

CyberArk.PAM-DEF.v2024-12-16.q135

Exam Code:	PAM-DEF
Exam Name:	CyberArk Defender - PAM
Certification Provider:	CyberArk
Free Question Number:	135
Version:	v2024-12-16
# of views:	806
# of Questions views:	1350
https://www.freeqas.com/qa/CyberArk/PAM-DEF/CyberArk.PAM-DEF.v2024-12-16.q135.html	

NEW QUESTION: 1

In a rule using "Privileged Session Analysis and Response" in PTA, which session options are available to configure as responses to activities?

- A. Suspend, Terminate, None
- B. Suspend, Terminate, Lock Account
- C. Pause, Terminate, None
- D. Suspend, Terminate

Answer: ([SHOW ANSWER](#))

Explanation

<https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security-Configuration.htm?To> These are the session response options that can be configured in a rule using Privileged Session Analysis and Response in PTA. These options determine how PTA reacts to suspicious activities detected in a privileged session. Suspend means that the session is paused and the user is notified. Terminate means that the session is ended and the user is disconnected. None means that no action is taken on the session, but the event is still recorded and reported. You can find more information about these options and how to configure them in the reference below.

NEW QUESTION: 2

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 must be uploaded using third party tools.
- C. They cannot be onboarded to the Password Vault.
- D. They are not part of the Discovery Process.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 3

Match the built-in Vault User with the correct definition.

This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.	Drag answer here	Administrator
This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements.	Drag answer here	Batch
This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history.	Drag answer here	CYBERARK The Identity Security Company
This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe.	Drag answer here	Auditor

Answer:

This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.	This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.	Administrator
This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements.	This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history.	Batch
This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history.	This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe.	Master
This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe.	This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements.	Auditor

This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.

Administrator

This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history.

Batch

This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary, and cannot be removed from any Safe.

Master

This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements.

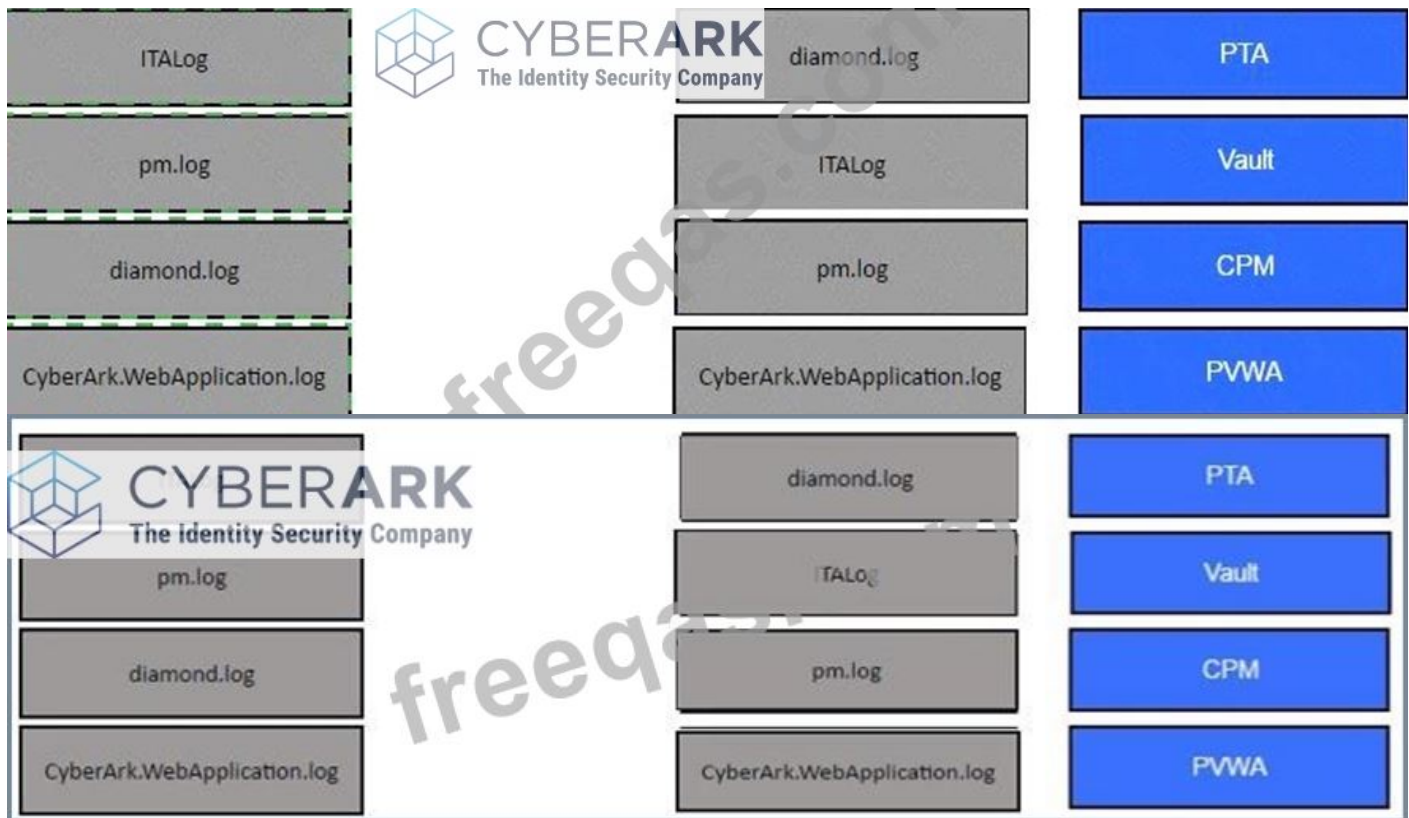
Auditor

NEW QUESTION: 4

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

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

Answer:



NEW QUESTION: 5

Select the best practice for storing the Master CD.

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 6

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 ([LEAVE A REPLY](#))

NEW QUESTION: 7

In accordance with best practice, SSH access is denied for root accounts on UNIX/LINUX system .

What is the BEST way to allow CPM to manage root accounts?

- A.** Create a non-privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account as the Logon account of the target server's root account.
- B.** Create a privileged account on the target server. Allow this account the ability to SSH directly from the CPM machine. Configure this account as the Reconcile account of the target server's root account.
- C.** Configure the CPM to allow SSH logins.
- D.** Configure the Unix system to allow SSH logins.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 8

An auditor initiates a live monitoring session to PSM server to view an ongoing live session. When the auditor's machine makes an RDP connection the PSM server, which user will be used?

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 9

Your organization has a requirement to allow users to "check out passwords" and connect to targets with the same account through the PSM.

What needs to be configured in the Master policy to ensure this will happen?

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

Answer: ([SHOW ANSWER](#)**)**

Explanation

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

References:

- * CyberArk's official documentation on Account check-out and check-in1.
- * The Master Policy overview provided by CyberArk2.

NEW QUESTION: 10

If a user is a member of more than one group that has authorizations on a safe, by default that user is granted_____.

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

Answer: D ([LEAVE A REPLY](#))

Explanation

When a user is a member of more than one group that has authorizations on a safe, by default that user is granted the cumulative permissions of all groups to which that user belongs. This means that the user will have the highest level of access that any of the groups have on the safe. For example, if one group has View and Retrieve permissions, and another group has Add and Delete permissions, the user will have View, Retrieve, Add, and Delete permissions on the safe. This is the default behavior of the vault, unless the Exclusive option is enabled on the safe. The Exclusive option restricts the user's permissions to only those of the group added to the safe first.

References:

- * [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.2: Safe Permissions, Slide 8: Cumulative Permissions
- * [Defender PAM Sample Items Study Guide], Question 1: Safe Permissions
- * [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section: Safe Properties, Subsection: Exclusive

NEW QUESTION: 11

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: ([SHOW ANSWER](#)**)**

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: 12

A new colleague created a directory mapping between the Active Directory groups and the Vault. Where can the newly Configured directory mapping be tested?

- A.** Connect to Sailpoint (or similar tool) to ensure the organizational unit is correctly named; log in to the PVWA with "Administrator" and confirm authentication succeeds.
- B.** Connect to the Active Directory and ensure the organizational unit exists.
- C.** Connect to the PrivateArk Client with the Administrator Account to see if there is a user in the Vault Admin Group.
- D.** Search for members that exist only in the mapping group to grant them safe permissions through the PVWA.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 13

You are creating a shared safe for the help desk.

What must be considered regarding the naming convention?

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

Answer: C ([LEAVE A REPLY](#))

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 ([LEAVE A REPLY](#))

Explanation

Being in Vault admins group only give you access to safes which are created during installation (safe created in installation process) -This is clearly mentioned in documents .

NEW QUESTION: 15

Which Master Policy Setting must be active in order to have an account checked-out by one user for a pre-determined amount of time?

- A.** Require dual control password access Approval
- B.** Enforce check-in/check-out exclusive access
- C.** Enforce one-time password access
- D.** Enforce check-in/check-out exclusive access & enforce one-time password access

Answer: (SHOW ANSWER)

Explanation

According to the CyberArk Defender PAM documentation, the Master Policy setting that must be active in order to have an account checked-out by one user for a pre-determined amount of time is Enforce check-in/check-out exclusive access. This setting enables organizations to permit users to check out a

'one-time' password and lock it so that no other users can retrieve it at the same time. After the user has used the password, the user checks the password back into the Vault. This ensures exclusive usage of the privileged account, enabling full control and tracking for the password. The duration of the check-out period can be configured in the platform settings for each account.

References:

- * Account check-out and check-in - CyberArk
- * Master Policy - CyberArk

NEW QUESTION: 16

A Vault administrator have associated a logon account to one of their Unix root accounts in the vault.

When attempting to verify the root account's password the Central Policy Manager (CPM) will:

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

Answer: (SHOW ANSWER)

Valid PAM-DEF Dumps shared by PrepPdf.com for Helping Passing PAM-DEF Exam!

PrepPdf.com now offer the **newest PAM-DEF exam dumps**, the PrepPdf.com PAM-DEF exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PAM-DEF dumps with Test Engine here:

<https://www.preppdf.com/CyberArk/PAM-DEF-prepaway-exam-dumps.html> (240 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 17

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

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

E. Audit Users

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 18

According to the DEFAULT Web Options settings, which group grants access to the REPORTS page?

A. PVWAMonitor

B. Auditors

C. PVWAUsers

D. Vault Admins

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 19

When managing SSH keys, the CPM stores the Public Key

A. On the target server

B. In the Vault

C. A & B

D. Nowhere because the public key can always be generated from the private key.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 20

You are creating a Dual Control workflow for a team's safe.

Which safe permissions must you grant to the Approvers group?

A. List accounts, Authorize account request

B. Retrieve accounts, Access Safe without confirmation

C. Retrieve accounts, Authorize account request

D. List accounts, Unlock accounts

Answer: C ([LEAVE A REPLY](#))

Explanation

When setting up a Dual Control workflow for a team's safe in CyberArk's Privileged Access Management (PAM), the Approvers group must be granted specific permissions to function effectively within the workflow.

The permissions required for the Approvers group are to 'Retrieve accounts' and 'Authorize account request'.

This allows the Approvers to retrieve the necessary account details and also to authorize requests for access as part of the dual control mechanism. These permissions ensure that the workflow operates smoothly and securely, with the Approvers having the ability to review and approve access requests as needed.

References: The answer is derived from the best practices and guidelines provided in the CyberArk Defender PAM course and learning resources, which include the official CyberArk

documentation and study guides. Specifically, the CyberArk documentation outlines the importance of the 'Retrieve accounts' and 'Authorize account request' permissions for Approvers in a Dual Control workflow

NEW QUESTION: 21

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: ([SHOW ANSWER](#))

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: 22

The vault supports Role Based Access Control.

- A. TRUE
- B. FALSE

Answer: A ([LEAVE A REPLY](#))

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: 23

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 24

Which item is an option for PSM recording customization?

- A. Windows events text recorder with automatic play-back
- B. Windows events text recorder and universal keystrokes recording simultaneously
- C. Universal keystrokes text recorder with windows events text recorder disabled
- D. Custom audio recording for windows events

Answer: C ([LEAVE A REPLY](#))

Explanation

For PSM recording customization, one of the options is to use the Universal keystrokes text recorder with the Windows events text recorder disabled. This configuration allows for the recording of all keystrokes that are typed during privileged sessions on all supported connections. However, it is important to note that Universal keystroke recording and Windows events recordings cannot be configured for the same PSM-RDP connection. By default, Windows events text recording is enabled for PSM-RDP connections, so to enable universal keystrokes text recording, the Windows events text recording must first be disabled¹.

References:

* CyberArk's official documentation on configuring recordings and audits in PSM, which includes details on how to customize text recorders and the limitations of configuring multiple recorders for the same connection¹

NEW QUESTION: 25

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 26

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. Update Account Properties
- C. Rename Accounts
- D. Manage Safe

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 27

Which of the following options is not set in the Master Policy?

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 28

Which statement is true about setting the reconcile account at the platform level?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 29

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

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

Answer: ([SHOW ANSWER](#))

Explanation

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

References:

- * CyberArk Docs - Export Vault Data (EVD) utility¹
- * CyberArk Docs - Export data to files

NEW QUESTION: 30

What is the purpose of the PrivateArk Server service?

- A. Maintains Vault metadata
- B. Sends email alerts from the Vault
- C. Executes password changes
- D. Makes Vault data accessible to components

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 31

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

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

Answer: C ([LEAVE A REPLY](#))

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"

Valid PAM-DEF Dumps shared by PrepPdf.com for Helping Passing PAM-DEF Exam!
PrepPdf.com now offer the **newest PAM-DEF exam dumps**, the PrepPdf.com PAM-DEF exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PAM-DEF dumps with Test Engine here:

NEW QUESTION: 32

Which of the Following can be configured in the Master Policy? Choose all that apply.

- A. Dual Control
- B. One Time Passwords
- C. Exclusive Passwords
- D. Password Reconciliation
- E. Ticketing Integration
- F. Required Properties
- G. Custom Connection Components
- H. Password Aging Rules

Answer: (SHOW ANSWER)

Explanation

The Master Policy is a centralized overview of the security and compliance policy of privileged accounts in the organization. It allows the administrator to configure compliance driven rules that are defined as the baseline for the enterprise. The Master Policy includes the following main concepts1:

- * Basic policy rules: These rules allow the administrator to define specific aspects of privileged account management, such as privileged access workflows, password management, session monitoring and auditing.
- * Advanced policy rules: Some basic policy rules have related advanced settings that provide more granular control over the policy enforcement.
- * Exceptions: These are policy rules that differ from the overall Master Policy for a specific scope of accounts, such as accounts associated with a specific platform.

The Master Policy rules are divided into four sections2:

- * Privileged Access Workflows: These rules define how the organization manages access to privileged accounts, such as requiring dual control, one-time passwords, exclusive passwords, transparent connections, reason for access, etc.
- * Password Management: These rules determine how passwords are managed, such as requiring password change, password verification, password reconciliation, ticketing integration, required properties, custom connection components, etc.
- * Session Management: These rules determine whether or not privileged sessions are recorded and how they are monitored, such as requiring session isolation, session recording, session audit, etc.
- * Audit: This rule determines how Safe audits are retained, such as specifying the audit retention period.

Based on the above information, the following options can be configured in the Master Policy:

- * A. Dual Control: This is a basic policy rule in the Privileged Access Workflows section that determines whether users need to get approval from authorized users before accessing a privileged account².
- * B. One Time Passwords: This is a basic policy rule in the Privileged Access Workflows section that determines whether users can only use a password once before it is changed².
- * C. Exclusive Passwords: This is a basic policy rule in the Privileged Access Workflows section that determines whether users need to check out a password and prevent other users from accessing it until it is checked in².
- * H. Password Aging Rules: This is a basic policy rule in the Password Management section that determines how often passwords need to be changed².

The following options cannot be configured in the Master Policy:

- * D. Password Reconciliation: This is not a policy rule, but a process that restores the password of a privileged account to the value that is stored in the Vault, in case it is changed or out of sync³.
- * E. Ticketing Integration: This is not a policy rule, but a feature that enables the integration of the Vault with external ticketing systems, such as ServiceNow, Jira, etc.
- * F. Required Properties: This is not a policy rule, but a platform setting that determines which properties are mandatory for adding accounts to a platform.
- * G. Custom Connection Components: This is not a policy rule, but a platform setting that determines which connection components are used to connect to target systems, such as PVWA, PSM, PSMP, etc.

References:

- * 1: The Master Policy
- * 2: Master Policy Rules
- * 3: Password Reconciliation
- * : Ticketing Integration
- * : Required Properties
- * : Custom Connection Components

NEW QUESTION: 33

When should vault keys be rotated?

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 34

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

- A. LDAP Admin

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 35

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 ([LEAVE A REPLY](#))

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: 36

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

- A. FALSE
- B. TRUE

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 37

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

- A. True
- B. False

Answer: ([SHOW ANSWER](#)**)**

Explanation

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

NEW QUESTION: 38

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: ([SHOW ANSWER](#))

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: 39

How much disk space do you need on the server for a PAReplicate?

- A.** 500 GB
- B.** 1 TB
- C.** same as disk size on Satellite Vault
- D.** same as disk size on Primary Vault

Answer: ([SHOW ANSWER](#))

Explanation

The PAReplicate utility exports the Safe files from the CyberArk Vault to a computer on the local network where the Backup utility has been installed. The Safes are copied in a similar format and structure to the one in the Server. Therefore, the disk space required on the server for a PAReplicate is the same as the disk size on the Primary Vault¹. References: Use the CyberArk Backup Process

NEW QUESTION: 40

You need to enable the PSM for all platforms.

Where do you perform this task?

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 41

Select the best practice for storing the Master CD.

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

Answer: C ([LEAVE A REPLY](#))

Explanation

The best practice for storing the Master CD is to store it in a secure location, such as a physical safe. The Master CD contains the server key, the public recovery key, and the private recovery key, which are essential for starting, operating, and recovering the Vault. These keys are sensitive and should be protected from unauthorized access, loss, or damage. Therefore, storing the CD in a physical safe ensures that the keys are kept in a secure location when not in use, and that they are available when needed. This is the recommended option by CyberArk¹.

The other options are not best practices and should be avoided, as they expose the keys to potential risks, such as theft, corruption, or deletion. Copying the files to the Vault server and discarding the CD is not secure, as it makes the keys accessible to anyone who can access the Vault server or compromise its security. Copying the contents of the CD to a Hardware Security Module (HSM) and discarding the CD is not feasible, as the HSM can only store the server key, not the recovery keys². Storing the CD in a secure location, such as a physical safe, and copying the contents of the CD to a folder secured with NTFS permissions on the Vault is not necessary, as it creates redundant copies of the keys that may not be synchronized or updated. Moreover, NTFS permissions are not sufficient to protect the keys from malicious or accidental actions.

References:

* Server Keys - CyberArk, section "Server Keys"

* Store the Server Key in an HSM - CyberArk, section "Store the Server Key in an HSM"

NEW QUESTION: 42

Which report provides a list of account stored in the vault.

- A. Privileged Accounts Inventory
- B. Privileged Accounts Compliance Status
- C. Entitlement Report
- D. Active Log

Answer: (SHOW ANSWER)

Explanation

The report that provides a list of accounts stored in the vault is the Privileged Accounts Inventory report. This report can be generated in the Reports page in the PVWA by users who belong to the group that is specified in the ManageReportsGroup parameter in the Reports section of the Web Access Options in the System Configuration page¹. The Privileged Accounts Inventory report contains information such as the safe, folder, name, platform ID, username, address, group, last accessed date, last accessed by, last modified date, last modified by, verification date, checkout date, checked out by, age, change failure, verification failure, master pass folder, master pass name, disabled by, and disabled reason of each account stored in the vault².

References:

- * 1: Reports in PVWA
- * 2: Users List Report

NEW QUESTION: 43

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

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

Answer:

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

Explanation

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

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

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

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

References: PSM Health Check, PSM Health Check - CyberArk

NEW QUESTION: 44

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?

- Set the parameter IgnoreReconcileOnMissingAccount to No.
- Set the UnlockUserOnReconcile to Yes.
- Set the parameter ChangePasswordinResetMade to Yes.
- Set the parameter RCAAllowManualReconciliation to Yes.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 45

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

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 46

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

The screenshot shows the CyberArk interface with a list of steps to restore a Vault using PARestore for a Backup. The steps are listed in an 'Unordered' column and an 'Ordered Response' column.

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

Answer:

The screenshot shows the CyberArk interface with a list of steps to restore a Vault using PARestore for a Backup. The steps are listed in an 'Unordered Options' column and an 'Ordered Response' column.

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

The 'Ordered Response' column shows the steps in the correct sequence: CAVaultManager RecoverBackupFiles, CAVaultManager RestoreDB, BackupFilesDeletion=Yes,24,1,5,7d, PARestore vault.ini operator /FullVaultRestore, and BackupFilesDeletion=No.

Valid PAM-DEF Dumps shared by PrepPdf.com for Helping Passing PAM-DEF Exam!
PrepPdf.com now offer the **newest PAM-DEF exam dumps**, the PrepPdf.com PAM-DEF exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PAM-DEF dumps with Test Engine here:
<https://www.preppdf.com/CyberArk/PAM-DEF-prepaway-exam-dumps.html> (240 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 47

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

- A. TRUE
- B. FALSE

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 48

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

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 49

You have been given the requirement that certain accounts cannot have their passwords updated during business hours.

How can you set up a configuration to meet this requirement?

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 50

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 ([LEAVE A REPLY](#))

NEW QUESTION: 51

Which item is an option for PSM recording customization?

- A. Universal keystrokes text recorder with windows events text recorder disabled
- B. Windows events text recorder and universal keystrokes recording simultaneously
- C. Windows events text recorder with automatic play-back
- D. Custom audio recording for windows events

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 52

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: ([SHOW ANSWER](#)**)**

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: 53

What is the primary purpose of Dual Control?

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 54

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

- A. FALS
- B. TRUE

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 55

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

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 56

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: A,B,C ([LEAVE A REPLY](#))

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: 57

Which Master Policy Setting must be active in order to have an account checked-out by one user for a pre-determined amount of time?

- A. Enforce check-in/check-out exclusive access & Enforce one-time password access
- B. Enforce check-in/check-out exclusive access
- C. Enforce one-time password access
- D. Require dual control password access Approval

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 58

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: ([SHOW ANSWER](#)**)**

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: 59

DRAG DROP

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

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

Answer:

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

NEW QUESTION: 60

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

- A. diamond.log
- B. WebApplication.log
- C. ITAlog.log
- D. pm_error.log

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 61

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

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

Answer: ([SHOW ANSWER](#))

Explanation

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

* A comma delimited upload file: This is a text file that contains the passwords and their properties that will be uploaded to the Vault. The file must have a .csv extension and follow a specific format. The first line in the file defines the names of the password properties as specified in the Password Vault. Every other line represents a single password object and its property values, according to the properties specified in the first line¹.

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

* conf.ini: This is a configuration file that stores the parameters for the Password Upload Utility. The conf.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: InputFile, LogFile, and ErrorFile³.

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

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

* 1: Create the Password File

* 2: PACli.ini

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

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

Valid PAM-DEF Dumps shared by PrepPdf.com for Helping Passing PAM-DEF Exam! PrepPdf.com now offer the **newest PAM-DEF exam dumps**, the PrepPdf.com PAM-DEF exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PAM-DEF dumps with Test Engine here:

NEW QUESTION: 62

You have been asked to delegate the rights to unlock users to Tier 1 support. The Tier 1 support team already has an LDAP group for its members.

Arrange the steps to do this in the correct sequence.

Unordered Options

Ordered Response

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

Open LDAP Integration view.

Add Mapping to the existing LDAP integration.

Name the new mapping and set the mapping order.

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

Answer:

Unordered Options

Ordered Response

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

Open LDAP Integration view.

Add Mapping to the existing LDAP integration.

Name the new mapping and set the mapping order.

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

Explanation

The correct sequence to delegate the rights to unlock users to Tier 1 support with an existing LDAP group is as follows:

- * Sign into the PWA (V10) as a local user with the "Manage Directory Mapping" privilege.
- * Open LDAP Integration view.
- * Add Mapping to the existing LDAP integration.
- * Name the new mapping and set the mapping order.
- * Select required LDAP group and assign authorization "Activate Users".

Comprehensive Explanation: To delegate the rights to unlock users, you must first access the Privileged Web Access (PWA) with the appropriate privileges to manage directory mappings.

Then, navigate to the LDAP Integration view to add a new mapping to the existing LDAP integration. This mapping should be named and ordered correctly. Finally, select the LDAP group that represents Tier 1 support and assign the specific authorization needed to unlock users, which is "Activate Users" in this context¹².

References:

* CyberArk Docs: LDAP Integration in V102

* CyberArk Knowledge Article: How to delegate permissions to unlock Active Directory accounts¹

NEW QUESTION: 63

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 64

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: ([SHOW ANSWER](#))

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: 65

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

- A. PSMConnect

- B. PSMMaster
- C. PSMGwUser
- D. PSMAAdminConnect

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 66

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: ([SHOW ANSWER](#))

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 the Platform Management section of the PrivateArk 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: 67

What is the chief benefit of PSM?

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

D. Privileged session recording

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 68

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

A. False. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect.

B. False. Because if credentials are not stored in the vault, the PSM will prompt for credentials.

C. True.

D. False. Because the user can also enter credentials manually using Secure Connect.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 69

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

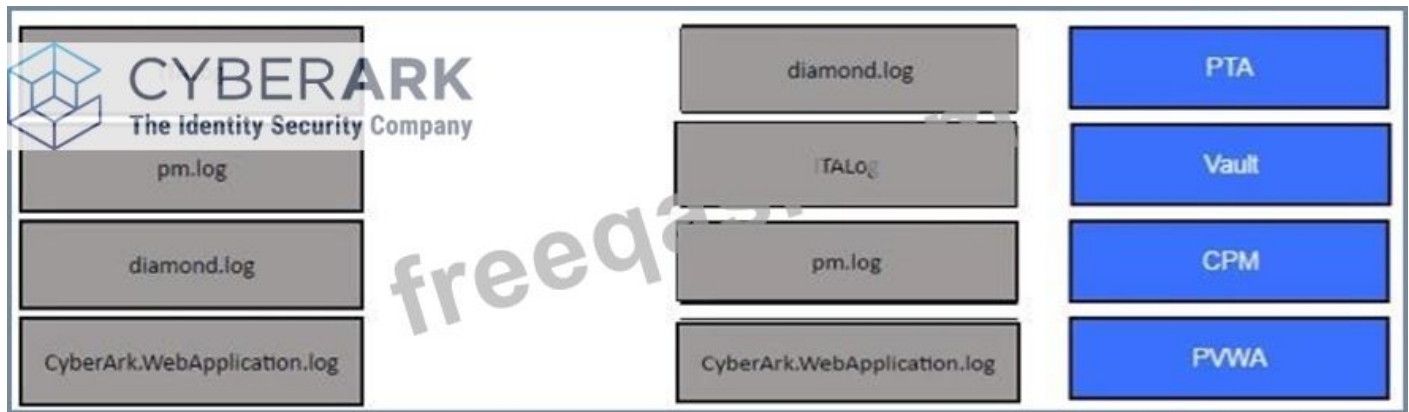
ITALog		PTA
pm.log		Vault
diamond.log		CPM
CyberArk.WebApplication.log		PVWA



Answer:

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





NEW QUESTION: 70

Which of these accounts onboarding methods is considered proactive?

- A. Accounts Discovery
- B. Detecting accounts with PTA
- C. A Rest API integration with account provisioning software
- D. A DNA scan

Answer: C ([LEAVE A REPLY](#))

Explanation

A Rest API integration with account provisioning software is considered a proactive account onboarding method, because it enables the automatic creation and management of accounts in the Vault as soon as they are provisioned in the target systems. This way, the accounts are secured from the start and do not need to be discovered or onboarded manually later. A Rest API integration with account provisioning software can be achieved by using the CyberArk Accounts Feed REST API, which allows external applications to send account information to the Vault¹. The other options are not proactive account onboarding methods, because they rely on the discovery of existing accounts that may have been exposed or compromised before being onboarded to the Vault. Accounts Discovery is a feature that enables the Vault to scan target systems and identify privileged accounts that are not managed by the Vault². Detecting accounts with PTA is a feature that enables the Privileged Threat Analytics (PTA) component to detect and alert on suspicious account activities and credential thefts³. A DNA scan is a feature that enables the Discovery and Audit (DNA) tool to scan Windows and Unix machines and generate a report on the privileged accounts and vulnerabilities found⁴.

References:

- * CyberArk Accounts Feed REST API - CyberArk, section "CyberArk Accounts Feed REST API"
- * Accounts Discovery - CyberArk, section "Accounts Discovery"
- * Detect and Respond to Privileged Account Threats - CyberArk, section "Detect and Respond to Privileged Account Threats"
- * CyberArk DNA - CyberArk, section "CyberArk DNA"

NEW QUESTION: 71

Which utilities could you use to change debugging levels on the vault without having to restart the vault.

Select all that apply.

- A. PAR Agent
- B. PrivateArk Server Central Administration
- C. Edit DBParm.ini in a text editor.
- D. Setup.exe

Answer: A,B (LEAVE A REPLY)

Explanation

To change debugging levels on the vault without having to restart the vault, you can use the following utilities:

* PAR Agent: This is a utility that runs on the vault server and allows you to change the debug level of the vault by editing the PARAgent.ini file. You can set the EnableTrace parameter to yes and specify the debug level in the DebugLevel parameter. The changes will take effect immediately without restarting the vault. The log file is located in the PARAgent.log file¹.

* PrivateArk Server Central Administration: This is a graphical user interface that runs on the vault server and allows you to change the debug level of the vault by selecting the vault server and clicking the Debug button. You can choose the debug level from a list of predefined options or enter a custom value. The changes will take effect immediately without restarting the vault. The log files are located in the Trace.dX files, where X is a number from 0 to 42.

You cannot use the following utilities to change debugging levels on the vault without having to restart the vault:

* Edit DBParm.ini in a text editor: This is a configuration file that stores the vault parameters, such as the database name, port, and password. Editing this file does not affect the debug level of the vault, and requires restarting the vault for the changes to take effect³.

* Setup.exe: This is an installation program that runs on the vault server and allows you to install, upgrade, or uninstall the vault. It does not allow you to change the debug level of the vault, and requires restarting the vault for any changes to take effect⁴. References:

* 1: Configure Debug Levels, Vault section, PARAgent subsection

* 2: Configure Debug Levels, Vault section, PrivateArk Server Central Administration subsection

* 3: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault, Section:

Configuring the Vault, Subsection: DBParm.ini

* 4: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault, Section:

Installing the Vault

NEW QUESTION: 72

By default, members of which built-in groups will be able to view and configure Automatic Remediation and Session Analysis and Response in the PVWA?

- A. Auditors

- B. Security Operators
- C. Vault Admins
- D. Security Admins

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 73

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 74

dbparm.ini is the main configuration file for the Vault.

- A. True
- B. False

Answer: ([SHOW ANSWER](#)**)**

Explanation

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

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

NEW QUESTION: 75

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

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

Ordered Response



Answer:

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

Ordered Response

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

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-Vau>

NEW QUESTION: 76

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

A. TRUE

B. FALSE

Answer: A (LEAVE A REPLY)

Explanation

Password verification can be restricted to specific days. This means that the CPM will only verify passwords on the days of the week specified in the VFExecutionDays parameter. The days of the week are represented by the first 3 letters of the name of the day. Sunday is represented by Sun, Monday by Mon, etc.

Valid PAM-DEF Dumps shared by PrepPdf.com for Helping Passing PAM-DEF Exam! PrepPdf.com now offer the **newest PAM-DEF exam dumps**, the PrepPdf.com PAM-DEF exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PAM-DEF dumps with Test Engine here:
<https://www.preppdf.com/CyberArk/PAM-DEF-prepaway-exam-dumps.html> (240 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 77

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

Answer: A,B,D ([LEAVE A REPLY](#))

NEW QUESTION: 78

Which master policy settings ensure non-repudiation?

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

Answer: C ([LEAVE A REPLY](#))

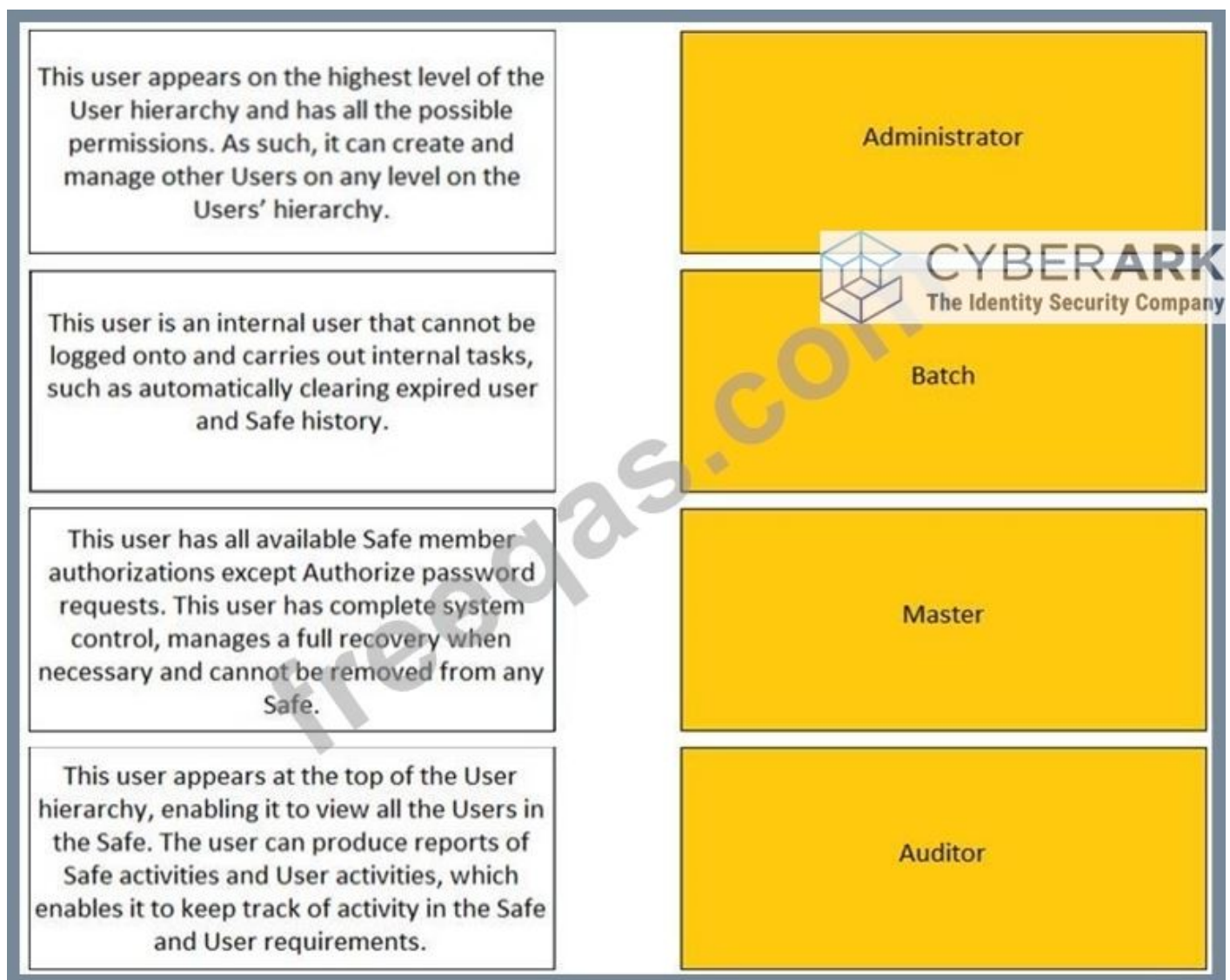
NEW QUESTION: 79

Match the built-in Vault User with the correct definition.

This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.	Drag answer here	Administrator
This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements.	Drag answer here	Batch
This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history.	Drag answer here	Master
This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe.	Drag answer here	Auditor

Answer:

This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.	This user appears on the highest level of the User hierarchy and has all the possible permissions. As such, it can create and manage other Users on any level on the Users' hierarchy.	Administrator
This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements.	This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history.	Batch
This user is an internal user that cannot be logged onto and carries out internal tasks, such as automatically clearing expired user and Safe history.	This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe.	Master
This user has all available Safe member authorizations except Authorize password requests. This user has complete system control, manages a full recovery when necessary and cannot be removed from any Safe.	This user appears at the top of the User hierarchy, enabling it to view all the Users in the Safe. The user can produce reports of Safe activities and User activities, which enables it to keep track of activity in the Safe and User requirements.	Auditor



NEW QUESTION: 80

The Password upload utility can be used to create safes.

A. TRUE

B. FALS

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 81

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

A. True; this is the default behavior

B. True, if the AllowFailback setting is set to "yes" in the padr.ini file

C. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the dbparm.ini file

D. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the padr.ini file

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 82

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

A. TRUE

B. FALSE

Answer: B ([LEAVE A REPLY](#))

Explanation

Customers who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, do not need to request approval to use the account. The 'Access Safe without confirmation' safe permission allows users to access accounts without confirmation from authorized users, even if the Master Policy or an exception enforces Dual Control¹. This means that users who have this permission can bypass the workflow process and access the account password or connect to the target system immediately. This permission can be granted to users or groups on a safe level by the safe owner or another user with the Manage Safe authorization². References:

* 1: Dual Control, Advanced Settings subsection

* 2: CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section:

Safe Authorizations, Table 2-1: Safe Authorizations

NEW QUESTION: 83

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: ([SHOW ANSWER](#)**)**

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: 84

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

A. TRUE

B. FALSE

Answer: ([SHOW ANSWER](#))

Explanation

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

References:

* 1: Vault Member Authorizations

NEW QUESTION: 85

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 ([LEAVE A REPLY](#))

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: 86

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: ([SHOW ANSWER](#))

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: 87

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 both one-time passwords and exclusive access for the appropriate platform in Master Policy.

B. Configure shared account mode on the appropriate safe.

C. Configure object level access control on the appropriate safe.

D. Configure one-time passwords for the appropriate platform in Master Policy.

Answer: **C** ([LEAVE A REPLY](#))

NEW QUESTION: 88

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

A. in PVWA at the account level

B. in PVWA in the platform configuration

C. in the Master policy of the PVWA

D. at the Safe level

E. in the CPM settings

Answer: ([SHOW ANSWER](#))

Explanation

A Reconcile account can be assigned in the Privileged Vault Web Access (PVWA) at both the account level and within the platform configuration. At the account level, a Reconcile account password can be defined which will override the account specified in the platform¹. In the platform configuration, you can navigate to Platform Management, select the platform, edit it, and then expand Automatic Password Management to enter the values in the 'ReconcileAccountSafe'

and 'ReconcileAccountName' fields, which will apply to all accounts attached to that specific platform2.

References:

- * CyberArk Docs - Reconcile Password1
- * CyberArk Community - Associate reconcile account with a specific platform

NEW QUESTION: 89

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

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

Answer:

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

NEW QUESTION: 90

A user needs to view recorded sessions through the PVWA.

Without giving auditor access, which safes does a user need access to view PSM recordings?
(Choose two.)

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

Answer: ([SHOW ANSWER](#))

Explanation

To view recorded sessions through the PVWA without having auditor access, a user needs access to two specific safes: the Recordings safe and the safe the account is in. The Recordings safe is where the PSM session recordings are stored, and users need permission to access this safe to view the recordings. Additionally, users need access to the safe where the account associated with the recorded session is stored, as this is where the session details and permissions are managed¹².

References:

- * CyberArk Docs - Configure video and text recordings³
- * CyberArk Community - Viewing PSM recorded sessions¹

NEW QUESTION: 91

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 ([LEAVE A REPLY](#))

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

exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PAM-DEF dumps with Test Engine here:
<https://www.preppdf.com/CyberArk/PAM-DEF-prepaway-exam-dumps.html> (240 Q&As
Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 92

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

A. FALS

B. TRUE

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 93

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

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



Answer:

Retrieve accounts/files	Required	Required
	Required	Not Required
View audit	Required	
Access Safe without confirmation	Not Required	
Create Folders	Not Required	

Explanation

* Retrieve accounts/files: Required

- * List accounts/files: Required
- * View audit: Required
- * Access Safe without confirmation: Not Required
- * Create Folders: Not Required

Comprehensive Explanation: To allow a group to view recordings in a recording safe, the required authorizations are Retrieve accounts/files, List accounts/files, and View audit. These authorizations enable the group members to access and view the session recordings stored within the safe. The Retrieve accounts/files permission allows users to retrieve files during PSM sessions. The List accounts/files permission enables users to see the list of accounts and files within the safe. The View audit authorization is necessary for users to view the audit records associated with the recordings¹.

References:

- * CyberArk Docs - Monitor Privileged Sessions

NEW QUESTION: 94

To manage automated onboarding rules, a CyberArk user must be a member of which group?

- A. Auditors
- B. Administrators
- C. CPM User
- D. Vault Admins

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 95

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

- A. TRUE
- B. FALSE

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 96

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

Answer: B,E ([LEAVE A REPLY](#))

NEW QUESTION: 97

To enable the Automatic response "Add to Pending" within PTA when unmanaged credentials are found, what are the minimum permissions required by PTAUser for the PasswordManager_pending safe?

- A. View Accounts, Update Account content, Update Account properties, Access Safe without confirmation, Manage Safe, View Audit
- B. Add accounts (includes update properties), Update Account content, Update Account properties, View Audit
- C. List Accounts, Add accounts (includes update properties), Delete Accounts, Manage Safe
- D. List Accounts, View Safe members, Add accounts (includes update properties), Update Account content, Update Account properties

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 98

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 99

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: ([SHOW ANSWER](#))

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: 100

Your organization requires all passwords be rotated every 90 days.

Where can you set this regulatory requirement?

- A. Safe Templates
- B. Platform Configuration
- C. Master Policy

D. PVWAConfig.xml

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 101

You are creating a Dual Control workflow for a team's safe.

Which safe permissions must you grant to the Approvers group?

- A. Retrieve accounts, Authorize account request
- B. List accounts, Unlock accounts
- C. List accounts, Authorize account request
- D. Retrieve accounts, Access Safe without confirmation

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 102

When onboarding multiple accounts from the Pending Accounts list, which associated setting must be the same across the selected accounts?

- A. Vault
- B. Platform
- C. Connection Component
- D. CPM

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 103

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

- A. It determines how far in advance audit data is collected for reports
- B. It instructs the CPM to initiate the password change process X number of days before expiration.
- C. It instructs the AIM Provider to 'skip the cache' during the defined time period
- D. It alerts users of upcoming password changes x number of days before expiration.

Answer: B ([LEAVE A REPLY](#))

Explanation

The number of days before the password expires (according to the ExpirationPeriod parameter) that the CPM will initiate a password change process. This parameter is not relevant if the policy will be applied to a member of an account group.

NEW QUESTION: 104

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

Answer:

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

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

NEW QUESTION: 105

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: A,C (LEAVE A REPLY)

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: 106

To manage automated onboarding rules, a CyberArk user must be a member of which group?

A. Vault Admins

B. CPM User

C. Auditors

D. Administrators

Answer: A (LEAVE A REPLY)

Explanation

To manage automated onboarding rules in CyberArk, a user must be a member of the Vault Admins group. This group has the necessary permissions to create and manage predefined rules that automatically onboard newly discovered accounts, which helps minimize the time it takes to onboard and securely manage accounts, reduces the time spent on reviewing pending accounts, and prevents human errors that may occur during manual onboarding¹.

References:

* CyberArk's official documentation on onboarding rules provides detailed information on the groups required to manage these rules, including the Vault Admins group¹.

Valid PAM-DEF Dumps shared by PrepPdf.com for Helping Passing PAM-DEF Exam! PrepPdf.com now offer the **newest PAM-DEF exam dumps**, the PrepPdf.com PAM-DEF exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PAM-DEF dumps with Test Engine here:

<https://www.preppdf.com/CyberArk/PAM-DEF-prepaway-exam-dumps.html> (240 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 107

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

A. in the CPM settings

B. in PVWA at the account level

C. in PVWA in the platform configuration

D. at the Safe level

E. in the Master policy of the PVWA

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 108

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

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

B. PSM for Windows (previously known as RDP Proxy)

C. PSM for SSH (previously known as PSM SSH Proxy)

D. All of the above

Answer: D ([LEAVE A REPLY](#))

Explanation

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

:

* Monitor Privileged Sessions - CyberArk

* Privileged Session Manager for Web - CyberArk

NEW QUESTION: 109

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

A. TRUE

B. FALSE

Answer: A ([LEAVE A REPLY](#))

Explanation

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

Auto-detection is a feature that enables the CPM to automatically discover and onboard accounts on target systems that are associated with a specific platform. Auto-detection can be configured in the Platform Management settings for each platform that supports this functionality. However, auto-detection has some limitations, such as requiring the CPM to have access to the target system, not supporting all platforms, and not providing comprehensive information about the accounts and their security risks¹. DNA, on the other hand, is a standalone scanning tool that can discover and audit privileged accounts across the network, regardless of the platform or the CPM access. DNA can provide additional discovery functions, such as identifying machines vulnerable

to Pass-the-Hash attacks, collecting reliable and comprehensive audit information, and generating reports and visual maps that evaluate the privileged account security status in the organization². DNA can also be used before or independently of the CyberArk PAM solution, as it does not require agents to be installed on target systems². References:

* 1: Auto-detection

* 2: CyberArk DNA Overview

NEW QUESTION: 110

An auditor initiates a live monitoring session to PSM server to view an ongoing live session. When the auditor's machine makes an RDP connection the PSM server, which user will be used?

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 111

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 ([LEAVE A REPLY](#))

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: 112

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

A. FALSE

B. TRUE

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 113

Which is the primary purpose of exclusive accounts?

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

B. More frequent password changes

C. Non-repudiation (individual accountability)

D. Reduced risk of credential theft

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 114

Which parameter controls how often the CPM looks for Soon-to-be-expired Passwords that need to be changed.

A. ImmediateInterval

B. HeadStartInterval

C. Interval

D. The CPM does not change the password under this circumstance

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 115

By default, members of which built-in groups will be able to view and configure Automatic Remediation and Session Analysis and Response in the PVWA?

A. Vault Admins

B. Security Admins

C. Security Operators

D. Auditors

Answer: B ([LEAVE A REPLY](#))

Explanation

Security Admins are the built-in group that can view and configure Automatic Remediation and Session Analysis and Response in the PVWA. These features are part of the Privileged Threat

Analytics (PTA) module, which is designed to detect and respond to anomalous activities and risky behaviors in the privileged environment. Security Admins have the permissions to access the PTA settings and configure the policies and actions for Automatic Remediation and Session Analysis and Response. References:

* Defender PAM Sample Items Study Guide, page 18, question 49

* Privileged Threat Analytics Implementation Guide, page 9, section "Security Admins"

NEW QUESTION: 116

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:

File Path:

XML Element:

Connection Type:

Optional Properties:

☐ Port:

☒ XML Attribute:

☒ Password Regex:

☐ Backup Password File:

☐ Usage Display Name:

 **CYBERARK**
The Identity Security Company

Address: [text box]
File Path: [text box]
XML Element: /configuration/appSettings/add[@key="PASSWORD"]
Connection Type: Windows File Sharing ▼

Port: [text box]
XML Attribute: value
Password Regex: (.*)
Backup Password File: [Select] ▼
Usage Display Name: [text box]

☐ 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 ([LEAVE A REPLY](#))

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: 117

Which file must be edited on the Vault to configure it to send data to PTA?

- A. my.ini
- B. PARAgent.ini
- C. dbparm.ini
- D. padr.ini

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 118

Which utilities could you use to change debugging levels on the vault without having to restart the vault. Select all that apply.

- A. PAR Agent
- B. Setup.exe
- C. Edit DBParm.ini in a text editor.
- D. PrivateArk Server Central Administration

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 119

You want to give a newly-created group rights to review security events under the Security pane. You also want to be able to update the status of these events.

Where must you update the group to allow this?

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 120

To enable the Automatic response "Add to Pending" within PTA when unmanaged credentials are found, what are the minimum permissions required by PTAUser for the PasswordManager_pending safe?

- A. List Accounts, View Safe members, Add accounts (includes update properties), Update Account content, Update Account properties
- B. List Accounts, Add accounts (includes update properties), Delete Accounts, Manage Safe
- C. Add accounts (includes update properties), Update Account content, Update Account properties, View Audit

D. View Accounts, Update Account content, Update Account properties, Access Safe without confirmation, Manage Safe, View Audit

Answer: ([SHOW ANSWER](#))

Explanation

To enable the automatic response "Add to Pending" within PTA when unmanaged credentials are found, the PTAUser needs to have the minimum permissions for the PasswordManager_pending safe as follows:

- * List Accounts: This permission allows the PTAUser to view the accounts in the safe and their properties.
- * View Safe members: This permission allows the PTAUser to view the members of the safe and their authorizations.
- * Add accounts (includes update properties): This permission allows the PTAUser to add new accounts to the safe and update their properties, such as name, address, platform, and policy.
- * Update Account content: This permission allows the PTAUser to update the password of the accounts in the safe.
- * Update Account properties: This permission allows the PTAUser to update the properties of the existing accounts in the safe, such as name, address, platform, and policy.

These permissions are required for the PTAUser to be able to detect unmanaged privileged accounts and add them to the pending accounts queue in the PasswordManager_pending safe. The PTAUser also needs to have the same permissions for the PasswordManager_reconcile safe to enable the automatic response "Reconcile credentials" for suspicious password change events. References: Configure PTA Remediations, Safe Member Authorizations

NEW QUESTION: 121

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: ([SHOW ANSWER](#))

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

Valid PAM-DEF Dumps shared by PrepPdf.com for Helping Passing PAM-DEF Exam! PrepPdf.com now offer the **newest PAM-DEF exam dumps**, the PrepPdf.com PAM-DEF exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PAM-DEF dumps with Test Engine here:
<https://www.preppdf.com/CyberArk/PAM-DEF-prepaway-exam-dumps.html> (240 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 122

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

- A. True; this is the default behavior
- B. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the padr.ini file
- C. True, if the AllowFailback setting is set to "yes" in the padr.ini file
- D. False, the Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the dbparm.ini file

Answer: B ([LEAVE A REPLY](#))

Explanation

According to the web search results, when a DR Vault Server becomes an active vault, it will not automatically revert back to DR mode once the Primary Vault comes back online. The Vault administrator must manually set the DR Vault to DR mode by setting "FailoverMode=no" in the padr.ini file¹. This file is located in the /opt/CARKaim/conf directory on the DR Vault machine². The Vault administrator must also stop the replication process on the DR Vault and restart the PrivateArk Server service¹. This procedure is known as a DR failback, which restores the original roles of the Primary Vault and the DR Vault after a failover¹. The AllowFailback setting in the padr.ini file does not affect the DR failback process, as it only determines whether the DR Vault can be used as a backup for another DR Vault in a cascading DR scenario³.

The dbparm.ini file is not relevant for the DR failback process, as it contains the database parameters for the Vault server. References:

- * Initiate a DR failback to the Production Vault - CyberArk
- * Install the Disaster Recovery application - CyberArk
- * Cascading DR - CyberArk
- * [dbparm.ini file - CyberArk]

NEW QUESTION: 123

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 PSM Gateway 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 ([LEAVE A REPLY](#))

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: 124

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: ([SHOW ANSWER](#)**)**

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: 125

The vault supports Subnet Based Access Control.

- A. TRUE
- B. FALSE

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 126

Which parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests.

- A. HeadStartInterval
- B. Interval
- C. ImmediateInterval
- D. The CPM does not change the password under this circumstance

Answer: B ([LEAVE A REPLY](#))

Explanation

This parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests. It is set in the Master Policy under the Dual Control section. The value of this parameter determines the frequency of the CPM's verification process for accounts that have been accessed by users who have received confirmation from authorized Safe owners. The CPM will change the password of these accounts according to the value of this parameter. References:

- * Dual Control - CyberArk
- * Dual control in V10 Interface - docs.cyberark.com
- * PAM-DEF CyberArk Defender - PAM Questions and Answers - Marks4sure

NEW QUESTION: 127

When creating an onboarding rule, it will be executed upon .

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

Answer: C ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 128

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: A,B ([LEAVE A REPLY](#))

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: 129

You want to generate a license capacity report.

Which tool accomplishes this?

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

Answer: B ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 130

A user requested access to view a password secured by dual-control and is unsure who to contact to expedite the approval process. The Vault Admin has been asked to look at the account and identify who can approve their request.

What is the correct location to identify users or groups who can approve?

- A. PrivateArk > Admin Tools > Users and Groups > Auditors (Group Membership)
- B. PVWA> Policies > Access Control (Safes) > Safe Members > Workflow > Authorize Password Requests
- C. PVWA> Administration > Platform Configuration > Edit Platform > UI & Workflow > Dual Control> Approvers
- D. PVWA> Account List > Edit > Show Advanced Settings > Dual Control > Direct Managers

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 131

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

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

Answer: A ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 132

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 133

Which command generates a full backup of the Vault?

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

Answer: A ([LEAVE A REPLY](#))

Explanation

The command PAReplicate.exe with the /FullBackup option is used to generate a full backup of the CyberArk Vault. This command requires the Vault configuration file (typically Vault.ini) and a credential file (specified with /LogonFromFile) that contains the user's encrypted logon credentials. The /FullBackup option indicates that a full backup of the Vault is to be performed, as opposed to an incremental backup¹.

References:

- * CyberArk Docs: Install the Vault Backup Utility²
- * CyberArk Knowledge Article: PAReplicate Configuration and Usage

NEW QUESTION: 134

Which of these accounts onboarding methods is considered proactive?

- A.** A DNA scan
- B.** Detecting accounts with PTA
- C.** A Rest API integration with account provisioning software
- D.** Accounts Discovery

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 135

Which of the following PTA detections require the deployment of a Network Sensor or installing the PTA Agent on the domain controller?

- A.** Unmanaged privileged access
- B.** Suspected credential theft
- C.** Over-Pass-The-Hash
- D.** Golden Ticket

Answer: D ([LEAVE A REPLY](#))

Valid PAM-DEF Dumps shared by PrepPdf.com for Helping Passing PAM-DEF Exam!

PrepPdf.com now offer the **newest PAM-DEF exam dumps**, the PrepPdf.com PAM-DEF exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com PAM-DEF dumps with Test Engine here:

<https://www.preppdf.com/CyberArk/PAM-DEF-prepaway-exam-dumps.html> (240 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)