

Exam Questions PAM-DEF

CyberArk Defender - PAM

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



NEW QUESTION 1

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

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

Answer: C

Explanation:

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

NEW QUESTION 2

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

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

Answer: A

Explanation:

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

NEW QUESTION 3

Which one the following reports is NOT generated by using the PVWA?

- A. Accounts Inventory
- B. Application Inventory
- C. Sales List
- D. Convince Status

Answer: C

Explanation:

The PVWA can generate various reports on the privileged accounts and applications in the system, based on different filters and criteria. However, the Safes List report is not one of them. The Safes List report is generated by using the PrivateArk Client, and it provides a list of Safes and their properties according to location. References: Defender-PAM Study Guide, Reports and Audits

NEW QUESTION 4

The vault supports Role Based Access Control.

- A. TRUE
- B. FALSE

Answer: A

Explanation:

The vault supports Role Based Access Control (RBAC), which is a method of granting access to resources based on the roles of users or groups. RBAC enables the administrator to define roles that represent different functions or responsibilities in the organization, and assign permissions to those roles according to the principle of least privilege. Users or groups can then be assigned to one or more roles, and inherit the permissions of those roles. RBAC simplifies the management of access control by reducing the complexity and redundancy of assigning permissions to individual users or groups. RBAC also enhances security and compliance by ensuring that users or groups only have the minimum level of access required to perform their tasks¹.

References:

? 1: Role Based Access Control

NEW QUESTION 5

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

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

Answer:

A

Explanation:

When a new domain controller is added to a domain, it is necessary to update the CyberArk infrastructure to ensure it can use the new domain controller for authentication. This involves updating the hosts file on the Vault server located at Windows\System32\Etc\Hosts to include the new domain controller's details. Additionally, within the PVWA Application, you need to navigate to Administration > LDAP Integration > Directories > Hosts and update the information there as well. This ensures that both the Vault server and the PVWA Application are aware of the new domain controller and can authenticate against it¹.

References:

? CyberArk's official documentation on configuring Active Directory integration, which includes details on setting up domain controllers for authentication².

? Information on adding Active Directory as a directory service in CyberArk Identity, which discusses the integration of domain controllers³.

NEW QUESTION 6

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

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

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

Answer: AB

Explanation:

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

? [Defender PAM Sample Items Study Guide], page 10, question 5

? [CyberArk Privileged Access Security Implementation Guide], page 30, table 2-1

? [CyberArk Privileged Access Security Administration Guide], page 43, section 3.2.2.1

NEW QUESTION 7

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

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

Answer: AC

Explanation:

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

NEW QUESTION 8

A new HTML5 Gateway has been deployed in your organization. Where do you configure the PSM to use the HTML5 Gateway?

- A. Administration > Options > Privileged Session Management > Configured PSM Servers> Connection Details > Add PSM Gateway
- B. Administration > Options > Privileged Session Management > Add Configured PSMGateway Servers
- C. Administration > Options > Privileged Session Management > Configured PSM Servers> Add PSM Gateway
- D. Administration > Options > Privileged Session Management > Configured PSM Servers> Connection Details

Answer: C

Explanation:

After deploying a new HTML5 Gateway in your organization, you configure the PSM to use the HTML5 Gateway by navigating to the Administration section in the PVWA. From there, you go to Options, then Privileged Session Management, and under Configured PSM Servers, you will find the option to Add PSM Gateway¹. This is where you can specify the details of the newly deployed HTML5 Gateway to ensure that the PSM can utilize it for secure remote access to target machines through an HTML5-based session. References:

? CyberArk's official documentation provides a step-by-step guide on how to install and configure the PSM HTML5 Gateway, including the process of adding the gateway to the PSM configuration¹.

? For more detailed instructions and best practices on configuring the PSM with an HTML5 Gateway, refer to the CyberArk Defender PAM course materials and study guides

NEW QUESTION 9

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 10

What is the purpose of the PrivateArk Database service?

- A. Communicates with components
- B. Sends email alerts from the Vault
- C. Executes password changes
- D. Maintains Vault metadata

Answer: D

Explanation:

The purpose of the PrivateArk Database service is to maintain the Vault metadata, which includes the information about the Safes, accounts, policies, users, groups, and audit records that are stored in the Vault. The PrivateArk Database service is a Windows service that manages the database files that contain the Vault data. The PrivateArk Database service is responsible for creating, updating, deleting, and backing up the database files, as well as performing encryption and compression operations on the data¹. The PrivateArk Database service is installed automatically as part of the Vault server installation and can be configured using the DBParm.ini file².

The other options are not the purpose of the PrivateArk Database service, although they may be related to other services or components of the Vault. The PrivateArk Server service is the service that communicates with the components, such as the PVWA, the CPM, the PSM, and the PTA, and handles the requests from the clients and components³. The Event Notification Engine service is the service that sends email alerts from the Vault, based on predefined events and recipients⁴. The Central Policy Manager component is the component that executes password changes, verifications, and reconciliations for the accounts that are managed by the Vault. References:

- ? Server Components - CyberArk, section “The PrivateArk Server process (Dbmain)”
- ? DBParm.ini - CyberArk, section “Main parameters”
- ? Server Components - CyberArk, section “The PrivateArk Server process (Dbmain)”
- ? Event Notification Engine - CyberArk, section “Event Notification Engine”
- ? [Change Passwords - CyberArk], section “Change Passwords”

NEW QUESTION 10

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

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

Answer: A

Explanation:

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

- ? CyberArk Docs: Connect through PSM for SSH¹
- ? CyberArk Docs: Connect to Unix machines (using PSM for SSH)²

NEW QUESTION 14

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

- A. TRUE
- B. FALSE

Answer: B

Explanation:

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

- ? Predefined users and groups
- ? Safe member authorizations

NEW QUESTION 16

DRAG DROP

Match each automatic remediation to the correct PTA security event.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

References:

? CyberArk Docs: Configure security events

NEW QUESTION 17

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 22

You are logging into CyberArk as the Master user to recover an orphaned safe.

Which items are required to log in as Master?

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

Answer: A

Explanation:

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

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

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

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

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

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

NEW QUESTION 26

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

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

Answer: C

Explanation:

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

NEW QUESTION 28

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

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

Answer: D

Explanation:

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

? CyberArk Docs: One-time passwords and exclusive accounts¹

? CyberArk Knowledge Article: CPM: What is the difference between "One Time" and "Exclusive" passwords?²

NEW QUESTION 33

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 37

Platform settings are applied to .

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

Answer: D

Explanation:

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

NEW QUESTION 42

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

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

Answer: D

Explanation:

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

is running if the user was able to conduct a session, and the PVWAMonitor group is not a valid group in CyberArk. References:
 ? Monitor Privileged Sessions - CyberArk, section "The MONITORING page"

NEW QUESTION 45

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

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

Answer: A

Explanation:

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

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

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

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

References: Manage SSH Keys, Use SSH Keys

NEW QUESTION 47

DRAG DROP

Match each key to its recommended storage location.

Recovery Private Key	Drag answer here	Store on the Vault Server Disk Drive
Recovery Public Key	Drag answer here	Store in a Hardware Security Module
Server Key	Drag answer here	Store in a Physical Safe
SSH Keys	Drag answer here	Store in the Vault

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

? The recommended storage locations for each key are as follows:

? Recovery Private Key: It is recommended to store the Recovery Private Key on the Vault Server Disk Drive. This is because the Recovery Private Key is used to decrypt the data stored in the Vault.

? Recovery Public Key: It is recommended to store the Recovery Public Key in a Hardware Security Module. This is because the Recovery Public Key is used to encrypt the data stored in the Vault.

? Server Key: It is recommended to store the Server Key in a Physical Safe. This is because the Server Key is used to open the Vault, much like the key of a physical Vault. The key is required to start the Vault, after which the Server Key can be removed until the Server is restarted. When the Vault is stopped, the information stored in the Vault is completely inaccessible without that key.

? SSH Keys: It is recommended to store the SSH Keys in the Vault. This is because the SSH Keys are used to connect to remote machines using the SSH protocol. The Vault can manage the passwords and sessions for the SSH Keys and provide secure access to the target systems.

References: Server keys - CyberArk, Cyberark Key Storage Plugin (Enterprise) - Rundeck

NEW QUESTION 52

You need to recover an account localadmin02 for target server 10.0.123.73 stored in Safe Team1.

What do you need to recover and decrypt the object? (Choose three.)

- A. Recovery Private Key
- B. Recover.exe
- C. Vault data
- D. Recovery Public Key
- E. Server Key
- F. Master Password

Answer: ABC

Explanation:

To recover and decrypt an account that is stored in a Safe, you need the following items:

? Recovery Private Key: This is a key that is used to decrypt the data stored in the Vault. It is located on the Master CD, which is a physical CD that contains the Private Recovery Key, a file named RecPriv.key.

? Recover.exe: This is a utility that is used to recover information from a Safe's external files in case of loss or corruption of that Safe. The files are decrypted and saved as readable files. The utility can be run from the command line or the graphical user interface.

? Vault data: This is the data that is stored in the Vault, such as accounts, safes, platforms, policies, users, groups, and audit records. The Vault data is encrypted

using the Recovery Public Key, which is a key that is used to encrypt the data stored in the Vault. The Vault data can be recovered from the Vault server disk drive or from a backup file.

References: Recover, Server keys, Export Vault Information

NEW QUESTION 56

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 61

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 63

To ensure all sessions are being recorded, a CyberArk administrator goes to the master policy and makes configuration changes.

Which configuration is correct?

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

Answer: C

Explanation:

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

NEW QUESTION 64

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

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

Answer: D

Explanation:

According to the CyberArk Defender PAM documentation¹, the Master user is the only user that can access all passwords in the Vault. The Master user is a special user that is created during the initial installation of the Vault and has full permissions on all Safes and accounts in the Vault. The Master user can also perform administrative tasks, such as backup and restore the Vault, change the Vault license, and manage the recovery key. The Master user is the only user that can log on to the Vault in case of a disaster using the recovery key. The Master user's password is not stored in the Vault and cannot be changed or retrieved by any other user.

The Administrator user is a predefined user that is created during the initial installation of the Vault and has the Vault Admin authorization. The Administrator user can perform administrative tasks, such as create and manage users and groups, define platforms and policies, and monitor Vault activity. However, the Administrator user cannot access any passwords in the Vault unless they are explicitly added as a member of a Safe that contains the passwords².

The Vault administrators group is a predefined group that is created during the initial installation of the Vault and has the Vault Admin authorization. The members of the Vault administrators group can perform the same administrative tasks as the Administrator user, but they cannot access any passwords in the Vault unless

they are explicitly added as a member of a Safe that contains the passwords2.

The auditors group is a predefined group that is created during the initial installation of the Vault and has the Audit Users authorization. The members of the auditors group can view

and generate reports on the Vault activity, but they cannot access any passwords in the Vault unless they are explicitly added as a member of a Safe that contains the passwords2. References:

? Master User - CyberArk

? Predefined users and groups - CyberArk

NEW QUESTION 67

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 70

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 74

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

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

Answer: ABC

Explanation:

To add a user directly to the Vault Admin Group in CyberArk, you can use the following methods:

? REST API: The REST API allows for programmatic management of users and groups within the Vault, including adding users to the Vault Admin Group1.

? PrivateArk Client: The PrivateArk Client provides a graphical interface for managing users and groups, and it can be used to add users directly to the Vault Admin Group2.

? PACLI: The PACLI (Privileged Access Command Line Interface) is a command- line tool that enables administrators to manage the Vault, including adding users to groups2.

These methods provide different ways to manage users and their group memberships within the CyberArk Vault, offering flexibility for administrators to choose the most suitable approach for their needs.

References:

? CyberArk’s official documentation on using the REST API to manage users and groups1.

? Information on managing users and groups through the PrivateArk Client and PACLI2.

NEW QUESTION 76

Which of the following properties are mandatory when adding accounts from a file? (Choose three.)

- A. Safe Name
- B. Platform ID
- C. All required properties specified in the Platform
- D. Username
- E. Address
- F. Hostname

Answer: ABC

Explanation:

When adding accounts from a file, certain properties are mandatory to ensure that the accounts can be properly managed within the CyberArk Privileged Access Security system. The Safe Name is required to determine where the account will be stored.

The Platform ID is necessary to apply the correct management policies to the account. Additionally, all required properties specified in the Platform must be included to meet the specific requirements for account management as defined by the platform configuration¹.

References:

? CyberArk's official documentation on adding multiple accounts from a file, which outlines the mandatory information needed for each account, including Safe Name, Platform ID, and other required properties based on the account's policy requirements¹.

NEW QUESTION 81

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

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

Answer: A

Explanation:

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

? 1: Privileged Account Management, Min Validity Period subsection

NEW QUESTION 85

When on-boarding account using Accounts Feed, Which of the following is true?

- A. You must specify an existing Safe where account will be stored when it is on boarded to the Vault
- B. You can specify the name of a new safe that will be created where the account will be stored when it is on-boarded to the Vault.
- C. You can specify the name of a new Platform that will be created and associated with the account
- D. Any account that is on boarded can be automatically reconciled regardless of the platform it is associated with.

Answer: B

Explanation:

When on-boarding accounts using Accounts Feed, you can either select an existing safe or create a new one to store the accounts. You can also specify the platform, policy, and owner for each account. However, you cannot create a new platform using Accounts Feed, and not all platforms support automatic reconciliation. References:

? Accounts Feed - CyberArk

? CyberArk University

? [Defender-PAM Sample Items Study Guide]

NEW QUESTION 89

A password compliance audit found:

- 1) One-time password access of 20 domain accounts that are members of Domain Admins group in Active Directory are not being enforced.
- 2) All the sessions of connecting to domain controllers are not being recorded by CyberArk PSM.

What should you do to address these findings?

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

Answer: A

Explanation:

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

? CyberArk Docs: One-time passwords and exclusive accounts¹

NEW QUESTION 90

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 \:*<>|. 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 93

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 98

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 102

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

- A. TRUE
- B. FALSE

Answer: B

Explanation:

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

NEW QUESTION 106

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 111

What is the maximum number of levels of authorization you can set up in Dual Control?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B

Explanation:

Dual Control is a feature that allows you to set up a workflow for approving access requests to sensitive accounts. You can configure up to two levels of authorization for each account, meaning that you need up to two different authorizers to approve the request before the user can access the account. The authorizers can be either users or groups, and they can have different approval methods, such as email, SMS, or CyberArk interface. References:

? [Defender PAM] course, Module 5: Privileged Session Management, Lesson 5.2:

Dual Control

? [Defender PAM Sample Items Study Guide], Question 31

? [CyberArk Documentation], Dual Control

NEW QUESTION 115

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

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

Answer: C

Explanation:

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

References:

? CyberArk Docs - Manage users in PrivateArk client1

NEW QUESTION 120

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 125

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 127

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 128

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

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

Answer: ABC

Explanation:

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

? Configure ad hoc connections

? Ad Hoc Connections

? Privileged Remote Access Management – PAM Remote Access

NEW QUESTION 130

Which report shows the accounts that are accessible to each user?

- A. Activity report
- B. Entitlement report
- C. Privileged Accounts Compliance Status report
- D. Applications Inventory report

Answer: B

Explanation:

The report that shows the accounts that are accessible to each user is the Entitlement report. According to the web page in the edge browser, the Entitlement report provides information about users' entitlement rights in PAM - Self-Hosted regarding user, Safe, active platform, target machine, target account, etc. This report includes each user's effective access control and authorization level on each account that the user has access to in PAM - Self-Hosted. The Entitlement report can be generated in PVWA or PrivateArk1.

NEW QUESTION 132

It is possible to restrict the time of day, or day of week that a [b]reconcile[/b] process can occur

- A. TRUE
- B. FALSE

Answer: A

Explanation:

It is possible to restrict the time of day, or day of week that a reconcile process can occur by using the Reconcile Safe option in thePlatform Management section of thePrivateArk Client. This option allows the administrator to define the reconcile schedule for each platform, which specifies when the reconcile process can run and how often it should be performed. The reconcile schedule can be set to run daily, weekly, monthly, or on specific days and times. By restricting the reconcile process, the administrator can reduce the risk of unauthorized access to the accounts and improve the performance of the system. References:

? [Defender PAM Course], Module 5: Reconcile and Rotate, Lesson 1: Reconcile and Rotate Overview, Slide 9: Reconcile Safe

? [Defender PAM Study Guide], Section 5.1: Reconcile and Rotate Overview, Page 24: Reconcile Safe

? [CyberArk Documentation], Privileged Access Security Implementation Guide, Chapter 5: Configure the Vault, Section 5.4: Configure Platforms, Subsection 5.4.2: Reconcile Safe

NEW QUESTION 137

What is the primary purpose of One Time Passwords?

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

Answer: A

Explanation:

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

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

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

? C. Non-repudiation (individual accountability). This is not the primary purpose of

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

? D. To force a 'collusion to commit' fraud ensuring no single actor may use a

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

References:

? 1: One-time password

NEW QUESTION 140

VAULT authorizations may be granted to .

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

Answer: AC

Explanation:

Vault Authorizations

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

NEW QUESTION 142

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

- A. True
- B. False

Answer: A

Explanation:

According to the web search results, a Simple Mail Transfer Protocol (SMTP) integration is critical for monitoring Vault activity and facilitating workflow processes, such as Dual Control. SMTP is a protocol that enables the sending and receiving of email messages. By integrating SMTP with CyberArk Defender PAM, the Event Notification Engine (ENE) can automatically send email notifications about PAM activities to predefined users¹. For example, the ENE can notify users about password requests, password confirmations, password changes, password verifications, password reconciliations, password access, password usage, password expiration, and password violations¹. The ENE can also notify users about system events, such as Vault backup, Vault restore, Vault shutdown, Vault startup, and Vault license expiration¹. These notifications help to monitor the Vault activity and ensure compliance with the security policies.

SMTP integration is also essential for facilitating workflow processes, such as Dual Control. Dual Control is a feature that enables authorized Safe owners to either grant or deny requests to access accounts. This feature adds an additional measure of protection, in that it enables you to see who wants to access the information in the Safe, when, and for what purpose. The Master Policy enables organizations to ensure that passwords can only be retrieved after permission or 'confirmation' has been granted from an authorized Safe Owner(s). This is known as Dual Control². SMTP integration enables the ENE to send email notifications to the requesters and the confirmers about the status of the password requests. The ENE can also send reminders to the confirmers if they have not responded to the requests within a specified time period². These notifications help to streamline the workflow process and ensure timely and secure access to the accounts.

References:

? Email notifications - CyberArk

? Dual Control - CyberArk

NEW QUESTION 146

Where can you check that the LDAP binding is using TCP/636?

- A. in Active Directory under "Users OU" => "User Properties" => "External Bindings" => "Port"
- B. in PVWA, under "LDAP Integration" => "LDAP" => "Directories" => "" => "Hosts" => "Host"
- C. in PrivateArk Client, under "Tools" => "Administrative Tools" => "Directory Mapping" => ""
- D. From the PVWA, connect to the domain controller using Test-NetConnection on Port 636.

Answer: D

Explanation:

To check that the LDAP binding is using TCP/636, you can use the Test- NetConnection cmdlet from the PVWA to connect to the domain controller on Port 636. This method allows you to verify that the LDAP service is listening on the secure port and that the connection can be established using SSL/TLS, which is typically associated with port 636¹.

References:

? CyberArk Docs - LDAP Integration²

? CyberArk Knowledge Article - How to test outgoing LDAP external directory connectivity to the vault

NEW QUESTION 148

You created a new safe and need to ensure the user group cannot see the password, but can connect through the PSM.

Which safe permissions must you grant to the group? (Choose two.)

- A. List Accounts Most Voted
- B. Use Accounts Most Voted

- C. Access Safe without Confirmation
- D. Retrieve Files
- E. Confirm Request

Answer: BD

Explanation:

To ensure that a user group can connect through the Privileged Session Manager (PSM) without seeing the password, you must grant the Use Accounts and Retrieve Files permissions to the group for the safe. The Use Accounts permission allows users to initiate sessions using accounts without viewing the account details or

passwords. The Retrieve Files permission enables users to retrieve files during PSM sessions without having access to the passwords¹.

References:

? CyberArk Docs - Safe Permissions

NEW QUESTION 149

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 150

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

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

Answer: AB

Explanation:

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

References:

? CyberArk Docs - Reports in PVWA¹

? CyberArk Docs - Generate the Report²

NEW QUESTION 153

DRAG DROP

Match the log file name with the CyberArk Component that generates the log.

ITALog		PTA
pm.log		Vault
diamond.log		CPM
CyberArk.WebApplication.log		PVWA

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

? Log Files

? [Defender PAM Sample Items Study Guide], Question 46, page 16

NEW QUESTION 155

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

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

Answer: C

Explanation:

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

NEW QUESTION 156

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 159

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 164

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 167

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

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

Answer: D

Explanation:

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

References:

? CyberArk Docs - Onboarding rules

NEW QUESTION 172

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 174

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 175

You created a new platform by duplicating the out-of-box Linux through the SSH platform.

Without any change, which Text Recorder Type(s) will the new platform support? (Choose two.)

- A. SSH Text Recorder
- B. Universal Keystrokes Text Recorder
- C. Events Text Recorder
- D. SQL Text Recorder
- E. Telnet Commands Text Recorder

Answer: AB

Explanation:

When a new platform is created by duplicating the out-of-the-box Linux through the SSH platform, it will support the SSH Text Recorder and the Universal Keystrokes Text Recorder by default. The SSH Text Recorder is designed to record all the keystrokes that are typed during privileged sessions on SSH connections¹. The Universal Keystrokes Text Recorder can record all the keystrokes that are typed during privileged sessions on all supported connections¹. These text recorders are automatically enabled at the Master Policy level and can be customized at the platform level¹. References:

? CyberArk Docs: Recordings and Audits

NEW QUESTION 178

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 179

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 182

You are troubleshooting a PVWA slow response. Which log files should you analyze first? (Choose two.)

- A. ITALog.log
- B. web.config
- C. CyberArk.WebApplication.log
- D. CyberArk.WebConsole.log

Answer: CD

Explanation:

When troubleshooting a slow response in the Privileged Vault Web Access (PVWA), the first log files to analyze are the CyberArk.WebApplication.log and CyberArk.WebConsole.log. These logs contain detailed information about the activities carried out by the PVWA and can help identify any problems that may occur. The log files are created by the PVWA and stored on the Web server in the location specified in the LogFolder parameter in the web.config file¹. By examining these logs, you can track business flows and troubleshoot failures without having to enable debug mode. References:
? CyberArk Docs - PVWA Logging¹

NEW QUESTION 187

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 190

DRAG DROP

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- ? Shut down the PrivateArk Server Service on the DR Vault.
- ? In the PADR.ini file, set Failover Mode = No and remove the last two lines.
- ? Start the PrivateArk Disaster Recovery Service.

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

- ? Shut down the PrivateArk Server Service on the DR Vault to stop the Vault from being active.
- ? Modify the PADR.ini file by setting Failover Mode to No and removing the last two lines that were added during the failover process. This reconfigures the DR Vault to standby mode.
- ? Start the PrivateArk Disaster Recovery Service to complete the transition back to standby mode1.

References:

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

NEW QUESTION 191

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

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

Answer: AC

Explanation:

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

- ? CyberArk Docs: Monitor system health1
- ? CyberArk Docs: System Health Dashboard details

NEW QUESTION 192

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

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

Answer: D

Explanation:

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

References:

- ? CyberArk Docs - Web applications for PSM2
- ? CyberArk Docs - Configure PSM to connect to Web applications1

NEW QUESTION 193

What is the chief benefit of PSM?

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

Answer: D

Explanation:

According to the web search results, the chief benefit of PSM is to provide both privileged session isolation and privileged session recording. Privileged session isolation means that the PSM server acts as a proxy between the user and the target machine, preventing the user from directly accessing the target machine or

exposing the privileged account credentials. Privileged session recording means that the PSM server captures and stores a video and a transcript of the user's activity on the target machine, enabling auditing and monitoring of the privileged session. These benefits help to enhance the security and compliance of the privileged access management solution, as they prevent credential exposure, restrict unauthorized access, detect malicious activity, and provide evidence for forensic analysis

NEW QUESTION 195

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

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

Answer: B

Explanation:

The Immediate Interval setting in a CPM policy is used to control how often the CPM looks for User Initiated CPM work, such as manual password changes, retrievals, or requests. The Immediate Interval setting defines the frequency, in minutes, that the CPM will check the accounts that are associated with the policy and perform the actions that were initiated by the users. For example, if the Immediate Interval is set to 2, the CPM will check the accounts every 2 minutes and change, retrieve, or authorize the passwords according to the user requests. The Immediate Interval setting does not affect System Initiated CPM work, such as password changes, verifications, or reconciliations that are triggered by the policy settings, such as Expiration Period or One Time Password. These actions are controlled by the Interval setting in the CPM policy. The Immediate Interval setting also does not control how often the CPM rests between password changes or the maximum amount of time the CPM will wait for a password change to complete. These parameters are configured in the CPM.ini file, which is stored in the root folder of the <CPM username> Safe. References:

? [Defender PAM eLearning Course], Module 5: Password Management, Lesson 5.1: CPM Policies, Slide 9: CPM Policy Settings

? [Defender PAM Sample Items Study Guide], Question 6: CPM Policy Settings

? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 5: Managing Passwords, Section: CPM Policy Settings, Subsection: Immediate Interval

NEW QUESTION 198

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 203

In the screenshot displayed, you just configured the usage in CyberArk and want to update its password. What is the least intrusive way to accomplish this?

Required Properties:

Address:	webserver1.lab.local
File Path:	C:\inetpub\wwwroot\web.config
XML Element:	/configuration/appSettings/add[@key="PASSWORD"]
Connection Type:	Windows File Sharing

Optional Properties:

<input type="checkbox"/> Port:	
<input checked="" type="checkbox"/> XML Attribute:	value
<input checked="" type="checkbox"/> Password Regex:	(.*)
<input type="checkbox"/> Backup Password File:	[Select]
<input type="checkbox"/> Usage Display Name:	

☐ Disable automatic management for this account

Reason: No Reason

Save Cancel

- A. Use the "change" button on the usage's details page.
- B. Use the "change" button on the parent account's details page.
- C. Use the "sync" button on the usage's details page.

D. Use the “reconcile” button on the parent account’s details page.

Answer: C

Explanation:

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. To update the password of a usage, the least intrusive way is to use the “sync” button on the usage’s details page. This will synchronize the password value between the Vault and the file, without changing the actual password. The “change” button will initiate a password change process by the CPM, which will generate a new random password for the usage and the file. The “reconcile” button will initiate a password reconcile process by the CPM, which will use a reconcile account to reset the password of the usage and the file to the value stored in the Vault. References: Usages, Manage passwords for usages

NEW QUESTION 205

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 208

CyberArk recommends implementing object level access control on all Safes.

- A. True
- B. False

Answer: B

Explanation:

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

NEW QUESTION 211

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 212

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 217

The Password upload utility can be used to create safes.

- A. TRUE
- B. FALSE

Answer: A

Explanation:

The Password Upload utility can be used to create safes, as well as password objects, folders, and platforms. The Password Upload utility works with the CyberArk Password Vault to create password objects from a passwords list and store them in the Vault. This enables you to upload large numbers of passwords automatically and makes the Vault implementation process quicker and more automatic. The Password Upload utility initiates the Vault environment required to store passwords in the safe and start working with them. This includes creating new safes, adding the CPM user as a safe owner, and sharing the safe with the Password Vault Web Access¹. References:

? 1: Password Upload Utility

NEW QUESTION 221

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 226

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 229

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

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

Answer: C

Explanation:

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

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

RestAPI Functions

? [Onboarding RestAPI Functions Guide], Introduction

NEW QUESTION 230

Time of day or day of week restrictions on when password verifications can occur configured in .

- A. The Master Policy
- B. The Platform settings
- C. The Safe settings

D. The Account Details

Answer: C

Explanation:

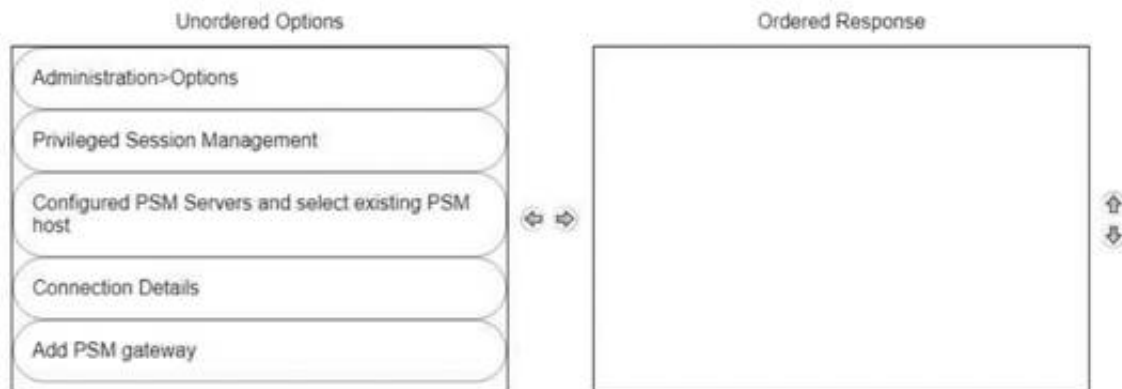
Time of day or day of week restrictions on when password verifications can occur are configured in the Safe settings. This is a security feature that prevents Safes from being opened except at certain times (e.g., 8 a.m. to 5 p.m.). If a user tries to enter at a time that has not been designated for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

NEW QUESTION 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.



- 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 233

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 236

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 237

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 240

Which processes reduce the risk of credential theft? (Choose two.)

- A. require dual control password access approval
- B. require password change every X days
- C. enforce check-in/check-out exclusive access
- D. enforce one-time password access

Answer: BD

NEW QUESTION 241

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

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

Answer: C

Explanation:

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

NEW QUESTION 242

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 244

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 249

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 250

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

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

Answer: BD

Explanation:

When configuring a discovery scan for UNIX, you must specify theCPM Scanner and thelist of machines to scan. The CPM Scanner is the component responsible for executing the discovery process, and it requires a list of target machines to scan for new and modified accounts and their dependencies. This list can be provided in the form of a CSV file for UNIX machines1. The discovery process will then scan the predefined machines to identify privileged accounts that should be onboarded into the Vault for secure and automated management according to enterprise compliance policies2. References:
? CyberArk Docs - Manage discovery processes1
? CyberArk Docs - Scan for accounts using Account Discovery

NEW QUESTION 254

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual PAM-DEF Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the PAM-DEF Product From:

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

Money Back Guarantee

PAM-DEF Practice Exam Features:

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