CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM

NEW QUESTION 1
You have been asked to turn off the time access restrictions for a safe. Where is this setting found?

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

Answer: A

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

NEW QUESTION 2
Which accounts can be selected for use in the Windows discovery process? (Choose two.)

A. an account stored in the Vault
B. an account specified by the user
C. the Vault Administrator
D. any user with Auditor membership
E. the PasswordManager user

Answer: AB

Explanation:
During the Windows discovery process in CyberArk Defender PAM, accounts that can be selected for use include an account that is already stored in the Vault and an account that is specified by the user. The discovery process scans predefined machines for new and modified accounts and their dependencies. After the scan, accounts that should be onboarded into the Vault for secure and automatic management are identified12. References: The information provided is based on general knowledge of CyberArk PAM best practices and the account discovery process as outlined in CyberArk's official documentation1

NEW QUESTION 3
Which one the following reports is NOT generated by using the PVWA?

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

Answer: C

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

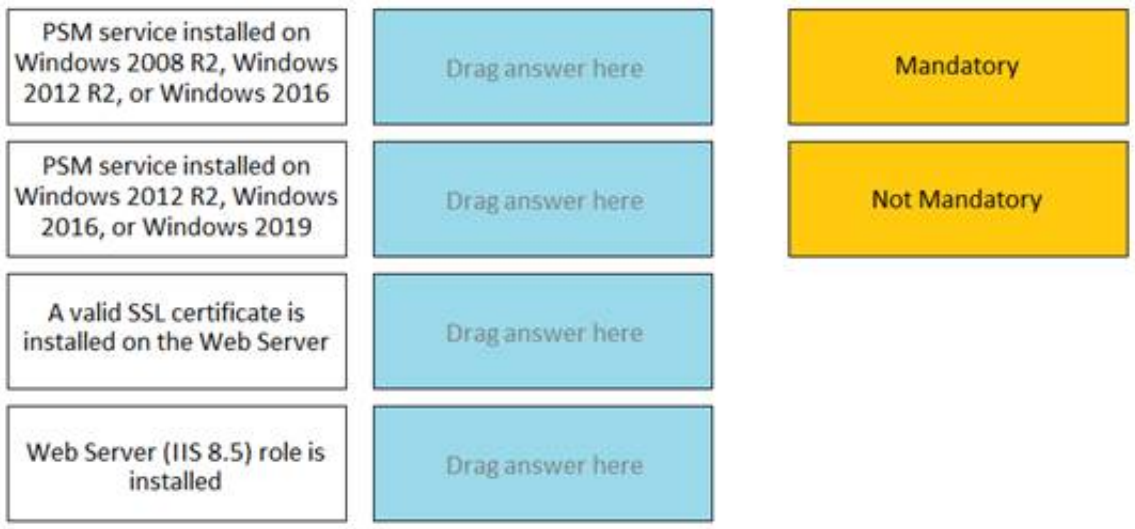
NEW QUESTION 4
Which of the following Privileged Session Management (PSM) solutions support live monitoring of active sessions?

A. PSM (i.e., launching connections by clicking on the connect button in the Password Vault Web Access (PVWA)
B. PSM for Windows (previously known as RDP Proxy)
C. PSM for SSH (previously known as PSM-SSH Proxy)
D. All of the above

Answer: D

Explanation:
According to the web search results, all of the Privileged Session Management (PSM) solutions support live monitoring of active sessions. PSM, PSM for Windows, and PSM for SSH enable authorized users to monitor active sessions from their workstation and take part in controlling these sessions. Users can also suspend or terminate active sessions based on their group assignment. By default, active session monitoring is enabled at system level for all authorized users, and can be disabled at platform level. Active session monitoring can also be disabled at system level, but when it is disabled, it cannot be enabled at platform level. PSM can automatically suspend or terminate sessions when notified by PTA or a third party threat analytics tool1. Authorized users monitor or terminate an active session using the same connection method (RDP file or HTML5 Gateway) as the end user

NEW QUESTION 5
DRAG DROP
For each listed prerequisite, identify if it is mandatory or not mandatory to run the PSM Health Check.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
According to the CyberArk documentation1, the prerequisites for running the PSM Health Check are:
? PSM service installed on Windows 2016 or Windows 2019
? Web Server (IIS 8.5) role is installed
? A valid SSL certificate is installed on the Web Server
Therefore, these prerequisites are mandatory for the PSM Health Check to work properly. The PSM service installed on Windows 2008 R2 is not mandatory, as it is not supported by the PSM Health Check2.
References: PSM Health Check, PSM Health Check - CyberArk

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

NEW QUESTION 6
The vault supports Role Based Access Control.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 7
A new domain controller has been added to your domain. You need to ensure the CyberArk infrastructure can use the new domain controller for authentication. Which locations must you update?

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

Answer: A

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

NEW QUESTION 8
When the CPM connects to a database, which interface is most commonly used?

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

Answer: B

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

NEW QUESTION 9
What is the purpose of a linked account?

A. To ensure that a particular collection of accounts all have the same password.
B. To ensure a particular set of accounts all change at the same time.
C. To connect the CPNI to a target system.
D. To allow more than one account to work together as part of a password management process.

Answer: D

Explanation:
A linked account is an account that is associated with another account to enable the password management process. A linked account can be used for various purposes, such as logging on to a target system, changing the password of another account, or enabling privileged commands. A linked account can be defined either on the platform level or on the account level, depending on the type and scope of the linked account. The types of linked accounts that are supported by CyberArk are1:
? Logon account: An account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the CPM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the CPM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account.
? Reconcile account: An account that contains the password used in reconciliation processes. Reconciliation is 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 sync. A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the target account, the CPM can use the reconcile account to restore the password of the target account, in case it is changed or out of sync.
? Other additional accounts: Additional accounts can be used in various cases. For example:
The other options are not the purpose of a linked account, because:
? A. To ensure that a particular collection of accounts all have the same password.
This is not the purpose of a linked account, but of a group account. A group account is an account that is associated with multiple target systems that share the same credentials. A group account allows the CPM to manage the password of multiple systems with a single password object in the Vault2.
? B. To ensure a particular set of accounts all change at the same time. This is not the purpose of a linked account, but of a password change schedule. A password change schedule is a feature that allows the administrator to define a time frame for changing the passwords of a set of accounts. A password change schedule can be configured either in the Master Policy or in the Platform settings3.
? C. To connect the CPNI to a target system. This is not the purpose of a linked account, but of a service account. A service account is an account that is used by a service or an application to connect to a target system. A service account can be managed by the Central Credential Provider (CCP), which is a component that provides applications and services with the credentials they need to access target systems4.
References:
? 1: Linked Accounts
? 2: Group Accounts
? 3: Password Change Schedule
? 4: Service Accounts

NEW QUESTION 10
Which of the following logs contains information about errors related to PTA?

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

Answer: B

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

NEW QUESTION 10
What is the purpose of the PrivateArk Database service?

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

Answer: D

Explanation:
The purpose of the PrivateArk Database service is to maintain the Vault metadata, which includes the information about the Safes, accounts, policies, users, groups, and audit records that are stored in the Vault. The PrivateArk Database service is a Windows service that manages the database files that contain the Vault data. The PrivateArk Database service is responsible for creating, updating, deleting, and backing up the database files, as well as performing encryption and compression operations on the data1. The PrivateArk Database service is installed automatically as part of the Vault server installation and can be configured using the DBParm.ini file2.
The other options are not the purpose of the PrivateArk Database service, although they may be related to other services or components of the Vault. The PrivateArk Server service is the service that communicates with the components, such as the PVWA, the CPM, the PSM, and the PTA, and handles the requests from the clients and components3. The Event Notification Engine service is the service that sends email alerts from the Vault, based on predefined events and recipients4. The Central Policy Manager component is the component that executes password changes, verifications, and reconciliations for the accounts that are managed by the Vault. References:
? Server Components - CyberArk, section “The PrivateArk Server process (Dbmain)”
? DBParm.ini - CyberArk, section “Main parameters”
? Server Components - CyberArk, section “The PrivateArk Server process (Dbmain)”
? Event Notification Engine - CyberArk, section “Event Notification Engine”
? [Change Passwords - CyberArk], section “Change Passwords”

NEW QUESTION 13
A user is receiving the error message “ITATS006E Station is suspended for User jsmith” when attempting to sign into the Password Vault Web Access (PVWA). Which utility would a Vault administrator use to correct this problem?

A. createcredfile.exe
B. cavaultmanager.exe
C. PrivateArk
D. PVWA

Answer: C

Explanation:
The PrivateArk is a utility that allows the Vault administrator to access and manage the Vault data, users, groups, policies, and settings. The PrivateArk can be used to correct the problem of a user receiving the error message “ITATS006E Station is suspended for User jsmith” when attempting to sign into the PVWA. The error message means that the user has exceeded the number of invalid password attempts and has been locked out from the Vault. To unlock the user, the Vault administrator can use the PrivateArk to activate the suspended station for the user in the Trusted Net Areas1.
The other options are not utilities that can be used to correct this problem. The createcredfile.exe is a utility that creates a credential file for the CPM to connect to the target systems2. The cavaultmanager.exe is a utility that performs various Vault maintenance tasks, such as backup, restore, and encryption3. The PVWA is not a utility, but a web interface that allows the users to access and use the Vault features, such as
managing accounts, requesting passwords, and initiating sessions. References:
? Vault - ITATS006E Station is suspended for User Administrator - force.com, section “Resolution”
? Create a Credential File - CyberArk, section “Create a Credential File”
? Vault Maintenance - CyberArk, section “Vault Maintenance”
? [Password Vault Web Access - CyberArk], section “Password Vault Web Access”

NEW QUESTION 15
Which Cyber Are components or products can be used to discover Windows Services or Scheduled Tasks that use privileged accounts? Select all that apply.

A. Discovery and Audit (DMA)
B. Auto Detection (AD)
C. Export Vault Data (EVD)
D. On Demand Privileges Manager (OPM)
E. Accounts Discovery

Answer: ABE

Explanation:
Discovery and Audit (DMA), Auto Detection (AD), and Accounts Discovery are CyberArk components or products that can be used to discover Windows Services or Scheduled Tasks that use privileged accounts.
? Discovery and Audit (DMA) is a tool that scans Windows servers and workstations
to identify privileged accounts that are used by Windows Services or Scheduled Tasks. DMA can also generate reports on the usage and risks of these accounts.
? Auto Detection (AD) is a feature of the CyberArk Privileged Account Security
Solution that automatically detects and onboards privileged accounts that are used by Windows Services or Scheduled Tasks. AD can also monitor and rotate the passwords of these accounts.
? Accounts Discovery is a feature of the CyberArk Privileged Account Security
Solution that scans the network to discover privileged accounts on various platforms, including Windows. Accounts Discovery can also identify accounts that are used by Windows Services or Scheduled Tasks.
References:
? : Discovery and Audit (DMA) User Guide
? : Auto Detection Implementation Guide
? : Accounts Discovery Implementation Guide

NEW QUESTION 20
Which Vault authorization does a user need to have assigned to able to generate the "Entitlement Report" from the reports page in PVWA? (Choose two.)

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

Answer: BD

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

NEW QUESTION 25
As long as you are a member of the Vault Admins group you can grant any permission on any safe.

A. TRUE
B. FALSE

Answer: B

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

NEW QUESTION 30
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: A

Explanation:
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security- Configuration.htm?TocPath=End%20User%7CSecurity%20Events%7C3
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.
Reference:
Configure security events

NEW QUESTION 31
You want to give a newly-created group rights to review security events under the Security pane. You also want to be able to update the status of these events. Where must you update the group to allow this?

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

Answer: D

Explanation:
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security- Events.htm?TocPath=End%20User%7CSecurity%20Events%7C2#Permissions

NEW QUESTION 32
When an account is unable to change its own password, how can you ensure that password reset with the reconcile account is performed each time instead of a change?

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

Answer: C

Explanation:
In CyberArk's Privileged Access Management (PAM), when an account cannot change its own password, setting the parameter IgnoreReconcileOnMissingAccount to No ensures that the reconcile account is used for password reset. This is because the reconcile account has the necessary

permissions to reset the password when the primary account cannot do so. References: The information provided is based on general knowledge of CyberArk PAM best practices and is not taken from any specific CyberArk Defender PAM course or learning resources.

NEW QUESTION 35
You are concerned about the Windows Domain password changes occurring during business hours.
Which settings must be updated to ensure passwords are only rotated outside of business hours?

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

Answer: B

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

NEW QUESTION 39
Which of the following Privileged Session Management solutions provide a detailed audit log of session activities?

A. PSM (i.e., launching connections by clicking on the "Connect" button in the PVWA)
B. PSM for Windows (previously known as RDP Proxy)
C. PSM for SSH (previously known as PSM SSH Proxy)
D. All of the above

Answer: D

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

NEW QUESTION 43
Platform settings are applied to .

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

Answer: D

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

NEW QUESTION 47
Target account platforms can be restricted to accounts that are stored m specific Safes using the Allowed Safes property.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 50
A user has successfully conducted a short PSM session and logged off. However, the user cannot access the Monitoring tab to view the recordings.

What is the issue?

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

Answer: D

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

NEW QUESTION 55
DRAG DROP
Match each key to its recommended storage location.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? The recommended storage locations for each key are as follows:
? Recovery Private Key: It is recommended to store the Recovery Private Key on the Vault Server Disk Drive. This is because the Recovery Private Key is used to decrypt the data stored in the Vault.
? Recovery Public Key: It is recommended to store the Recovery Public Key in a Hardware Security Module. This is because the Recovery Public Key is used to encrypt the data stored in the Vault.
? Server Key: It is recommended to store the Server Key in a Physical Safe. This is because the Server Key is used to open the Vault, much like the key of a physical Vault. The key is required to start the Vault, after which the Server Key can be removed until the Server is restarted. When the Vault is stopped, the information stored in the Vault is completely inaccessible without that key.
? SSH Keys: It is recommended to store the SSH Keys in the Vault. This is because the SSH Keys are used to connect to remote machines using the SSH protocol. The Vault can manage the passwords and sessions for the SSH Keys and provide secure access to the target systems.
References: Server keys - CyberArk, Cyberark Key Storage Plugin (Enterprise) - Rundeck

NEW QUESTION 57
Which master policy settings ensure non-repudiation?

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

Answer: B

Explanation:
Non-repudiation in the context of CyberArk Master Policy settings refers to the assurance that a user cannot deny the validity of their actions. The settings that ensure non-repudiation are those that enforce accountability and traceability of actions. Enforcing check-in/check-out exclusive access ensures that only one user can access an account at a time, and their actions can be traced back to themEnforcing one-time password access means that passwords are used only once and then changed, which prevents the reuse of credentials and ties actions to specific instances of access12.
References:
? CyberArk Docs: Master Policy Rules2
? CyberArk Docs: The Master Policy1

NEW QUESTION 60
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

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 65
Which user is automatically added to all Safes and cannot be removed?

A. Auditor
B. Administrator
C. Master
D. Operator

Answer: C

Explanation:
The user that is automatically added to all Safes and cannot be removed is the Master user. The Master user is a predefined user that is created during the Vault installation and has full permissions on all Safes and accounts. The Master user is the only user that can perform certain tasks, such as creating other predefined users, managing the Vault configuration, and restoring the Vault from a backup. The Master user cannot be deleted or modified by any other user, and is always a member of every Safe12. References:
? Predefined users and groups - CyberArk, section “Master”
? Safes and Safe members - CyberArk, section “Safe members overview”

NEW QUESTION 68
Which combination of Safe member permissions will allow end users to log in to a remote machine transparently but NOT show or copy the password?

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

Answer: B

Explanation:
The Use Accounts permission enables Safe members to log in to a remote machine through a PSM connection from the Accounts List or the Account Details page. The List Accounts permission enables Safe members to view the Accounts list. However, to show or copy the password, the Safe members also need the Retrieve Accounts permission, which allows them to view and copy the account value in the Account Details
page or the Accounts list. Therefore, the combination of Use Accounts and List Accounts will allow end users to log in to a remote machine transparently but not show or copy the password. References:
? Safe Members - CyberArk1, section “Permissions”
? Safes and Safe members - CyberArk2, section “Safe members overview”

NEW QUESTION 69
CyberArk implements license limits by controlling the number and types of users that can be provisioned in the vault.

A. TRUE
B. FALSE

Answer: B

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

NEW QUESTION 73
Users can be resulted to using certain CyberArk interfaces (e.g.PVWA or PACLI).

A. TRUE
B. FALSE

Answer: A

Explanation:
Users can be restricted to using certain CyberArk interfaces (e.g. PVWA or PACLI) by using the User Type property. The User Type property is a parameter that can be configured in the User Management settings for each user. The User Type property defines which interfaces the user can access the Vault through, such

as PVWA, PrivateArk Client, PACLI, PSM, etc. The User Type property is determined by the CyberArk license and can be assigned to users when they are added to the Vault or when their properties are updated. For example, if a user is assigned the User Type of EPVUser, they can access the Vault through PVWA, PrivateArk Client, PrivateArk Webclient, PACLI, and
PIMSU. However, if a user is assigned the User Type of BizUser, they can only access the Vault through PVWA1. Therefore, by using the User Type property, administrators can control and restrict which CyberArk interfaces the users can use. References:
? 1: Manage users, Types of users subsection

NEW QUESTION 78
How does the Vault administrator apply a new license file?

A. Upload the license.xml file to the system Safe and restart the PrivateArk Server service
B. Upload the license.xml file to the system Safe
C. Upload the license.xml file to the Vault Internal Safe and restart the PrivateArk Server service
D. Upload the license.xml file to the Vault Internal Safe

Answer: C

Explanation:
According to the CyberArk Defender PAM documentation1, the Vault administrator can apply a new license file by uploading the license.xml file to the Vault Internal Safe and restarting the PrivateArk Server service. The Vault Internal Safe is a special Safe that contains the Vault configuration files, including the license file. The Vault administrator can access this Safe from the PrivateArk Client and replace the existing license file with the new one. After that, the Vault administrator must restart the PrivateArk Server service for the changes to take effect. This procedure can be done either from the Vault machine or from a remote machine. References:
? Manage the CyberArk License - CyberArk

NEW QUESTION 79
What is the purpose of the HeadStartInterval setting m a platform?

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

Answer: B

Explanation:
The purpose of the HeadStartInterval setting in a platform is to instruct the CPM to initiate the password change process X number of days before expiration. This setting is used when the platform has the One Time Password feature enabled, which means that the passwords are changed every time they are retrieved by a user. The HeadStartInterval setting defines the number of days before the password expires (according to the ExpirationPeriod parameter) that the CPM will start the password change process. This gives the CPM enough time to change the password before it becomes invalid, and ensures that the user will always receive a valid password when they request it1. The HeadStartInterval setting can be configured in the Platform Management settings for each platform that supports One Time Passwords. The default value is 0, which means that the CPM will start the password change process on the same day as the password expiration date1.
The other options are not the purpose of the HeadStartInterval setting in a platform:
? A. It determines how far in advance audit data is collected for reports. This option
is not related to the HeadStartInterval setting, which does not affect the audit data collection or reporting. The audit data is collected by the Vault server and stored in the Audit database, and the reports are generated by the PVWA or the PrivateArk Client based on the audit data2.
? C. It instructs the AIM Provider to ‘skip the cache’ during the defined time period.
This option is not related to the HeadStartInterval setting, which does not affect the AIM Provider or the cache mechanism. The AIM Provider is a component that enables applications to securely retrieve credentials from the Vault without requiring human intervention. The cache mechanism is a feature that allows the AIM Provider to store credentials locally for a limited time, in case of a temporary network failure or Vault unavailability3.
? D. It alerts users of upcoming password changes x number of days before
expiration. This option is not related to the HeadStartInterval setting, which does not alert users of anything. The HeadStartInterval setting only instructs the CPM to initiate the password change process, not to notify the users. The users do not need to be aware of the password changes, as they are performed automatically by the CPM and do not affect the user experience1. References:
? 1: Privileged Account Management, Min Validity Period subsection
? 2: Reports and Audits
? 3: Application Identity Manager

NEW QUESTION 80
The Vault administrator can change the Vault license by uploading the new license to the system Safe.

A. True
B. False

Answer: A

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

NEW QUESTION 85
Which methods can you use to add a user directly to the Vault Admin Group? (Choose three.)

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

F. Sailpoint

Answer: ABC

Explanation:
To add a user directly to the Vault Admin Group in CyberArk, you can use the following methods:
? REST API: The REST API allows for programmatic management of users and groups within the Vault, including adding users to the Vault Admin Group1.
? PrivateArk Client: The PrivateArk Client provides a graphical interface for managing users and groups, and it can be used to add users directly to the Vault Admin Group2.
? PACLI: The PACLI (Privileged Access Command Line Interface) is a command- line tool that enables administrators to manage the Vault, including adding users to groups2.
These methods provide different ways to manage users and their group memberships within the CyberArk Vault, offering flexibility for administrators to choose the most suitable approach for their needs.
References:
? CyberArk's official documentation on using the REST API to manage users and groups1.
? Information on managing users and groups through the PrivateArk Client and PACLI2.

NEW QUESTION 89
Accounts Discovery allows secure connections to domain controllers.

A. TRUE
B. FALSE

Answer: B

NEW QUESTION 93
It is possible to leverage DNA to provide discovery functions that are not available with auto-detection.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 94
Which of the following properties are mandatory when adding accounts from a file? (Choose three.)

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

Answer: ABC

Explanation:
When adding accounts from a file, certain properties are mandatory to ensure that the accounts can be properly managed within the CyberArk Privileged Access Security system. The Safe Name is required to determine where the account will be stored.
The Platform ID is necessary to apply the correct management policies to the account. Additionallya, ll required properties specified in the Platform must be included to meet the specific requirements for account management as defined by the platform configuration1.
References:
? CyberArk's official documentation on adding multiple accounts from a file, which outlines the mandatory information needed for each account, including Safe Name, Platform ID, and other required properties based on the account's policy requirements1.

NEW QUESTION 98
What is the name of the Platform parameters that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy?

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

Answer: A

Explanation:
The name of the Platform parameter that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy is Min Validity Period. This parameter defines the number of minutes to wait from the last retrieval of the account until it is replaced. This gives the user a minimum period to be

able to use the password before it is changed by the CPM. The Min Validity Period parameter can be configured in the Platform Management settings for each platform that supports One Time Passwords. The default value is 60 minutes, but it can be modified according to the organization's security policy1. The Min Validity Period parameter is also used to release exclusive accounts automatically1. References:
? 1: Privileged Account Management, Min Validity Period subsection

NEW QUESTION 103
You are creating a shared safe for the help desk.
What must be considered regarding the naming convention?

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

Answer: D

Explanation:
When creating a shared safe for the help desk in CyberArk's Privileged Access Management (PAM), it is important to adhere to the naming conventions set forth by CyberArk. One of the key considerations is that certain characters are not permitted in the safe name. Specifically, the characters V:*<>".| are not allowed in the naming of safes. This is to ensure compatibility and prevent issues with the file system or the CyberArk application itself, as these characters may interfere with normal operations or be reserved for specific functions within the operating system or the application.
References: The information regarding safe naming conventions is based on CyberArk's best practices and guidelines, which are detailed in the official CyberArk documentation and study guides. It is important to consult the CyberArk Defender PAM resources and documents to ensure compliance with these standards

NEW QUESTION 107
PSM for Windows (previously known as "RDP Proxy") supports connections to the following target systems

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

Answer: D

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

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

Answer: A

Explanation:
According to the web search results, when an auditor initiates a live monitoring session to PSM server to view an ongoing live session, the auditor's machine makes an RDP connection to the PSM server using the PSMAdminConnect user. The PSMAdminConnect user is a local or domain user that starts PSM sessions on the PSM machine for authorized users who want to monitor or terminate active sessions1. The PSMAdminConnect user has limited permissions and access rights on the PSM server, and its credentials are managed by the CPM. The PSMAdminConnect user retrieves the credentials of the target account from the vault and uses them to establish a secure connection to the target machine. The auditor can then view the live session through the PSM session, while the PSM server records and audits the session activity.

NEW QUESTION 112
What is the maximum number of levels of authorization you can set up in Dual Control?

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

Answer: B

Explanation:
Dual Control is a feature that allows you to set up a workflow for approving access requests to sensitive accounts. You can configure up to two levels of authorization for each account, meaning that you need up to two different authorizers to approve the request before the user can access the account. The authorizers can be either users or groups, and they can have different approval methods, such as email, SMS, or CyberArk interface. References:
? [Defender PAM] course, Module 5: Privileged Session Management, Lesson 5.2:
Dual Control
? [Defender PAM Sample Items Study Guide], Question 31
? [CyberArk Documentation], Dual Control

NEW QUESTION 114
A Vault administrator have associated a logon account to one of their Unix root accounts in
the vault. When attempting to verify the root account's password the Central Policy Manager (CPM) will:

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

Answer: C

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

NEW QUESTION 115
In the Private Ark client under the Tools menu > Administrative Tools > Users and Groups, which option do you use to update users' Vault group memberships?

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

Answer: C

Explanation:
In the PrivateArk client, to update users' Vault group memberships, you use the Member Of tab. After logging in as an administrative user and navigating to the Users and Groups window, you select a user and click Update. In theMember Of tab, you can manage the user's group memberships by adding or removing them from groups within the Vault1.
References:
? CyberArk Docs - Manage users in PrivateArk client1

NEW QUESTION 117
PSM captures a record of each command that was executed in Unix.

A. TRIE
B. FALSE

Answer: A

Explanation:
PSM captures a record of each command that was executed in Unix by using the SSH text recorder. This is a feature that enables PSM to record all the keystrokes that are typed during privileged sessions on SSH connections, including Unix systems. The SSH text recorder can be configured in the Platform Management settings for each platform that uses the SSH protocol. The text recordings are stored and protected in the Vault server and are accessible to authorized auditors. The text recordings can also be used for auditing and compliance purposes, as they provide a detailed trace of the actions performed by the users on the target systems1. References:
? 1: Introduction to PSM for SSH, How it works subsection, Text recordings paragraph

NEW QUESTION 119
For an account attached to a platform that requires Dual Control based on a Master Policy exception, how would you configure a group of users to access a password without approval.

A. Create an exception to the Master Policy to exclude the group from the workflow process.
B. Edith the master policy rule and modify the advanced' Access safe without approval' rule to include the group.
C. On the safe in which the account is stored grant the group the' Access safe without audit' authorization.
D. On the safe in which the account is stored grant the group the' Access safe without confirmation' authorization.

Answer: D

Explanation:
Dual Control is a feature that requires the approval of another user before accessing a password. It is based on a Master Policy rule that applies to all accounts attached to platforms that have this rule enabled. However, there may be situations where a group of users needs to access a password without approval, such as in an emergency or for troubleshooting purposes. In this case, an exception can be made by granting the group the 'Access safe without confirmation' authorization on the safe in which the account is stored. This authorization bypasses the Dual Control workflow and allows the group to retrieve the password without waiting for approval. However, the password retrieval will still be audited and recorded in the Vault.

NEW QUESTION 122
Secure Connect provides the following. Choose all that apply.

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

Answer:

ABC

Explanation:
Secure Connect provides the following features:
? A. PSM connections to target devices that are not managed by CyberArk. This is true, because Secure Connect is a feature that enables users to connect to target systems through PSM without storing the account credentials in the vault. Secure Connect allows users to provide their own credentials at the time of connection, and these credentials are not saved or managed by CyberArk. Secure Connect can be used with any connection component that supports PSM, such as RDP, SSH, WinSCP, etc1.
? B. Session Recording. This is true, because Secure Connect sessions are recorded by PSM and stored in the Vault, just like regular PSM sessions. The recorded sessions can be viewed and audited by authorized users through the PVWA or the PSM web interface2.
? C. Real-time live session monitoring. This is true, because Secure Connect sessions can be monitored in real-time by authorized users through the PSM web interface. The PSM web interface allows users to view the live session screen, send messages to the session user, pause or terminate the session, and take control of the session if needed3.
The following feature is not provided by Secure Connect:
? D. PSM connections from a terminal without the need to login to the PVWA. This is false, because Secure Connect requires users to login to the PVWA and initiate the connection from there. The PVWA provides the URL for the Secure Connect session, which contains the target system address and the connection component ID. The user then needs to copy and paste the URL into a browser or a remote connection manager to launch the session1.
References:
? 1: Secure Connect
? 2: Recorded Sessions
? 3: PSM Web Interface

NEW QUESTION 123
Which report shows the accounts that are accessible to each user?

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

Answer: B

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

NEW QUESTION 125
If PTA is integrated with a supported SIEM solution, which detection becomes available?

A. unmanaged privileged account
B. privileged access to the Vault during irregular days
C. riskySPN
D. exposed credentials

Answer: D

Explanation:
When Privileged Threat Analytics (PTA) is integrated with a supported Security Information and Event Management (SIEM) solution, the detection of exposed credentials becomes available. This integration allows PTA to detect when a user is connected to a machine with a privileged account without first retrieving the credential from the CyberArk Digital Vault. In such cases, PTA can prompt an immediate credential rotation and send an alert to the SIEM, indicating a suspected credential theft1.
References:
? CyberArk Docs - SIEM Integration2
? CyberArk Blog - Integrate CyberArk with a SIEM Solution1

NEW QUESTION 128
It is possible to restrict the time of day, or day of week that a [b]reconcile[/b] process can occur

A. TRUE
B. FALSE

Answer: A

Explanation:
It is possible to restrict the time of day, or day of week that a reconcile process can occur by using the Reconcile Safe option in thePlatform Management section of thePrivateArk Client. This option allows the administrator to define the reconcile schedule for each platform, which specifies when the reconcile process can run and how often it should be performed. The reconcile schedule can be set to run daily, weekly, monthly, or on specific days and times. By restricting the reconcile process, the administrator can reduce the risk of unauthorized access to the accounts and improve the performance of the system. References:
? [Defender PAM Course], Module 5: Reconcile and Rotate, Lesson 1: Reconcile and Rotate Overview, Slide 9: Reconcile Safe
? [Defender PAM Study Guide], Section 5.1: Reconcile and Rotate Overview, Page 24: Reconcile Safe
? [CyberArk Documentation], Privileged Access Security Implementation Guide, Chapter 5: Configure the Vault, Section 5.4: Configure Platforms, Subsection 5.4.2: Reconcile Safe

NEW QUESTION 132
VAULT authorizations may be granted to .

A. Vault Users

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

Answer: AC

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

NEW QUESTION 135
One can create exceptions to the Master Policy based on .

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

Answer: B

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

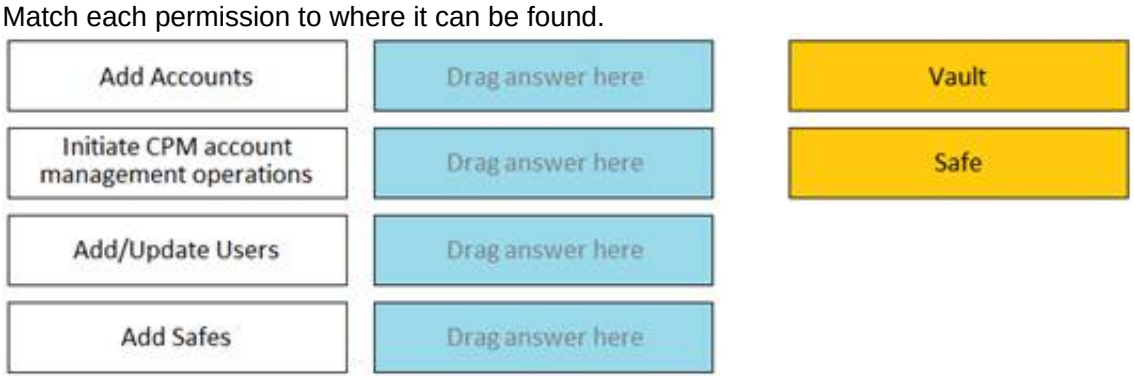
NEW QUESTION 137
The vault supports Subnet Based Access Control.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 138
DRAG DROP
Match each permission to where it can be found.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Add Accounts: This permission is associated with the ability to add new accounts to the CyberArk Vault. It is typically found in the Vault's administrative settings where account management is handled.
? Initiate CPM account management operations: This permission allows users to initiate operations related to the Central Policy Manager (CPM) for account management within a Safe. It is found in the Safe's permissions settings.
? Add/Update Users: This permission enables the addition or updating of user information in the Vault. It is found in the Vault's user management settings.
? Add Safes: This permission is related to the creation of new Safes in the Vault. It is found in the Vault's administrative settings where Safe management is conducted.
References:
? The permissions and their locations can be referenced in the CyberArk Defender PAM course materials and official documentation, which provide detailed information on the management of permissions within the CyberArk solution.

NEW QUESTION 142
Which service should NOT be running on the DR Vault when the primary Production Vault is up?

A. PrivateArk Database
B. PrivateArk Server
C. CyberArk Vault Disaster Recovery (DR) service
D. CyberArk Logical Container

Answer: C

Explanation:
The user that is automatically added to all Safes and cannot be removed is the Master user. The Master user is a predefined user that is created during the Vault installation and has full permissions on all Safes and accounts. The Master user is the only user that can perform certain tasks, such as creating other predefined users, managing the Vault configuration, and restoring the Vault from a backup. The Master user cannot be deleted or modified by any other user, and is always a member of every Safe12. References:
? Predefined users and groups - CyberArk, section “Master”
? Safes and Safe members - CyberArk, section “Safe members overview”

NEW QUESTION 147
Which parameter controls how often the CPM looks for Soon-to-be-expired Passwords that need to be changed.

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

Answer: A

NEW QUESTION 149
When onboarding multiple accounts from the Pending Accounts list, which associated setting must be the same across the selected accounts?

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

Answer: A

Explanation:
When onboarding multiple accounts from the Pending Accounts list, all the selected accounts must be associated with the same platform. This is necessary because the platform setting determines how the accounts will be managed within CyberArk, including the policies and behaviors that apply to those accounts. If an account contains dependencies, those dependencies are automatically onboarded with the account. This ensures that all accounts and their dependencies are managed consistently and according to the correct policies1.
References:
? CyberArk’s official documentation on Onboarding Accounts and SSH Keys1.

NEW QUESTION 151
Can the 'Connect' button be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied?

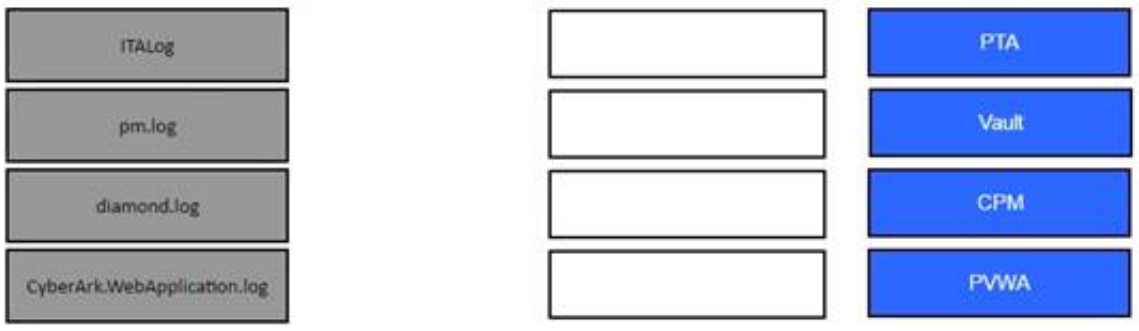
A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction.
B. Yes, only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component.
C. Yes, if a logon account is associated with the root account.
D. No, it is not possible.

Answer: B

Explanation:
The ‘Connect’ button is a feature of the PVWA that allows users to initiate a privileged session to a target system through PSM without revealing the account credentials. The ‘Connect’ button can be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, but only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component. A logon account is a linked account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the PSM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the PSM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account. The PSM-SSH connection component is a predefined connection component that enables users to connect to Unix systems through PSM using SSH. The PSM-SSH connection component supports the use of logon accounts to access root accounts on Unix systems1.
The other options are not correct, because:
? A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction. This is not correct, because PMTerminal.exe is a process that is used by the PSM-RDP connection component, not the PSM-SSH connection component. PMTerminal.exe is a terminal emulator that enables users to connect to Windows systems through PSM using RDP. PMTerminal.exe does not bypass the root SSH restriction, but rather uses the credentials stored in the Vault to authenticate to the target system2.
? C. Yes, if a logon account is associated with the root account. This is not correct, because a logon account alone is not sufficient to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied. The user also needs to connect through the PSM-SSH connection component, which supports the use of logon accounts to access root accounts on Unix systems1.
? D. No, it is not possible. This is not correct, because it is possible to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, as explained in option B.
References:
? 1: Logon Accounts for SSH and Telnet Connections
? 2: Connect through PSM for SSH

NEW QUESTION 153
DRAG DROP

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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
? Log Files
? [Defender PAM Sample Items Study Guide], Question 46, page 16

NEW QUESTION 154
Customers who have the ‘Access Safe without confirmation’ safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.

A. TRUE
B. FALSE

Answer: B

Explanation:
Customers who have the ‘Access Safe without confirmation’ safe permission on a safe where accounts are configured for Dual control, do not need to request approval to use the account. The ‘Access Safe without confirmation’ safe permission allows users to access accounts without confirmation from authorized users, even if the Master Policy or an exception enforces Dual Control1. This means that users who have this permission can bypass the workflow process and access the account password or connect to the target system immediately. This permission can be granted to users or groups on a safe level by the safe owner or another user with the Manage Safe authorization2. References:
? 1: Dual Control, Advanced Settings subsection
? 2: CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section: Safe Authorizations, Table 2-1: Safe Authorizations

NEW QUESTION 159
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

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 163
A newly created platform allows users to access a Linux endpoint. When users click to connect, nothing happens.
Which piece of the platform is missing?

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

Answer: A

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

NEW QUESTION 165
Which permissions are needed for the Active Directory user required by the Windows Discovery process?

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

Answer: D

Explanation:
The Active Directory user required by the Windows Discovery process needs to have Read permissions in the OU to scan and all sub-OUs1. This allows the Discovery process to scan predefined machines for new and modified accounts and their dependencies without requiring elevated privileges such as Domain Admin or LDAP Admin rights. The Read permission is sufficient for the Discovery process to retrieve the necessary information about the accounts that should be onboarded into the Vault. References:
? CyberArk's official documentation on managing discovery processes outlines the permissions required for the Discovery process, including the need for Read permissions for the Active Directory user performing the discovery1.
? Additional details on the required credentials for scanning and the Discovery process can be found in the supported target machines section of CyberArk's documentation2.

NEW QUESTION 166
For Digital Vault Cluster in a high availability configuration, how does the cluster determine if a node is down?

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

Answer: A

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

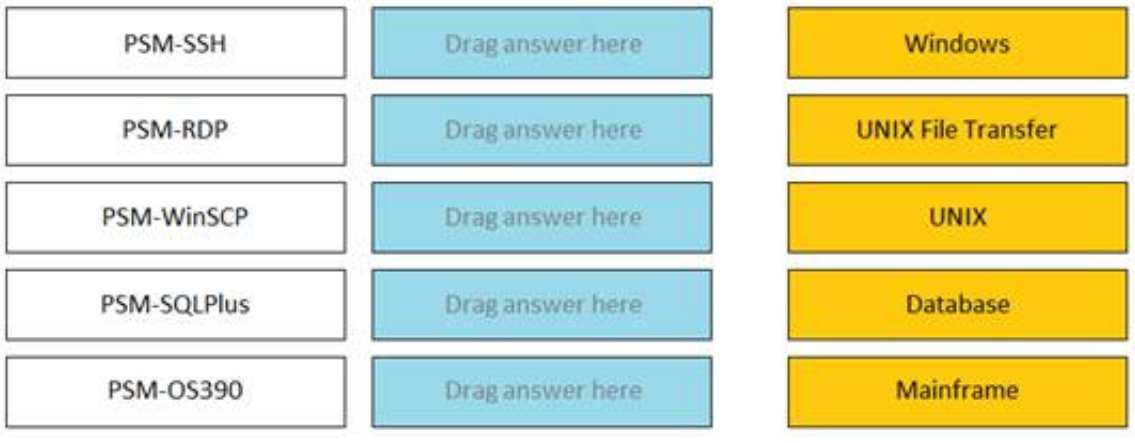
NEW QUESTION 170
Which report could show all accounts that are past their expiration dates?

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

Answer: A

Explanation:
The Privileged Account Compliance Status report shows the compliance status of all privileged accounts in the Vault, based on the expiration date and password change policy. This report can help identify accounts that are past their expiration dates and need to be updated or removed. References:
? [Defender PAM Sample Items Study Guide], page 18, question 90
? [CyberArk Privileged Access Security Documentation], version 12.3, Reports Guide, page 27, Privileged Account Compliance Status report

NEW QUESTION 172
DRAG DROP
Match the connection component to the corresponding OS/Function.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
? A connection component is a set of parameters that defines how PSM connects to a target system using a specific protocol or application. Different connection components are suitable for different types of systems or functions. The correct matches are as follows:
? PSM-SSH: This connection component enables transparent connections to UNIX machines using the SSH protocol. It supports various UNIX flavors, such as

Linux, Solaris, AIX, and HP-UX.
? PSM-RDP: This connection component enables transparent connections to Windows machines using the RDP protocol. It supports various Windows versions, such as Windows Server, Windows 10, and Windows 7.
? PSM-WinSCP: This connection component enables transparent connections to UNIX machines using the WinSCP application. It supports file transfer operations, such as upload, download, delete, and rename, between the local and remote machines.
? PSM-SQLPlus: This connection component enables transparent connections to Oracle databases using the SQL*Plus application. It supports various Oracle versions, such as Oracle 12c, Oracle 11g, and Oracle 10g.
? PSM-OS390: This connection component enables transparent connections to IBM mainframes using the OS/390 protocol. It supports various mainframe applications, such as TSO, CICS, and IMS.
References: Connection Components, Connection Component Parameters

NEW QUESTION 176
Due to corporate storage constraints, you have been asked to disable session monitoring and recording for 500 testing accounts used for your lab environment. How do you accomplish this?

A. Master Policy>select Session Management>add Exceptions to the platform(s)>disable Session Monitoring and Recording policies
B. Administration>Platform Management>select the platform(s)>disable Session Monitoring and Recording Most Voted
C. Polices>Access Control (Safes)>select the safe(s)>disable Session Monitoring and Recording policies
D. Administration>Configuration Options>Options>select Privilege Session Management>disable Session Monitoring and Recording policies

Answer: D

Explanation:
To disable session monitoring and recording for a large number of accounts due to storage constraints, you would navigate to the Administration section of the CyberArk Privileged Access Security (PAS) solution, specifically to the Configuration Options. From there, you would select the Privilege Session Management (PSM) options and disable the Session Monitoring and Recording policies. This action would apply the changes to the specified accounts, thus disabling the session monitoring and recording features for them1. References: The answer is based on general knowledge of CyberArk PAS and best practices for managing session policies within the system. For specific steps and detailed procedures, please refer to the official CyberArk Defender PAM course materials and documentation

NEW QUESTION 179
Which file must be edited on the Vault to configure it to send data to PTA?

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

Answer: A

Explanation:
To configure the CyberArk Vault to send data to Privileged Threat Analytics (PTA), you must edit the dbparm.ini file on the Vault. This file contains parameters that specify how the Vault should forward syslog events to PTA, ensuring that the Vault can send secured syslog data to PTA for analysis and threat detection1.
References:
? CyberArk Docs: Configure Vault Trusted Connection to PTA2
? Netenrich: CyberArk Vault via Syslog1

NEW QUESTION 183
A user with administrative privileges to the vault can only grant other users privileges that he himself has.

A. TRUE
B. FALSE

Answer: B

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

NEW QUESTION 186
Within the Vault each password is encrypted by:

A. the server key
B. the recovery public key
C. the recovery private key
D. its own unique key

Answer: D

Explanation:
According to the web search results, within the Vault each password is encrypted by its own unique key. This key is generated by the Vault when the password is added to the Vault and is stored in the Vault's database. The password key is encrypted by the safe key, which is the key of the safe that contains the password. The safe key is encrypted by the server key, which is the key that opens the Vault. The server key is encrypted by the public recovery key, which is part of the asymmetric recovery key that enables the Master User to log on to the Vault in case of a disaster. This layered encryption scheme ensures that each password is protected by multiple keys and that no single key can compromise the security of the Vault

NEW QUESTION 190
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

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.

NEW QUESTION 191
Which built-in report from the reports page in PVWA displays the number of days until a password is due to expire?

A. Privileged Accounts Inventory
B. Privileged Accounts Compliance Status
C. Activity Log
D. Privileged Accounts CPM Status

Answer: A

Explanation:
ThePrivileged Accounts Inventory report in PVWA includes a column that displays the Age of the password, which indicates the number of days since the password was created1. This information can be used to determine how many days are left until a password is due to expire, based on the password policy's expiration settings.
References:
? CyberArk's official documentation on PVWA reports provides a list of available reports and their descriptions, including the Privileged Accounts Inventory report which contains details about password age and other relevant information1.

NEW QUESTION 195
According to CyberArk, which issues most commonly cause installed components to display as disconnected in the System Health Dashboard? (Choose two.)

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

Answer: AC

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

NEW QUESTION 199
Which is the primary purpose of exclusive accounts?

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

Answer: D

Explanation:
According to the web search results, exclusive accounts are a feature of CyberArk Defender PAM that enables organizations to permit users to check out a 'one-time' password and lock it so that no other users can retrieve it at the same time1. After the user has used the password, the user checks the password back into the Vault. This ensures exclusive usage of the privileged account, enabling full control and tracking for the password. The duration of the check-out period can be configured in the platform settings for each account1.
The primary purpose of exclusive accounts is to prevent a single user from accessing a sensitive account without authorization, which could lead to fraud or misuse of privileges. By requiring a check-out and check-in process, exclusive accounts ensure that there is a 'collusion to commit' fraud, meaning that at least two users are involved in the malicious activity and are accountable for it. One user must check out the password and use it, while another user must approve the check-in and verify the password change. This way, exclusive accounts add an additional measure of protection and accountability for accessing sensitive accounts.

NEW QUESTION 202

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

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

Answer: D

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

NEW QUESTION 205
Your customer, ACME Corp, wants to store the Safes Data in Drive D instead of Drive C. Which file should you edit?

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

Answer: A

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

NEW QUESTION 209
What is the chief benefit of PSM?

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

Answer: D

Explanation:
According to the web search results, the chief benefit of PSM is to provide both privileged session isolation and privileged session recording. Privileged session isolation means that the PSM server acts as a proxy between the user and the target machine, preventing the user from directly accessing the target machine or exposing the privileged account credentials. Privileged session recording means that the PSM server captures and stores a video and a transcript of the user's activity on the target machine, enabling auditing and monitoring of the privileged session. These benefits help to enhance the security and compliance of the privileged access management solution, as they prevent credential exposure, restrict unauthorized access, detect malicious activity, and provide evidence for forensic analysis

NEW QUESTION 210
SAFE Authorizations may be granted to . Select all that apply.

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

Answer: ABCD

Explanation:
SAFE Authorizations may be granted to Vault Users, Vault Groups, LDAP Users, and LDAP Groups. These are the four types of users that can be defined in the Vault and assigned permissions to access Safes and manage passwords. Vault Users and Vault Groups are created and managed within the Vault, while LDAP Users and LDAP Groups are imported from an external directory service such as Active Directory. References:
? Defender PAM Course, Module 4: Managing Safes, Lesson 4.2: Safe Authorizations, slide 4
? Defender PAM Sample Items Study Guide, Question 39, page 15
? CyberArk Privileged Access Security Documentation, Vault Administration Guide, Chapter 4: Managing Safes, Section: Safe Authorizations, page 4-12

NEW QUESTION 213
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: B

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 217
In the Private Ark client, how do you add an LDAP group to a CyberArk group?

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

Answer: C

Explanation:
To add an LDAP group to a CyberArk group, you need to use the Private Ark client and follow these steps1:
? In the Users and Groups tree, select the CyberArk group that you want to add the
LDAP group to.
? In the Properties pane, click Member Of.
? Click Add > LDAP Group.
? In the LDAP Group dialog box, enter the name of the LDAP group and click OK. References: Add an LDAP group to a Vault group

NEW QUESTION 219
You need to enable the PSM for all platforms. Where do you perform this task?

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

Answer: A

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

NEW QUESTION 222
The password upload utility must run from the CPM server

A. TRUE
B. FALSE

Answer: A

Explanation:
According to the CyberArk documentation1, the Password Upload utility must run from the Central Policy Manager (CPM) server. This utility works by uploading passwords and their properties into the Password Vault from a pre-prepared file, creating the required environment, when necessary. It is run from a command line whenever a password upload is required1.

NEW QUESTION 227
CyberArk recommends implementing object level access control on all Safes.

A. True
B. False

Answer: B

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

NEW QUESTION 228
dbparm.ini is the main configuration file for the Vault.

A. True
B. False

Answer: B

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

NEW QUESTION 229
The Password upload utility can be used to create safes.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 230
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 the Active Directory and ensure the organizational unit exists.
B. 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.
C. Search for members that exist only in the mapping group to grant them safe permissions through the PVWA.
D. Connect to the PrivateArk Client with the Administrator Account to see if there is a user in the Vault Admin Group.

Answer: C

Explanation:
The newly configured directory mapping can be tested by searching for members that exist only in the mapping group to grant them safe permissions through the PVWA (Privileged Vault Web Access). This process allows you to verify that the directory mapping is functioning correctly by ensuring that only the intended users, who are part of the specific Active Directory group, are granted access to the safes in the CyberArk Vault12.
References:
? CyberArk Docs - Create directory mapping1
? CyberArk Docs - Edit directory mapping3
? CyberArk Docs - LDAP Integration in PVWA

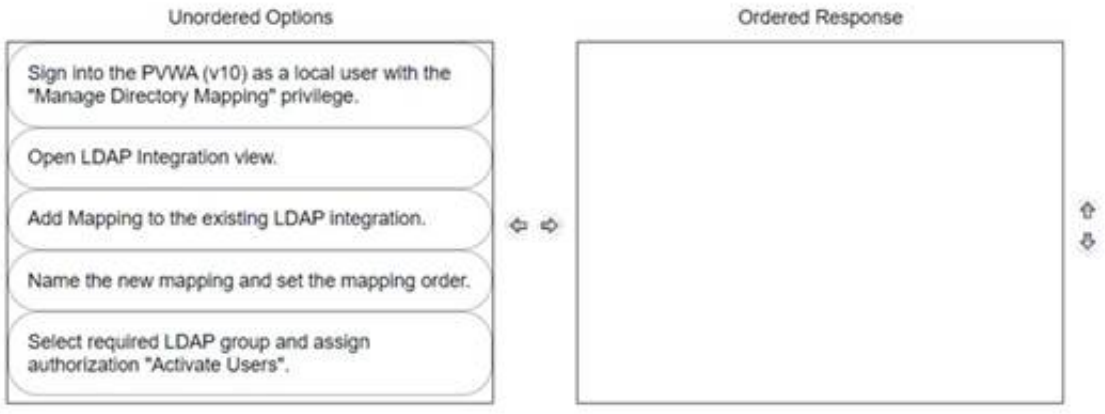
NEW QUESTION 235
To enable the Automatic response “Add to Pending” within PTA when unmanaged credentials are found, what are the minimum permissions required by PTAUser for the PasswordManager_pending safe?

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: A

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 240
DRAG DROP
You have been asked to delegate the rights to unlock users to Tier 1 support. The Tier 1 support team already has an LDAP group for its members.
Arrange the steps to do this in the correct sequence.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 245
DRAG DROP
Match each PTA alert category with the PTA sensors that collect the data for it.

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 248
Which of the following PTA detections require the deployment of a Network Sensor or installing the PTA Agent on the domain controller?

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

Answer: C

Explanation:
According to the CyberArk Defender PAM documentation1, the PTA detection that requires the deployment of a Network Sensor or installing the PTA Agent on the domain controller is Golden Ticket. A Golden Ticket is a type of attack that involves creating a forged Kerberos Ticket Granting Ticket (TGT) that grants the attacker access to any resource in the domain. The attacker needs to compromise the domain controller and steal the KRBTGT account password hash to create the Golden Ticket. The PTA Network Sensor or the PTA Agent can detect this attack by analyzing the network traffic and identifying anomalies in the Kerberos protocol, such as TGTs with abnormal lifetime, encryption type, or renewal time. The PTA Server then alerts the security team and provides details about the attack, such as the source IP, the target domain, and the ticket properties. References:
? PTA Network Sensors - CyberArk

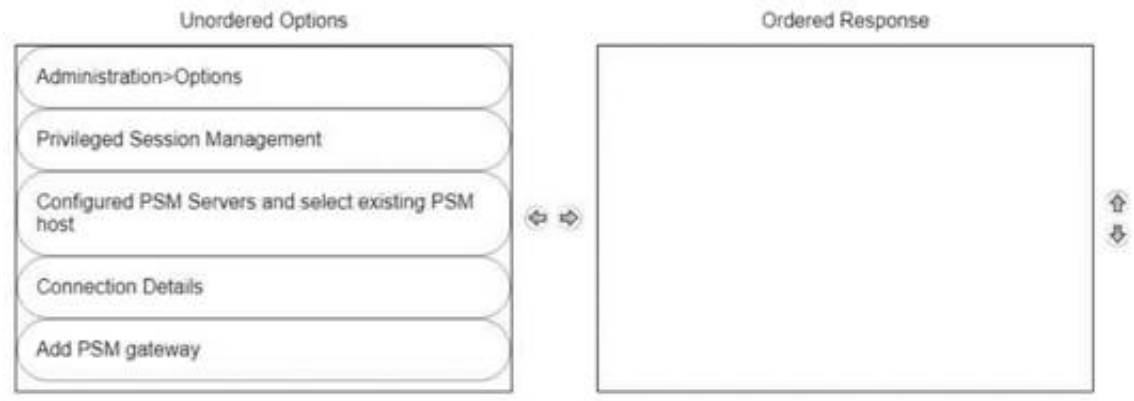
NEW QUESTION 253
How much disk space do you need on the server for a PAReplicate?

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

Answer: D

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 256
DRAG DROP
A new HTML5 Gateway has been deployed in your organization.
From the PVWA, arrange the steps to configure a PSM host to use the HTML5 Gateway in the correct sequence.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 259
Which processes reduce the risk of credential theft? (Choose two.)

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

Answer: BD

NEW QUESTION 264
You have been asked to identify the up or down status of Vault services. Which CyberArk utility can you use to accomplish this task?

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

Answer: C

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

NEW QUESTION 269
When Dual Control is enabled a user must first submit a request in the Password Vault Web Access (PVWA) and receive approval before being able to launch a

secure connection via PSM for Windows (previously known as RDP Proxy).

A. True
B. False, a user can submit the request after the connection has already been initiated via the PSM for Windows

Answer: A

Explanation:
According to the CyberArk Defender PAM documentation1, when Dual Control is enabled, a user must first submit a request in the Password Vault Web Access (PVWA) and receive approval before being able to launch a secure connection via PSM for Windows (previously known as RDP Proxy). This is a security feature that ensures that passwords can only be retrieved after permission or 'confirmation' has been granted from an authorized Safe Owner(s). The user must specify the reason for accessing the account, whether they will access it once or multiple times, and the time period during which they will access it. The request is then sent to the authorized Safe Owners, who can either confirm or reject it. The number of confirmations required is defined in the Master Policy. Only after the user receives the required confirmations, they can activate the request and access the account through PSM for Windows. This way, Dual Control adds an additional measure of protection and accountability for accessing sensitive accounts.

NEW QUESTION 272
You receive this error:
"Error in changepass to user domain\user on domain server(\domain.(winRc=5) Access is denied."
Which root cause should you investigate?

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

Answer: A

Explanation:
The error message "Error in changepass to user domain\user on domain server(\domain.(winRc=5) Access is denied" suggests that the account attempting to change the password does not have the necessary permissions to do so. This could be due to several reasons, such as the account not being part of the appropriate group with password change privileges, or specific restrictions set on the account that prevent password changes. It's important to verify the account's permissions and ensure it has the ability to change its own password within the domain.
References: The conclusion is based on common issues encountered in CyberArk's Privileged Access Management (PAM) when managing account passwords and the associated error codes. The CyberArk documentation and community discussions provide insights into troubleshooting such errors, where insufficient permissions are a frequent cause

NEW QUESTION 275
DRAG DROP
Arrange the steps to restore a Vault using PARestore for a Backup in the correct sequence.

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

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 279
You have associated a logon account to one your UNIX cool accounts in the vault. When attempting to [b]change [/b] the root account's password the CPM will…..

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

Answer: C

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

AutoLogonSequenceWithLogonAccount parameter for a Unix platform:

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

This parameter instructs the CPM to log in to the system as the logon account, enter the logon password, run the su - command to switch to the root user, enter the logon password again, run the change command to change the root password, exit the root session, and exit the logon session1.
The other options are not correct, as follows:
? A. Log in to the system as root, then change root's password. This option is not possible, because the root account cannot be used for direct logon. The logon account is associated with the root account to enable the CPM to access the system and change the password1.
? B. Log in to the system as the logon account, then change root's password. This option is not effective, because the logon account does not have the permission to change the root's password. The logon account needs to elevate itself to the root user by using the su command before changing the password1.
? D. None of these. This option is not valid, because there is a correct answer among the choices.
References:
? 1: Logon Accounts for SSH and Telnet Connections

NEW QUESTION 281
What is required to manage loosely connected devices?

A. PSM for SSH
B. EPM
C. PSM
D. PTA

Answer: B

Explanation:
To manage loosely connected devices, which are not always connected to the network, CyberArk uses the Endpoint Privilege Manager (EPM). EPM is capable of rotating credentials of accounts on Windows and macOS devices that are loosely connected to the enterprise network. It operates over the internet and can communicate with the corporate PVWA to retrieve the new password and change it on the device1. References: The information provided is based on general knowledge of CyberArk PAM
best practices and the management of loosely connected devices as outlined in CyberArk's official documentation1.

NEW QUESTION 282
What is the purpose of the password change process?

A. To test that CyberArk is storing accurate credentials for accounts
B. To change the password of an account according to organizationally defined password rules
C. To allow CyberArk to manage unknown or lost credentials
D. To generate a new complex password

Answer: B

Explanation:
The purpose of the password change process is to change the password of an account according to organizationally defined password rules. The password change process is a feature of CyberArk that enables the Central Policy Manager (CPM) to manage the passwords of privileged accounts that are stored in the Vault. The CPM can change the passwords automatically or manually, based on predefined policies, schedules, or user requests. The password change process ensures that the passwords are secure, compliant, and synchronized with the target systems and the Vault. The password change process also supports different types of accounts, such as one-time passwords, exclusive accounts, and dual accounts1.
The other options are not the main purpose of the password change process, although they may be related to some aspects of it. The password change process does not test that CyberArk is storing accurate credentials for accounts, although it may verify the password validity before changing it. The password change process does not allow CyberArk to manage unknown or lost credentials, although it may reconcile the passwords if they are out of sync with the target systems. The password change process does not generate a new complex password, although it may use a random password generation mechanism to create a new password that meets the password policy requirements. References:
? Change Passwords - CyberArk, section "Change Passwords"

NEW QUESTION 284
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

PAM-DEF Practice Exam Features:

* PAM-DEF Questions and Answers Updated Frequently

* PAM-DEF Practice Questions Verified by Expert Senior Certified Staff

* PAM-DEF Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* PAM-DEF Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year