- D. View Entitlements
- E. List Accounts

Answer: BD

Explanation:

D. View Entitlements: This authorization allows the user to view the entitlements, which is essential for generating reports that include access control and authorization levels on accounts.
 * B. Audit Users: Having ‘Audit Users’ permission is crucial as it enables the user to perform audit-related activities, which are typically part of generating entitlement reports12.
 These authorizations ensure that the user has the necessary permissions to access and compile the data required for the Entitlement Report within the CyberArk PVWA.

NEW QUESTION 8

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 9

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 10

When are external vault users and groups synchronized by default?

- A. They are synchronized once every 24 hours between 1 AM and 5 A
- B. Most Voted
- C. They are synchronized once every 24 hours between 7 PM and 12 AM.
- D. They are synchronized every 2 hours.
- E. They are not synchronized according to a specific schedule.

Answer: A

Explanation:

By default, external vault users and groups are synchronized once every 24 hours between 1 AM and 5 AM. This synchronization schedule is determined by the AutoSyncExternalObjects parameter in the DBParm.ini file, which specifies that the Vault's external users and groups will be synchronized with the External Directory during this time frame¹.

References:

? CyberArk Docs - Synchronize External Users and Groups in the Vault with the External Directory

NEW QUESTION 10

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

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

Answer: A

Explanation:

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

? CyberArk's official documentation provides a detailed procedure on how to configure PTA to send alerts to emails, including the use of the /opt/tomcat/utility/emailConfiguration.sh command

NEW QUESTION 13

Which statement is correct concerning accounts that are discovered, but cannot be added to the Vault by an automated onboarding rule?

- A. They are added to the Pending Accounts list and can be reviewed and manually uploaded.
- B. They cannot be onboarded to the Password Vault.
- C. They must be uploaded using third party tools.
- D. They are not part of the Discovery Process.

Answer: A

Explanation:

When accounts are discovered by CyberArk but do not match any automated onboarding rule, they are added to the Pending Accounts list. This allows administrators to review these accounts and decide whether to onboard them manually into the Vault. The Pending Accounts list serves as a holding area for

accounts that require further review or do not meet the criteria set by existing onboarding rules¹.

References:

? CyberArk's official documentation on Onboarding Rules, which explains the process of managing accounts that are discovered but not automatically onboarded¹.

NEW QUESTION 17

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 19

Which of the following Privileged Session Management solutions provide a detailed audit log of session activities?

- A. PSM (i.e., launching connections by clicking on the "Connect" button in the 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:

All of the Privileged Session Management solutions provide a detailed audit log of session activities. PSM, PSM for Windows, and PSM for SSH enable organizations to secure, control and monitor privileged access to network devices by using Vaulting technology to manage privileged accounts and create detailed session audits and video recordings of all IT administrator privileged sessions on remote machines¹. PSM also provides additional audit features such as SQL Command Level Audit, Windows Events Audit, and Universal Keystrokes Audit¹. PSM for Web captures a detailed transcript of cloud application user activity to enable a security manager or auditor the ability to monitor sessions for suspicious or restricted operations². References:

? Monitor Privileged Sessions - CyberArk

? Privileged Session Manager for Web - CyberArk

NEW QUESTION 22

Target account platforms can be restricted to accounts that are stored in specific Safes using the Allowed Safes property.

- A. TRUE
- B. FALSE

Answer: A

Explanation:

Target account platforms can be restricted to accounts that are stored in specific Safes using the Allowed Safes property. This property is a parameter that can be configured in the Platform Management settings for each platform. The Allowed Safes property specifies the name or names of the Safes where the platform can be applied. The default value is .*, which means that the platform can be used in any Safe. However, if you want to limit the platform to certain Safes, you can enter the name or names of the Safes, separated by a pipe (|) character. For example, if you want to restrict the platform to Safes called WindowsPasswords and LinuxPasswords, you can enter AllowedSafes=(WindowsPasswords)|(LinuxPasswords). This feature is useful for preventing unauthorized users from accessing passwords, especially if you implement the reconciliation functionality. It also helps the CPM to focus its search operations on specific Safes, instead of scanning all Safes it can see in the Vault¹. References:

? 1: Limit Platforms to Specific Safes

NEW QUESTION 27

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 30

Which master policy settings ensure non-repudiation?

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

Answer: B

Explanation:

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

References:

? CyberArk Docs: Master Policy Rules²

? CyberArk Docs: The Master Policy¹

NEW QUESTION 31

When a DR Vault Server becomes an active vault, it will automatically fail back to the original state once the Primary Vault comes back online.

- A. True; this is the default behavior
- B. False; this is not possible
- C. True, if the AllowFailback setting is set to "yes" in the padr.ini file
- D. True, if the AllowFailback setting is set to "yes" in the dbparm.ini file

Answer: C

Explanation:

When a DR Vault Server becomes an active vault, it will automatically fail back to the original state once the Primary Vault comes back online, if the AllowFailback setting is set to "yes" in the padr.ini file. The padr.ini file is the configuration file for the Disaster Recovery application, which enables the DR Vault to replicate data from the Primary Vault and take over its role in case of a failure. The AllowFailback setting determines whether the DR Vault will automatically switch back to the passive mode when the Primary Vault is restored. The default value of this setting is "no", which means that the DR Vault will remain active until a manual failback is performed¹. To enable the automatic

failback, the setting must be changed to "yes" and the padr service must be restarted¹. The dbparm.ini file is not relevant to this setting, as it is the main configuration file for the Vault database². References:

? Configure the DR Vault - CyberArk, section "AllowFailback"

? DBParm.ini - CyberArk, section "Main parameters"

NEW QUESTION 36

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

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

Answer: B

Explanation:

A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the account that has been changed manually, the CPM can use the reconcile account to restore the password of the account to the value that is stored in the Vault, in case it is changed or out of sync. This process is called password reconciliation and it ensures that the passwords are synchronized and available for use. To configure the account so that the CPM can resume management automatically, the platform that the account belongs to must have the following parameters set¹:

? RCAutomaticReconcileWhenUnsynced: This parameter determines whether passwords will be reconciled automatically after the CPM detects a password on a remote machine that is not synchronized with its corresponding password in the Vault. The acceptable values are Yes or No.

? RCReconcileReasons: This parameter determines the codes that represent the CPM plugin errors that will launch a reconciliation process. The acceptable values are plug-in return codes separated by a comma.

? RCFromHour, RCToHour: These parameters determine the time frame in hours during which the CPM can reconcile passwords, either manually or automatically. The acceptable values are 0-23 or -1 for none.

? RCExecutionDays: This parameter determines the days of the week when the CPM will reconcile passwords. The acceptable values are days of the week, separated by commas.

References:

? 1: Password Reconciliation

NEW QUESTION 38

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 39

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

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

Answer: B

Explanation:

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

? Safe Members - CyberArk1, section “Permissions”

? Safes and Safe members - CyberArk2, section “Safe members overview”

NEW QUESTION 44

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 48

When a group is granted the 'Authorize Account Requests' permission on a safe Dual Control requests must be approved by

- A. Any one person from that group
- B. Every person from that group
- C. The number of persons specified by the Master Policy
- D. That access cannot be granted to groups

Answer: C

Explanation:

When a group is granted the ‘Authorize Account Requests’ permission on a safe, dual control requests must be approved by the number of persons specified by the Master Policy. This means that the request will be sent to all the members of the group, but only a certain number of them need to confirm it for the request to be authorized. The Master Policy defines the number of required approvers for each level of confirmation, as well as the number of levels. For example, if the Master Policy requires two approvers at the first level and one approver at the second level, then the request will be sent to the group and two members of the group must confirm it before it is sent to the second level of confirmation, where one more approver is needed. References:

? Request access

? Safe Members

? CyberArk Defender - PAM Exam Practice Test

NEW QUESTION 52

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

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

Answer: A

Explanation:

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

NEW QUESTION 57

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

- A. True
- B. False

Answer: A

Explanation:

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

NEW QUESTION 59

To change the safe where recordings are kept for a specific platform, which setting must you update in the platform configuration?

- A. SessionRecorderSafe Most Voted
- B. SessionSafe
- C. RecordingsPath
- D. RecordingLocation

Answer: A

Explanation:

To change the safe where recordings are kept for a specific platform, you must update the SessionRecorderSafe setting in the platform configuration. This setting specifies the name of the safe where the Privileged Session Manager (PSM) recordings will be stored. After updating the SessionRecorderSafe setting, you need to restart the PSM service or wait for the new settings to be applied, which typically takes about 10 minutes. Once the new settings are in effect, any new PSM sessions initiated will have their recordings stored in the newly specified safe1.

References:

? CyberArk Docs - How to Create/Change/Configure PSM Recording Safes

NEW QUESTION 63

How do you create a cold storage backup?

- A. On the DR Vault, install PAReplicate according to the Installation guide, configure the logon ini file, and define the Schedule tasks for full and incremental backups.
- B. Install the Vault Backup utility on a different machine from the Enterprise Password Vault server and trigger the full backup.
- C. Configure the backup options in the PVWA.
- D. On the DR Vault, configure the cold storage backup path in TSParm.ini file.

Answer: A

Explanation:

To create a cold storage backup, you would install thePAReplicate utility on the DR Vault as per the installation guide. This utility is part of the CyberArk Vault's backup solution and is used to export the encrypted contents of your Safes securely to a computer outside the Vault environment. After installation, you would configure the logon ini file with the necessary credentials and define the scheduled tasks for both full and incremental backups. This ensures that the Safes are regularly backed up and that the data is available for recovery if needed1.

References:

? CyberArk's official documentation on using the CyberArk Backup Process, which includes details on the PAReplicate utility and how to configure it for cold storage backups1.

? Additional information on installing the Vault Backup Utility and configuring backup options, which provides context for the correct answer

NEW QUESTION 67

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 69

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 74

You are creating a shared safe for the help desk.

What must be considered regarding the naming convention?

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

Answer: D

Explanation:

When creating a shared safe for the help desk in CyberArk's Privileged Access Management (PAM), it is important to adhere to the naming conventions set forth by CyberArk. One of the key considerations is that certain characters are not permitted in the safe name. Specifically, the characters V:*<>".| are not allowed in the naming of safes. This is to ensure compatibility and prevent issues with the file system or the CyberArk application itself, as these characters may interfere with normal operations or be reserved for specific functions within the operating system or the application.

References: The information regarding safe naming conventions is based on CyberArk's best practices and guidelines, which are detailed in the official CyberArk documentation and study guides. It is important to consult the CyberArk Defender PAM resources and documents to ensure compliance with these standards

NEW QUESTION 79

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

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

Answer: A

Explanation:

The Privileged Accounts Inventory Report provides information about all the privileged accounts in the system, based on different filters, such as safe, platform, policy, and owner. To run this report through the Reports page in PVWA on a specific safe, the user needs to have the following permissions on that safe:

? List Accounts: This permission allows the user to view the accounts in the safe and their properties, such as name, address, platform, and policy.

? View Safe Members: This permission allows the user to view the members of the safe and their authorizations, such as owners, users, and groups.

These permissions are required to show complete account inventory information for the specific safe. Other permissions, such as Manage Safe Owners, Access Safe without confirmation, Manage Safe, and View Audit, are not relevant for this report. References: Reports and Audits - CyberArk, Safe Member Authorizations

NEW QUESTION 82

PSM for Windows (previously known as "RDP Proxy") supports connections to the following target systems

- A. Windows
- B. UNIX
- C. Oracle
- D. All of the above

Answer: D

Explanation:

PSM for Windows supports connections to various types of target systems, including Windows, UNIX, Oracle, and others. PSM for Windows uses different connection components to establish and manage the sessions, depending on the type and protocol of the target system. For example, PSM-RDP is used for Windows systems, PSM-SSH and PSM-Telnet are used for UNIX systems, PSM-Toad and PSM-SQLPlus are used for Oracle databases, and so on. References:

? PSM for Windows

? Connect through Privileged Session Manager for Windows

? Supported connection components

NEW QUESTION 83

In your organization the "click to connect" button is not active by default. How can this feature be activated?

- A. Policies > Master Policy > Allow EPV transparent connections > Inactive
- B. Policies > Master Policy > Session Management > Require privileged session monitoring and isolation > Add Exception
- C. Policies > Master Policy > Allow EPV transparent connections > Active
- D. Policies > Master Policy > Password Management

Answer: C

Explanation:

The "click to connect" button is a feature that allows users to connect to target systems without entering their credentials manually. It is also known as EPV

transparent connections or PSM transparent connections. To activate this feature, you need to enable the Allow EPV transparent connections parameter in the Master Policy. This parameter determines whether users can use the “click to connect” button to initiate a privileged session from the PVWA. If the parameter is set to Active, the button is enabled and users can connect to target systems with one click. If the parameter is set to Inactive, the button is disabled and users need to copy the credentials and paste them in the target system login screen. References: Connect and configure - CyberArk, How to enable/disable Connect button in PVWA console - force.com

NEW QUESTION 85

A Vault administrator have associated a logon account to one of their Unix root accounts in the vault. When attempting to verify the root account’s password the Central Policy Manager (CPM) will:

- A. ignore the logon account and attempt to log in as root
- B. prompt the end user with a dialog box asking for the login account to use
- C. log in first with the logon account, then run the SU command to log in as root using the password in the Vault
- D. none of these

Answer: C

Explanation:

According to the web search results, when a Vault administrator has associated a logon account to one of their Unix root accounts in the vault, the CPM will log in first with the logon account, then run the SU command to log in as root using the password in the Vault1. This is a common use case for using a logon account, as the best practice for Unix systems is to disallow the root user from logging in using SSH, which is what the CPM uses to sign in to a system to manage the password2. The logon account can be defined on the target account level or on the platform level, making it available to all accounts associated with the platform2. The CPM can also use the logon account to initiate PSM sessions to the target machine3.

NEW QUESTION 89

Vault admins must manually add the auditors’ group to newly created safes so auditors will have sufficient access to run reports.

- A. TRUE
- B. FALSE

Answer: B

Explanation:

Vault admins do not need to manually add the auditors’ group to newly created safes, because the auditors’ group is automatically added to every safe in the vault by default. The auditors’ group has the View Audit authorization, which allows its members to view the safe’s activity and run reports. However, vault admins can remove the auditors’ group from specific safes if they want to restrict the access of the auditors. References: Predefined users and groups - CyberArk

NEW QUESTION 91

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

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

Answer: C

Explanation:

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

References:

? CyberArk Docs - Manage users in PrivateArk client1

NEW QUESTION 92

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 94

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 97

The Active Directory User configured for Windows Discovery needs which permission(s) or membership?

- A. Member of Domain Admin Group
- B. Member of LDAP Admin Group
- C. Read and Write Permissions
- D. Read Only Permissions

Answer: D

Explanation:

The Active Directory User configured for Windows Discovery requires Read Only Permissions. This level of permission allows the user to query and discover objects within the Active Directory without the ability to modify any objects or settings. Having read- only access is sufficient for discovery purposes, as it enables the user to retrieve necessary information without posing a risk of unintended changes to the directory¹.

References:

? Microsoft Learn: Configure discovery methods¹

NEW QUESTION 98

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 103

What is the configuration file used by the CPM scanner when scanning UNIX/Linux devices?

- A. UnixPrompts.ini
- B. plink.exe
- C. dbparm.ini
- D. PVConfig.xml

Answer: A

Explanation:

The configuration file used by the CPM scanner when scanning UNIX/Linux devices is UnixPrompts.ini. This file is located in the CPM scanner installation folder and can be customized according to the UNIX/Linux machine's specific configuration. The file contains parameters that define the prompts and paths for various commands and files used by the CPM scanner, such as login password, sudo password, sudo error, passwd file, group file, shadow file, and sudoers file.

References: Configure the CPM

Scanner, CPM Scanner parameters file (CACPMScanner.exe.config)

NEW QUESTION 108

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 111

Where can PTA be configured to send alerts? (Choose two.)

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

Answer: AB

Explanation:

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

References:

? CyberArk Docs: Send PTA Alerts to Email1

NEW QUESTION 112

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 114

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 117

The vault supports Subnet Based Access Control.

- A. TRUE
- B. FALSE

Answer: A

Explanation:

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

NEW QUESTION 118

In order to connect to a target device through PSM, the account credentials used for the connection must be stored in the vault?

- A. True.
- B. Fals
- C. Because the user can also enter credentials manually using Secure Connect.
- D. Fals
- E. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect.
- F. Fals
- G. Because if credentials are not stored in the vault, the PSM will prompt forcredentials.

Answer: B

Explanation:

In order to connect to a target device through PSM, the account credentials used for the connection do not necessarily have to be stored in the vault. The user can also enter credentials manually using Secure Connect, which 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, etc. To use Secure Connect, the user needs to specify the target system address and the connection component ID in the URL, and then enter the credentials in the PSM login screen1.

The other options are not correct, because:

? A. True. This is not correct, because as explained above, the user can also enter credentials manually using Secure Connect.

? C. False. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect. This is not correct, because PSM Connect 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 PSM Connect user is not used to log into the target device as the end user2.

? D. False. Because if credentials are not stored in the vault, the PSM will prompt for credentials. This is not correct, because this option is essentially the same as Secure Connect, which is the correct answer.

References:

? 1: Secure Connect

? 2: PSMConnect and PSMAdminConnect

NEW QUESTION 123

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

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

Answer: C

Explanation:

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

? Use the CyberArk Backup Process - CyberArk, section “Use the CyberArk Backup Process”

? Install the Vault Backup Utility - CyberArk, section “Backup utilities”

? Disaster Recovery - CyberArk, section “Disaster Recovery”

? Distributed Vaults - CyberArk, section “Distributed Vaults”

? [High Availability - CyberArk], section “High Availability”

NEW QUESTION 126

DRAG DROP

Match each permission to where it can be found.

Add Accounts	Drag answer here	Vault
Initiate CPM account management operations	Drag answer here	Safe
Add/Update Users	Drag answer here	
Add Safes	Drag answer here	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

? Add Accounts: This permission is associated with the ability to add new accounts to the CyberArk Vault. It is typically found in the Vault's administrative settings where account management is handled.

? Initiate CPM account management operations: This permission allows users to initiate operations related to the Central Policy Manager (CPM) for account management within a Safe. It is found in the Safe's permissions settings.

? Add/Update Users: This permission enables the addition or updating of user information in the Vault. It is found in the Vault's user management settings.

? Add Safes: This permission is related to the creation of new Safes in the Vault. It is found in the Vault's administrative settings where Safe management is conducted.

References:

? The permissions and their locations can be referenced in the CyberArk Defender PAM course materials and official documentation, which provide detailed information on the management of permissions within the CyberArk solution.

NEW QUESTION 128

What can you do to ensure each component server is operational?

- A. Logon to PVWA with v10 UI, navigate to Healthcheck, and validate each component server is connected to the Vault.
- B. Ping each component server to ensure connectivity.
- C. Use the PrivateArk client to connect to the Vault server and validate all the services are running.
- D. Install the Vault Server interface on a remote machine to avoid interactive logon to the Vault OS and review the ITALog.log through the Vault Server interface.

Answer: A

Explanation:

To ensure that each component server is operational, you can log on to the Privileged Vault Web Access (PVWA) with the version 10 user interface, navigate to the Healthcheck section, and validate that each component server is connected to the Vault. The System Health dashboard in PVWA provides a high-level visual representation of the health status of the different CyberArk components, including whether the Vault service is up and whether the component servers are connected¹.

References:

? CyberArk Docs - Monitor system health

NEW QUESTION 132

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

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

Answer: A

Explanation:

In a default CyberArk installation, to view the "reports" page in the PVWA (Privileged Web Access), a user must be a member of the PVWAMonitor group¹. This group is specified in the ManageReportsGroup parameter in the Reports section of the Web Access Options in the System Configuration page. Being a member of this group grants the user the necessary permissions to generate and view reports within the PVWA. References:

? CyberArk's official documentation on Reports in PVWA outlines the requirement for users to belong to the PVWAMonitor group to access the reports page and generate reports¹.

NEW QUESTION 133

Your organization requires all passwords be rotated every 90 days. Where can you set this regulatory requirement?

- A. Master Policy
- B. Safe Templates
- C. PVWAConfig.xml
- D. Platform Configuration

Answer: D

Explanation:

The platform configuration defines the password management settings for each type of account, such as the password complexity, rotation frequency, verification method, and reconciliation options. You can set the regulatory requirement for password rotation in the platform configuration by specifying the number of days in the Password Change Interval parameter. This parameter determines how often the CPM will change the passwords of the accounts that are associated with the platform. For example, if you set the Password Change Interval to 90, the CPM will change the passwords every 90 days. References: Credentials Rotation - CyberArk, How do I manage or change passwords stored in CyberArk?

NEW QUESTION 137

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 138

Which permissions are needed for the Active Directory user required by the Windows Discovery process?

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

Answer: D

Explanation:

The Active Directory user required by the Windows Discovery process needs to have Read permissions in the OU to scan and all sub-OUs¹. This allows the Discovery process to scan predefined machines for new and modified accounts and their dependencies without requiring elevated privileges such as Domain Admin or LDAP Admin rights. The Read permission is sufficient for the Discovery process to retrieve the necessary information about the accounts that should be onboarded into the Vault. References:

? CyberArk's official documentation on managing discovery processes outlines the permissions required for the Discovery process, including the need for Read permissions for the Active Directory user performing the discovery¹.

? Additional details on the required credentials for scanning and the Discovery process can be found in the supported target machines section of CyberArk's documentation².

NEW QUESTION 139

The Accounts Feed contains:

- A. Accounts that were discovered by CyberArk in the last 30 days
- B. Accounts that were discovered by CyberArk that have not yet been onboarded
- C. All accounts added to the vault in the last 30 days
- D. All users added to CyberArk in the last 30 days

Answer: B

Explanation:

The Accounts Feed is a feature of the CyberArk Privileged Access Security Solution that enables the discovery and provisioning of privileged accounts in the environment. The Accounts Feed contains the accounts that were discovered by CyberArk that have not yet been onboarded to the Vault. These accounts are displayed in the Pending Accounts page in the PVWA, where the user can view, analyze, and onboard them according to various criteria. The Accounts Feed helps the user to identify and manage the unmanaged privileged accounts that pose a security risk¹.

The other options are not correct, because:

? A. Accounts that were discovered by CyberArk in the last 30 days. This is not correct, because the Accounts Feed does not contain all the accounts that were discovered by CyberArk in the last 30 days, but only the ones that have not yet been onboarded. The accounts that were already onboarded to the Vault are not part of the Accounts Feed, but are displayed in the Accounts page in the PVWA¹.

? C. All accounts added to the vault in the last 30 days. This is not correct, because the Accounts Feed does not contain the accounts that were added to the Vault, but the ones that are waiting to be onboarded. The accounts that were added to the Vault are not part of the Accounts Feed, but are displayed in the Accounts page in the PVWA¹.

? D. All users added to CyberArk in the last 30 days. This is not correct, because the Accounts Feed does not contain the users that were added to CyberArk, but the accounts that are waiting to be onboarded. The users that were added to CyberArk are not part of the Accounts Feed, but are displayed in the Users page in the PVWA¹.

References:

? 1: Accounts Feed

NEW QUESTION 140

For Digital Vault Cluster in a high availability configuration, how does the cluster determine if a node is down?

- A. The heartbeat s no longer detected on the private network.
- B. The shared storage array is offline.
- C. An alert is generated in the Windows Event log.
- D. The Digital Vault Cluster does not detect a node failure.

Answer: A

Explanation:

In a Digital Vault Cluster environment, each node has a Cluster Vault Manager (CVM) service that monitors the local resources and the status of the other node via a private network¹. The CVM service sends a heartbeat signal to the other node every few seconds to check its availability². If the heartbeat is not detected for a certain period of time, the CVM service assumes that the other node is down and triggers a failover process³. The failover process involves shutting down the resources on the failed node and starting them on the available node⁴. References: Digital Vault Cluster environment, CyberArk High-Availability Vault Cluster, Manage the CyberArk Digital Cluster Vault Server, Local resources failover process

NEW QUESTION 141

Select the best practice for storing the Master CD.

- A. Copy the files to the Vault server and discard the CD
- B. Copy the contents of the CD to a Hardware Security Module (HSM) and discard the CD
- C. Store the CD in a secure location, such as a physical safe
- D. Store the CD in a secure location, such as a physical safe, and copy the contents of the CD to a folder secured with NTFS permissions on the Vault

Answer: C

Explanation:

The best practice for storing the Master CD is to store it in a secure location, such as a physical safe. The Master CD contains the server key, the public recovery key, and the private recovery key, which are essential for starting, operating, and recovering the Vault. These keys are sensitive and should be protected from unauthorized access, loss, or damage. Therefore, storing the CD in a physical safe ensures that the keys are kept in a secure location when not in use, and that they are available when needed. This is the recommended option by CyberArk¹.
 The other options are not best practices and should be avoided, as they expose the keys to potential risks, such as theft, corruption, or deletion. Copying the files to the Vault server and discarding the CD is not secure, as it makes the keys accessible to anyone who can access the Vault server or compromise its security. Copying the contents of the CD to a Hardware Security Module (HSM) and discarding the CD is not feasible, as the HSM can only store the server key, not the recovery keys². Storing the CD in a secure location, such as a physical safe, and copying the contents of the CD to a folder secured with NTFS permissions on the Vault is not necessary, as it creates redundant copies of the keys that may not be synchronized or updated. Moreover, NTFS permissions are not sufficient to protect the keys from malicious or accidental actions. References:
 ? Server Keys - CyberArk, section "Server Keys"
 ? Store the Server Key in an HSM - CyberArk, section "Store the Server Key in an HSM"

NEW QUESTION 144

Which change could CyberArk make to the REST API that could cause existing scripts to fail?

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

Answer: C

Explanation:

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

NEW QUESTION 148

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

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

Answer: A

Explanation:

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

NEW QUESTION 151

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 156

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 160

What is the purpose of the CyberArk Event Notification Engine service?

- A. It sends email messages from the Central Policy Manager (CPM)
- B. It sends email messages from the Vault
- C. It processes audit report messages
- D. It makes Vault data available to components

Answer: B

Explanation:

The purpose of the CyberArk Event Notification Engine service is to send email notifications about Privileged Access Security solution activities automatically to predefined users. It is installed automatically as part of the Vault server installation as a service. The Event Notification Engine (ENE) can be configured to send email notifications for various events, such as password changes, password verifications, account onboarding, account deletion, audit reports, alerts, and more. The ENE can also support encrypted and authenticated email notifications, as well as high availability implementations¹. References:

? Event Notification Engine - CyberArk, section "Event Notification Engine"

NEW QUESTION 164

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 166

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

- A. TRUE
- B. FALSE

Answer: B

Explanation:

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

References:

? 1: Vault Member Authorizations

NEW QUESTION 169

When managing SSH keys, the CPM stored the Private Key

- A. In the Vault
- B. On the target server
- C. A & B
- D. Nowhere because the private key can always be generated from the public key.

Answer: A

Explanation:

When managing SSH keys, the CPM stores the private key in the Vault. The CPM generates a new random SSH key pair and updates the public SSH key on the target server. The new private SSH key is then stored in the Digital Vault where it benefits from all the accessibility and security features of the Vault. The private SSH key is never stored on the target server, as this would expose it to unauthorized access or theft. The private SSH key cannot be generated from the public key, as this would defeat the purpose of asymmetric encryption. References:

? Manage SSH Keys

? SSH Key Manager

? Use SSH Keys

NEW QUESTION 171

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 175

DRAG DROP

ADR Vault became active due to a failure of the primary Vault. Service on the primary Vault has now been restored. Arrange the steps to return the DR vault to its normal standby mode in the correct sequence.

Unordered Options

Shut down the PrivateArk Server Service on the DR Vault.

In the PADR.ini file, set Failover Mode = No and remove the last two lines.

Start the PrivateArk Disaster Recovery Service.

↔

Ordered Response

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

? Shut down the PrivateArk Server Service on the DR Vault.

? In the PADR.ini file, set Failover Mode = No and remove the last two lines.

? Start the PrivateArk Disaster Recovery Service.

Comprehensive Explanation: When the primary Vault service has been restored and you need to return the DR Vault to its normal standby mode, the steps are as follows:

? Shut down the PrivateArk Server Service on the DR Vault to stop the Vault from being active.

? Modify the PADR.ini file by setting Failover Mode to No and removing the last two lines that were added during the failover process. This reconfigures the DR Vault to standby mode.

? Start the PrivateArk Disaster Recovery Service to complete the transition back to standby mode1.

References:

? CyberArk Docs - Initiate a DR Failback to the Production Vault1

NEW QUESTION 176

Which is the primary purpose of exclusive accounts?

- A. Reduced risk of credential theft
- B. More frequent password changes
- C. Non-repudiation (individual accountability)

D. To force a 'collusion to commit' fraud ensuring no single actor may use a password without authorization

Answer: D

Explanation:

According to the web search results, exclusive accounts are a feature of CyberArk Defender PAM that enables organizations to permit users to check out a 'one-time' password and lock it so that no other users can retrieve it at the same time¹. After the user has used the password, the user checks the password back into the Vault. This ensures exclusive usage of the privileged account, enabling full control and tracking for the password. The duration of the check-out period can be configured in the platform settings for each account¹.

The primary purpose of exclusive accounts is to prevent a single user from accessing a sensitive account without authorization, which could lead to fraud or misuse of privileges. By requiring a check-out and check-in process, exclusive accounts ensure that there is a 'collusion to commit' fraud, meaning that at least two users are involved in the malicious activity and are accountable for it. One user must check out the password and use it, while another user must approve the check-in and verify the password change. This way, exclusive accounts add an additional measure of protection and accountability for accessing sensitive accounts.

NEW QUESTION 177

You want to generate a license capacity report. Which tool accomplishes this?

- A. Password Vault Web Access
- B. PrivateArk Client
- C. DiagnoseDB Report
- D. RestAPI

Answer: B

Explanation:

The license capacity report is a tool that provides information about the licensed user types and objects in the Vault. It enables users to see the maximum number of licenses for each user type or object, and the number of used licenses for each one. Only user types and objects that are limited by the license are displayed in this report. To generate a license capacity report, users need to use the PrivateArk Client, which is a graphical user interface that allows users to manage safes and their properties. Users can access the report from the Tools menu in the PrivateArk Client. References: Reporting License Usage, Manage the CyberArk License

NEW QUESTION 182

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 185

SAFE Authorizations may be granted to . Select all that apply.

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

Answer: ABCD

Explanation:

SAFE Authorizations may be granted to Vault Users, Vault Groups, LDAP Users, and LDAP Groups. These are the four types of users that can be defined in the Vault and assigned permissions to access Safes and manage passwords. Vault Users and Vault Groups are created and managed within the Vault, while LDAP Users and LDAP Groups are imported from an external directory service such as Active Directory. References:

? Defender PAM Course, Module 4: Managing Safes, Lesson 4.2: Safe Authorizations, slide 4

? Defender PAM Sample Items Study Guide, Question 39, page 15

? CyberArk Privileged Access Security Documentation, Vault Administration Guide, Chapter 4: Managing Safes, Section: Safe Authorizations, page 4-12

NEW QUESTION 189

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 193

You need to enable the PSM for all platforms. Where do you perform this task?

- A. Platform Management > (Platform) > UI & Workflows
- B. Master Policy > Session Management
- C. Master Policy > Privileged Access Workflows
- D. Administration > Options > Connection Components

Answer: A

Explanation:

To enable PSM for specific platforms, you need to go to Platform Management, select the platform you want to configure, click Edit, expand UI & Workflows, and select Privileged Session Management. There you can customize the PSM settings for that platform, such as the PSM server ID, the connection components, the PSM connection method, and the PSM recording options. You can also disable dual control for PSM connections if needed. References: Configure PSM for Specific Platforms

NEW QUESTION 198

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 202

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

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

Answer: A

Explanation:

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

? Configure PTA Remediations - CyberArk, section "Remediation Initiation"

NEW QUESTION 207

You received a notification from one of your CyberArk auditors that they are missing Vault level audit permissions. You confirmed that all auditors are missing the Audit Users Vault permission.

Where do you update this permission for all auditors?

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

Answer: B

Explanation:

To update the Vault level audit permissions for all auditors, you would use the Private Ark Client. Specifically, you would navigate to the Tools menu, select Administrative Tools, then Users and Groups. Within the Users and Groups section, you would select the Auditors group and go to the Authorizations tab. Here, you can manage and update the permissions for the Auditor group, including the Audit Users Vault permission. This ensures that all members of the Auditors group have the necessary permissions to perform their audit functions within the Vault1.

References:

- ? CyberArk's official documentation on predefined users and groups, which includes information on the Auditor user and the permissions associated with this role¹.
- ? Information on the administrative tools available in the Private Ark Client, which are used for managing users and groups, including auditors².

NEW QUESTION 212

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 214

What is the purpose of the Interval setting in a CPM policy?

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

Answer: A

Explanation:

The Interval setting in a CPM policy is used to control how often the CPM looks for System Initiated CPM work, such as password changes, verifications, and reconciliations. The Interval setting defines the frequency, in minutes, that the CPM will check the accounts that are associated with the policy and perform the required actions. For example, if the Interval is set to 60, the CPM will check the accounts every hour and change, verify, or reconcile the passwords according to the policy settings. The Interval setting does not affect User Initiated CPM work, such as manual password changes or retrievals, which are performed immediately upon request. The Interval setting also does not control how long the CPM rests between password changes or the maximum amount of time the CPM will wait for a password change to complete. These parameters are configured in the CPM.ini file, which is stored in the root folder of the <CPM username> Safe. References:
? [Defender PAM eLearning Course], Module 5: Password Management, Lesson 5.1: CPM Policies, Slide 9: CPM Policy Settings
? [Defender PAM Sample Items Study Guide], Question 4: CPM Policy Settings
? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 5: Managing Passwords, Section: CPM Policy Settings, Subsection: Interval

NEW QUESTION 219

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 220

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

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

Answer: D

Explanation:

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

NEW QUESTION 223

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 226

DRAG DROP

Match each PTA alert category with the PTA sensors that collect the data for it.

unmanaged privileged account	Drag answer here	Vault
anomalous access to multiple machines	Drag answer here	Logs, Vault, AWS (optional), Azure (optional)
suspicious activities detected in a privileged session	Drag answer here	Logs, Vault, AD (optional), AWS (optional), Azure (optional)
suspected credentials theft	Drag answer here	Network Sensor, PTA Windows Agent

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 231

DRAG DROP

A new HTML5 Gateway has been deployed in your organization.
From the PVWA, arrange the steps to configure a PSM host to use the HTML5 Gateway in the correct sequence.

Unordered Options

Administration>Options

Privileged Session Management

Configured PSM Servers and select existing PSM host

Connection Details

Add PSM gateway

Ordered Response

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

To configure a PSM host to use the HTML5 Gateway from the PVWA, you would typically follow these steps:
? Log into the PVWA with an administrative user.
? Navigate to Administration > Options.
? Right-click on Privileged Session Management and select Add Configured PSM Gateway Servers.
? Right-click Configured PSM Gateway Servers, then Add PSM Gateway Server.
? Select the newly added gateway server and enter a unique ID for the PSM HTML5 Gateway.
? Expand the newly created gateway server and enter the necessary configuration details.
Please note that these steps are based on general procedures for configuring a PSM host with an HTML5 Gateway and should be verified against the official CyberArk documentation or by a qualified CyberArk professional. For detailed instructions and best practices, refer to the CyberArk documentation123.

NEW QUESTION 236

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

- A. TRUE

B. FALSE

Answer: A

Explanation:

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

NEW QUESTION 238

You have been asked to secure a set of shared accounts in CyberArk whose passwords will need to be used by end users. The account owner wants to be able to track who was using an account at any given moment. Which security configuration should you recommend?

- A. Configure one-time passwords for the appropriate platform in Master Policy.
- B. Configure shared account mode on the appropriate safe.
- C. Configure both one-time passwords and exclusive access for the appropriate platform in Master Policy.
- D. Configure object level access control on the appropriate safe.

Answer: C

Explanation:

One-time passwords and exclusive access are security features that can be configured for a platform in the Master Policy. These features enhance the security and accountability of shared accounts by ensuring that each password is used only once and by only one user at a time. One-time passwords generate a new password for each check-out and check-in of an account, preventing password reuse and exposure. Exclusive access prevents multiple users from accessing the same account simultaneously, avoiding conflicts and confusion. By configuring both one-time passwords and exclusive access for the appropriate platform, the account owner can track who was using an account at any given moment and ensure that the passwords are always secure and unique. References
: One-Time Passwords, Exclusive Access, Master Policy

NEW QUESTION 242

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

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

Answer: ACD

Explanation:

When users are unable to launch Web Type Connection components from the PSM server, the CyberArk Support Team will require specific logs to debug the issue. The logs that are typically helpful in such cases include:

? PSMConsole.log: This log file contains informational messages and errors related to the PSM function, which can help identify issues with the PSM server's operation¹.

? PSMTrace.log: This log file includes errors and trace messages, which can provide detailed insights into the issues occurring during the PSM server's processes¹.

? <Session_ID>.Component.log: This log file contains errors and trace messages related to the connection component, which can be crucial for troubleshooting issues with launching Web Type Connection components¹.

These logs can provide the necessary information to understand the problem and assist the support team in resolving the issue effectively.

References:

? CyberArk's official documentation on PSM for Web Troubleshooting, which outlines the types of logs available and their purposes in the troubleshooting process¹.

? Additional resources on managing and interpreting PSM logs, which provide guidance on using logs for diagnosing and resolving issues with the PSM server²

NEW QUESTION 246

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

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

Answer: AB

Explanation:

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

References:

? CyberArk's official documentation on troubleshooting authentication issues, which includes steps on updating user passwords and creating new credential files¹.

? Community discussions and support articles on resolving DR user authentication failures, which provide practical insights and recommended actions²

NEW QUESTION 250

You receive this error:

“Error in changepass to user domain\user on domain server(\domain.(winRc=5) Access is denied.”

Which root cause should you investigate?

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

Answer: A

Explanation:

The error message “Error in changepass to user domain\user on domain server(\domain.(winRc=5) Access is denied” suggests that the account attempting to change the password does not have the necessary permissions to do so. This could be due to several reasons, such as the account not being part of the appropriate group with password change privileges, or specific restrictions set on the account that prevent password changes. It’s important to verify the account’s permissions and ensure it has the ability to change its own password within the domain.

References: The conclusion is based on common issues encountered in CyberArk’s Privileged Access Management (PAM) when managing account passwords and the associated error codes. The CyberArk documentation and community discussions provide insights into troubleshooting such errors, where insufficient permissions are a frequent cause

NEW QUESTION 253

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

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

Answer: B

Explanation:

The PTA can automatically suspend sessions if suspicious activities are detected in a privileged session, regardless of the session method. The PTA can suspend sessions that are made via the PSM, the PVWA, or directly to the target system. The PTA can also suspend sessions that are made via SSH, RDP, or other protocols. References:

? Defender PAM Sample Items Study Guide, page 24

? PTA User Guide, page 17

NEW QUESTION 258

DRAG DROP

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

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

- 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 263

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

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

Answer: C

Explanation:

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


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

This parameter instructs the CPM to log in to the system as the logon account, enter the logon password, run the su - command to switch to the root user, enter the logon password again, run the change command to change the root password, exit the root session, and exit the logon session1.

The other options are not correct, as follows:

- ? A. Log in to the system as root, then change root's password. This option is not possible, because the root account cannot be used for direct logon. The logon account is associated with the root account to enable the CPM to access the system and change the password1.
- ? B. Log in to the system as the logon account, then change root's password. This option is not effective, because the logon account does not have the permission to change the root's password. The logon account needs to elevate itself to the root user by using the su command before changing the password1.
- ? D. None of these. This option is not valid, because there is a correct answer among the choices.

References:

? 1: Logon Accounts for SSH and Telnet Connections

NEW QUESTION 266

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 267

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 272

.....

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](#)