CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM

NEW QUESTION 1
Which parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests.

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

Answer: B

Explanation:
This parameter controls how often the CPM looks for accounts that need to be changed from recently completed Dual control requests. It is set in the Master Policy under the Dual Control section. The value of this parameter determines the frequency of the CPM's verification process for accounts that have been accessed by users who have received confirmation from authorized Safe owners. The CPM will change the password of these accounts according to the value of this parameter. References:
? Dual Control - CyberArk
? Dual control in V10 Interface - docs.cyberark.com
? PAM-DEF CyberArk Defender – PAM

NEW QUESTION 2
A Vault Administrator team member can log in to CyberArk, but for some reason, is not given Vault Admin rights.
Where can you check to verify that the Vault Admins directory mapping points to the correct AD group?

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

Answer: C

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

NEW QUESTION 3
The primary purpose of exclusive accounts is to ensure non-repudiation (Individual accountability).

A. TRUE
B. FALSE

Answer: A

Explanation:
The primary purpose of exclusive accounts is to ensure non-repudiation (individual accountability). Exclusive accounts are accounts that can only be used by one user at a time, and are locked during usage. This means that no other user can access the same account until the current user releases it or the session expires. By using exclusive accounts, the organization can enforce individual accountability and traceability for the actions performed on the target systems. Exclusive accounts also reduce the risk of credential theft and unauthorized access, as the passwords are changed every time they
are retrieved by a user1. Exclusive accounts can be configured in the Master Policy under the Password Management section, by enabling the Exclusive Access rule2. References:
? 1: The Master Policy, One Time Password subsection
? 2: The Master Policy, Exclusive Access subsection

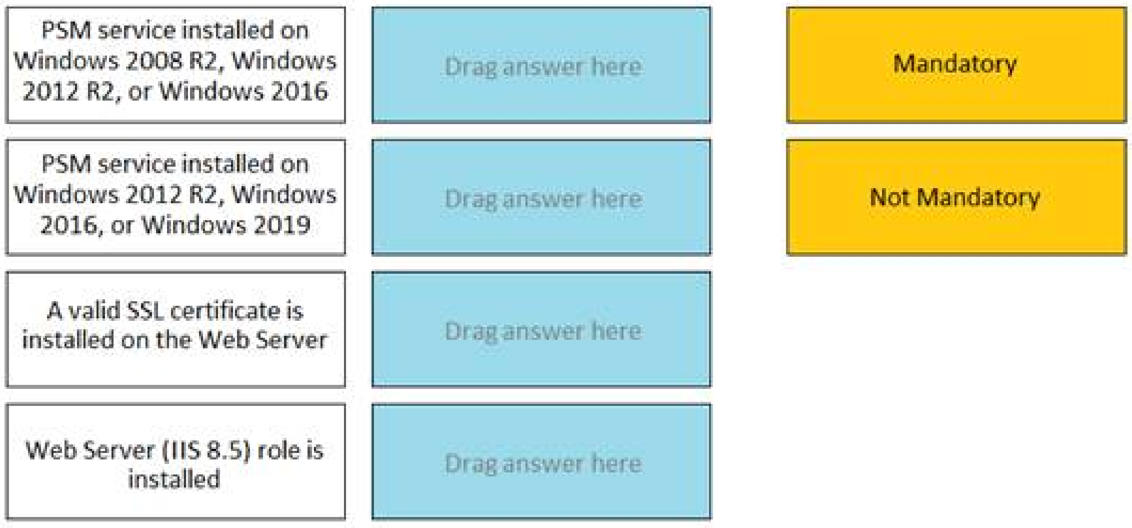
NEW QUESTION 4
Which parameters can be used to harden the Credential Files (CredFiles) while using CreateCredFile Utility? (Choose three.)

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

Answer: BCE

Explanation:
When using the CreateCredFile Utility to harden Credential Files (CredFiles), it is important to include parameters that enhance security. The Host IP Address, Client Hostname, and Vault IP Address are parameters that can be used to specify the environment in which the CredFile is valid, thereby restricting its use to specific machines or networks1. This helps prevent unauthorized access to the CredFile and ensures that it is only used in the intended context.
References:
? CyberArk's official documentation on the CreateCredFile utility provides insights into the security mechanisms used to protect credential files, including the use of environmental key materials such as application-based, machine-based, and component-based materials1.
? For a deeper understanding of how to secure Credential Files and the use of the CreateCredFile Utility, refer to the CyberArk Defender PAM course materials and study guide2.

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

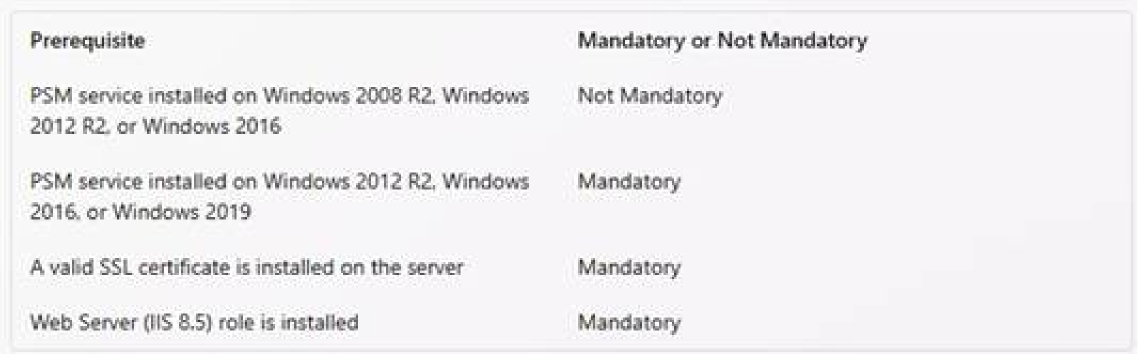


PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016	Drag answer here	Mandatory
PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019	Drag answer here	Not Mandatory
A valid SSL certificate is installed on the Web Server	Drag answer here	
Web Server (IIS 8.5) role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

A. Mastered
B. Not Mastered

Answer: A

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



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

NEW QUESTION 6
Which keys are required to be present in order to start the PrivateArk Server service?

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

Answer: AC

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

NEW QUESTION 7
A new HTML5 Gateway has been deployed in your organization. Where do you configure the PSM to use the HTML5 Gateway?

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

Answer: C

Explanation:
After deploying a new HTML5 Gateway in your organization, you configure the PSM to use the HTML5 Gateway by navigating to the Administration section in the PVWA. From there, you go to Options, then Privileged Session Management, and under Configured PSM Servers, you will find the option to Add PSM Gateway1. This is where you can specify the details of the newly deployed HTML5 Gateway to ensure that the PSM can utilize it for secure remote access to target machines through an HTML5-based session. References:
? CyberArk's official documentation provides a step-by-step guide on how to install and configure the PSM HTML5 Gateway, including the process of adding the gateway to the PSM configuration1.
? For more detailed instructions and best practices on configuring the PSM with an HTML5 Gateway, refer to the CyberArk Defender PAM course materials and

study guides

NEW QUESTION 8
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 9
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 10
What is required to enable access over SSH to a Unix account through both PSM and PSMP?

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

Answer: A

Explanation:
To enable access over SSH to a Unix account through both Privileged Session Manager (PSM) and Privileged Session Manager Proxy (PSMP), the platform must contain the necessary connection components for both PSM-SSH and PSMP-
SSH. This ensures that the system can handle SSH connections through PSM for a native user experience and through PSMP for secure, transparent connections to remote systems12. References:
? CyberArk Docs: Connect through PSM for SSH1
? CyberArk Docs: Connect to Unix machines (using PSM for SSH)2

NEW QUESTION 10
As long as you are a member of the Vault Admins group, you can grant any permission on any safe that you have access to.

A. TRUE
B. FALSE

Answer: B

Explanation:
Being a member of the Vault Admins group does not automatically grant you any permission on any safe that you have access to. The Vault Admins group is a predefined group that is created during the installation or upgrade of the vault. This group has the Vault Admin authorization, which allows its members to perform administrative tasks on the vault, such as managing users, groups, platforms, policies, and safes1. However, this authorization does not include any safe member authorizations, such as View, Retrieve, Use, or Manage Safe2. Therefore, to grant any permission on a safe, you need to be added as a safe member with the appropriate authorizations, either directly or through another group. The Vault Admins group can be added to safes with all safe member authorizations, but this is not done automatically for all safes. By default, this group is only added to a number of system safes, such as the Password Manager Safe, the PVWAConfig Safe, and the Notification Methods Safe3. For other safes, the Vault Admins group can be added manually by the safe owner or another user with the Manage Safe authorization4. References:
? 1: Predefined users and groups, Predefined groups subsection
? 2: [CyberArk Privileged Access Security Implementation Guide], Chapter 3: Managing Safes, Section: Safe Authorizations, Table 2-1: Safe Authorizations
? 3: What default groups can be automatically added to Safes when they are created?
? 4: [CyberArk Privileged Access Security Administration Guide], Chapter 3: Managing Safes, Section: Adding Safe Members

NEW QUESTION 11
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%7C
2#Permissions

NEW QUESTION 14
To use PSM connections while in the PVWA, what are the minimum safe permissions a user or group will need?

A. List Accounts, Use Accounts
B. List Accounts, Use Accounts, Retrieve Accounts
C. Use Accounts
D. List Accounts, Use Accounts, Retrieve Accounts, Access Safe without confirmation

Answer: B

Explanation:
To use PSM connections within the PVWA, a user or group needs to have permissions that allow them to list and use accounts, as well as retrieve account details. These permissions ensure that the user can view the accounts within a safe, initiate sessions using those accounts, and retrieve the necessary credentials for authentication during the session initiation process1.
References:
? CyberArk's official documentation on Safe Settings and permissions required for each safe in CyberArk's Enterprise Password Vault (EPV) components provides detailed information on the default safe configuration and permissions1.
? For more information on best practices for safe and safe member design, including the minimum permissions required for PSM connections, refer to CyberArk's best practices articles and study guides

NEW QUESTION 16
Which usage can be added as a service account platform?

A. Kerberos Tokens
B. IIS Application Pools
C. PowerShell Libraries
D. Loosely Connected Devices

Answer: B

Explanation:
A service account platform is a type of platform that defines how CyberArk manages passwords for service accounts, which are accounts that run applications or services on remote machines. A usage is a configuration that allows CyberArk to manage passwords for files, such as XML or INI files, that are stored on remote machines. A usage is associated with a parent account, which is the account that has access to the file. A usage can be added as a service account platform if the file contains the password of a service account. For example, IIS Application Pools is a usage that can be added as a service account platform, because it manages the passwords of the application pools that run on IIS servers. The other options, Kerberos Tokens, PowerShell Libraries, and Loosely Connected Devices, are not usages that can be added as service account platforms, because they do not manage passwords for service accounts. References: Usages, Service Account Platforms

NEW QUESTION 18
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 23
Which of the following statements are NOT true when enabling PSM recording for a target Windows server? (Choose all that apply)

A. The PSM software must be instated on the target server
B. PSM must be enabled in the Master Policy (either directly, or through exception)
C. PSMConnect must be added as a local user on the target server
D. RDP must be enabled on the target server

Answer: AC

Explanation:
The following statements are not true when enabling PSM recording for a target Windows server:
? A. The PSM software must be instated on the target server. This is not true, because the PSM software is installed on a dedicated server that acts as a proxy between the user and the target server. The PSM server intercepts the user's connection request, initiates the connection to the target server, and records the privileged session. The target server does not need to have the PSM software installed on it1.
? C. PSMConnect must be added as a local user on the target server. This is not true, because PSMConnect is a predefined user that is created on the PSM server during the installation. This user is used to establish the connection between the PSM server and the target server, and to run the PSM processes. The target server does not need to have a local user named PSMConnect on it2.
The following statements are true when enabling PSM recording for a target Windows server:
? B. PSM must be enabled in the Master Policy (either directly, or through exception). This is true, because the Master Policy is a centralized overview of the security and compliance policy of privileged accounts in the organization. It allows the administrator to configure compliance driven rules that are defined as the baseline for the enterprise. One of the rules in the Master Policy is the Session Isolation rule, which determines whether or not privileged sessions are isolated and recorded by PSM. This rule can be enabled either directly in the Master Policy, or through an exception for a specific scope of accounts3.
? D. RDP must be enabled on the target server. This is true, because RDP is the protocol that is used by PSM to connect to Windows servers. The target server must have RDP enabled and configured properly to allow the PSM server to access it. The PSM server must also have the RDP client installed on it4.
References:
? 1: Privileged Session Manager
? 2: PSMConnect and PSMAdminConnect
? 3: Session Isolation
? 4: Configure RDP for PSM

NEW QUESTION 24
What is the primary purpose of Dual Control?

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

Answer: D

Explanation:
Dual control is a feature of CyberArk Defender PAM that enables authorized Safe owners to either grant or deny requests to access accounts. This feature adds an additional measure of protection, in that it enables you to see who wants to access the information in the Safe, when, and for what purpose. The Master Policy enables organizations to ensure that passwords can only be retrieved after permission or 'confirmation' has been granted from an authorized Safe Owner (s). This is known as Dual Control. The primary purpose of dual control is to prevent a single user from accessing a sensitive account without authorization, which could lead to fraud or misuse of privileges.
By requiring confirmation from another authorized user, dual control ensures that there is a 'collusion to commit' fraud, meaning that at least two users are involved in the malicious activity and are accountable for it. References:
? Dual Control - CyberArk
? Dual Control - CyberArk
? Dual control in V10 Interface - docs.cyberark.com

NEW QUESTION 27
Where can you assign a Reconcile account? (Choose two.)

A. in PVWA at the account level
B. in PVWA in the platform configuration
C. in the Master policy of the PVWA
D. at the Safe level
E. in the CPM settings

Answer: AB

Explanation:
A Reconcile account can be assigned in the Privileged Vault Web Access (PVWA) at both the account level and within the platform configuration. At the account level, a Reconcile account password can be defined which will override the account specified in the platform1. In the platform configuration, you can navigate to Platform Management, select the platform, edit it, and then expand Automatic Password Management to enter the values in the 'ReconcileAccountSafe' and 'ReconcileAccountName' fields, which will apply to all accounts attached to that specific platform2.
References:
? CyberArk Docs - Reconcile Password1
? CyberArk Community - Associate reconcile account with a specific platform

NEW QUESTION 28
Which statement about the Master Policy best describes the differences between one-time password and exclusive access functionality?

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

Answer: D

Explanation:
The Master Policy in CyberArk defines the behavior of one-time passwords and exclusive accessExclusive access ensures that only one user can check out an account at any given time, effectively locking the account during its use to prevent simultaneous access1. On the other hand, one-time password functionality is designed to change the account's password after it is used, based on a timer set by the MinValidityPeriod parameter in the policy file. This means that once the password is checked out and the timer expires, the Central Policy Manager (CPM) will change the password2. These settings are often used together to maintain accountability and security for the usage of shared privileged accounts. References:
? CyberArk Docs: One-time passwords and exclusive accounts1
? CyberArk Knowledge Article: CPM: What is the difference between “One Time” and “Exclusive” passwords?2

NEW QUESTION 32
What does the minvalidity parameter on a platform policy determine?

A. time between a password retrieval and the account becoming eligible for a password change
B. timeout for users signed into the PVWA as configured in the global settings
C. minimum amount of time that Just in Time access is valid
D. time in minutes before an empty safe will be automatically deleted

Answer: A

Explanation:
The minvalidity parameter on a platform policy in CyberArk determines the minimum amount of time that must pass between the retrieval of a password and when the account becomes eligible for a password change. This parameter ensures that a user has a guaranteed period to use the password before it is changed again, providing stability and predictability in password management1. References: The information provided is based on general knowledge of CyberArk PAM best practices and the functionality of the minvalidity parameter as outlined in CyberArk's official documentation

NEW QUESTION 33
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 36
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 37

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 39
It is possible to restrict the time of day, or day of week that a [b]verify[/b] process can occur

A. TRUE
B. FALSE

Answer: A

Explanation:
It is possible to restrict the time of day, or day of week that a verify process can occur by using the Verify Time Window parameter in thePlatform Management page. This parameter allows the administrator to define a time window for each platform, during which the verify process can be performed. The verify process will not run outside of this time window, unless it is manually initiated by the administrator. This feature can help reduce the load on the target systems and the network during peak hours. References:
? [Defender PAM Course], Module 4: Managing Accounts, Lesson 2: Account Verification, Slide 8: Verify Time Window
? [Defender PAM Documentation], Version 12.3, Administration Guide, Chapter 4: Managing Platforms, Section: Verify Time Window

NEW QUESTION 44
You need to recover an account localadmin02 for target server 10.0.123.73 stored in Safe Team1.
What do you need to recover and decrypt the object? (Choose three.)

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

Answer: ABC

Explanation:
To recover and decrypt an account that is stored in a Safe, you need the following items:
? Recovery Private Key: This is a key that is used to decrypt the data stored in the Vault. It is located on the Master CD, which is a physical CD that contains the Private Recovery Key, a file named RecPrv.key.
? Recover.exe: This is a utility that is used to recover information from a Safe’s external files in case of loss or corruption of that Safe. The files are decrypted and saved as readable files. The utility can be run from the command line or the graphical user interface.
? Vault data: This is the data that is stored in the Vault, such as accounts, safes, platforms, policies, users, groups, and audit records. The Vault data is encrypted using the Recovery Public Key, which is a key that is used to encrypt the data stored in the Vault. The Vault data can be recovered from the Vault server disk drive or from a backup file.
References: Recover, Server keys, Export Vault Information

NEW QUESTION 45
Which PTA sensors are required to detect suspected credential theft?

A. Logs, Vault Logs
B. Logs, Network Sensor, Vault Logs
C. Logs, PSM Logs, CPM Logs
D. Logs, Network Sensor, EPM

Answer: B

Explanation:
Suspected credential theft is a detection that PTA reports when a user connects to a machine or a cloud service without first retrieving the required credentials from the Vault. To detect this event, PTA requires the following sensors:
? Logs: This sensor collects log data from various sources, such as SIEM, Unix, AWS, and Azure, and forwards it to the PTA Server for analysis.
? Network Sensor: This sensor taps the network and collects network traffic data, which is used by the PTA Server to run deep packet inspection algorithms and detect cyber attacks, such as PAC, OverPass the Hash, and Golden Ticket.
? Vault Logs: This sensor collects log data from the Vault and forwards it to the PTA Server for analysis. The Vault logs contain information about the users’ activities in the Vault, such as password retrieval, session initiation, and audit records.
References: What Detections Does PTA Report?, PTA Network Sensors

NEW QUESTION 47
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 48
To ensure all sessions are being recorded, a CyberArk administrator goes to the master policy and makes configuration changes.
Which configuration is correct?

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

Answer: C

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

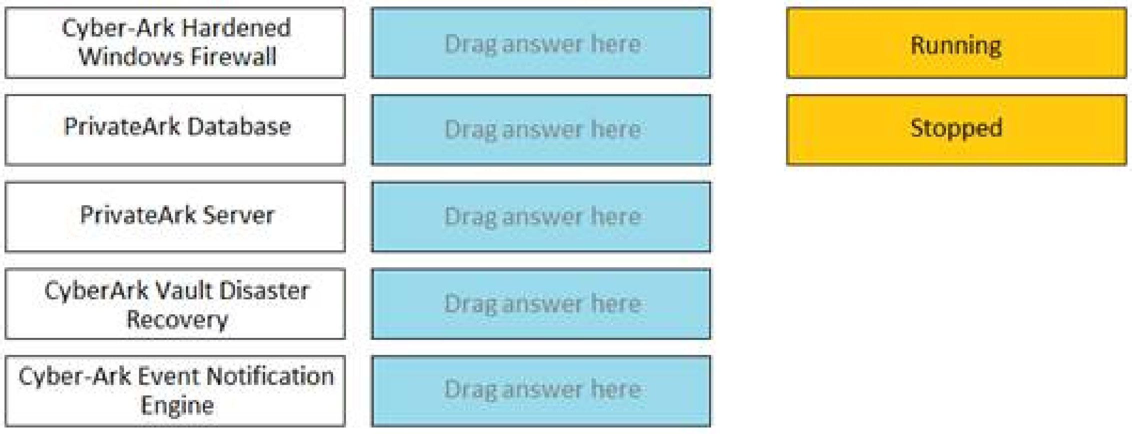
NEW QUESTION 50
How much disk space do you need on a server to run a full replication with PAReplicate?

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

Answer: D

Explanation:
When running a full replication with PAReplicate, it is essential to have at least the same amount of disk space on the server as the disk size of the Primary Vault. This ensures that there is sufficient space to replicate all the data from the Primary Vault without any issues. The disk space should be equal to or larger than the total size of the data being replicated to accommodate the full backup1.
References:
? CyberArk Docs: Install the Vault Backup Utility

NEW QUESTION 53
DRAG DROP
Match the Status of Service on a DR Vault to what is displayed when it is operating normally in Replication mode.



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

A. Mastered
B. Not Mastered

Answer: A

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

CyberArk Vault Disaster Recovery -> Running CyberArk Event Notification Engine -> Stopped
? Comprehensive Explanation: A DR Vault is a Vault that acts as a standby replica of the Primary Vault and is ready to take its place when the Primary Vault is unavailable. The DR Vault operates in Replication mode, which means it continuously replicates the data and metadata from the Primary Vault. In Replication mode, the following services have the following status on the DR Vault:
? Cyber-Ark Hardened Windows Firewall: This service provides firewall protection for the Vault server. It should be running on the DR Vault to ensure security.
? PrivateArk Database: This service manages the database that stores the metadata of the Vault. It should be stopped on the DR Vault, because the database is not active in Replication mode. The database is only activated when the DR Vault switches to Production mode.
? PrivateArk Server: This service manages the Vault server and its communication with other components. It should be stopped on the DR Vault, because the Vault server is not active in Replication mode. The Vault server is only activated when the DR Vault switches to Production mode.
? CyberArk Vault Disaster Recovery: This service manages the replication process between the Primary Vault and the DR Vault. It should be running on the DR Vault to ensure data synchronization and readiness for failover.
? Cyber-Ark Event Notification Engine: This service manages the event notifications and alerts for the Vault. It should be stopped on the DR Vault, because the event notifications are not relevant in Replication mode. The event notifications are only activated when the DR Vault switches to Production mode.
References: Primary-DR environment - CyberArk, Replicate the Primary Vault to the Satellite Vaults - CyberArk

NEW QUESTION 58
Due to network activity, ACME Corp's PrivateArk Server became active on the OR Vault while the Primary Vault was also running normally. All the components continued to point to the Primary Vault.
Which steps should you perform to restore DR replication to normal?

A. Replicate data from DR Vault to Primary Vault > Shutdown PrivateArk Server on DR Vault > Start replication on DR vault
B. Shutdown PrivateArk Server on DR Vault > Start replication on DR vault
C. Shutdown PrivateArk Server on Primary Vault > Replicate data from DR Vault to Primary Vault > Shutdown PrivateArk Server on DR Vault > Start replication on DR vault
D. Shutdown PrivateArk Server on DR Vault > Replicate data from DR Vault to Primary Vault > Shutdown PrivateArk Server on DR Vault > Start replication on DR vault

Answer: B

Explanation:
To restore DR replication to normal after network activity caused the PrivateArk Server on the DR Vault to become active while the Primary Vault was also running, you should first shut down the PrivateArk Server on the DR Vault. This ensures that the DR Vault is no longer active and can be prepared for replication. After shutting down the server, you should then start the replication process on the DR Vault to synchronize the data from the Primary Vault1.
References:
? CyberArk's official documentation on initiating a DR failback to the Production
Vault provides a detailed procedure for restoring DR replication to normal1.
? Additional information on monitoring backup and DR replications can be found in CyberArk's documentation2.
? For further study and understanding of the CyberArk Defender PAM course objectives and documents, the official CyberArk training resources and study guides are recommended3.

NEW QUESTION 60
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 62
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 63
A user needs to view recorded sessions through the PVWA.
Without giving auditor access, which safes does a user need access to view PSM recordings? (Choose two.)

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

Answer: AB

Explanation:
To view recorded sessions through the PVWA without having auditor access, a user needs access to two specific safes: the Recordings safe and thesafe the account is in. The Recordings safe is where the PSM session recordings are stored, and users need permission to access this safe to view the recordings. Additionally, users need access to the safe where the account associated with the recorded session is stored, as this is where the session details and permissions are managed12.
References:
? CyberArk Docs - Configure video and text recordings3
? CyberArk Community - Viewing PSM recorded sessions1

NEW QUESTION 65
When a group is granted the 'Authorize Account Requests' permission on a safe Dual Control requests must be approved by

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

Answer: C

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

NEW QUESTION 67
Which certificate type do you need to configure the vault for LDAP over SSL?

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

Answer: A

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

NEW QUESTION 70
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 74
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 79
If a user is a member of more than one group that has authorizations on a safe, by default that user is granted .

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

Answer: D

Explanation:
When a user is a member of more than one group that has authorizations on a safe, by default that user is granted the cumulative permissions of all groups to which that user belongs. This means that the user will have the highest level of access that any of the groups have on the safe. For example, if one group has View and Retrieve permissions, and another group has Add and Delete permissions, the user will have View, Retrieve, Add, and Delete permissions on the safe. This is the default behavior of the vault, unless the Exclusive option is enabled on the safe. The Exclusive option restricts the user's permissions to only those of the group added to the safe first. References:
? [Defender PAM eLearning Course], Module 3: Safes and Permissions, Lesson 3.2:
Safe Permissions, Slide 8: Cumulative Permissions
? [Defender PAM Sample Items Study Guide], Question 1: Safe Permissions
? [CyberArk Documentation Portal], CyberArk Privileged Access Security Implementation Guide, Chapter 3: Managing Safes, Section: Safe Properties, Subsection: Exclusive

NEW QUESTION 81
What is the name of the Platform parameters that controls how long a password will stay valid when One Time Passwords are enabled via the Master Policy?

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

Answer: A

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

NEW QUESTION 83
When on-boarding account using Accounts Feed, Which of the following is true?

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

Answer: B

Explanation:
When on-boarding accounts using Accounts Feed, you can either select an existing safe or create a new one to store the accounts. You can also specify the platform, policy, and owner for each account. However, you cannot create a new platform using Accounts Feed, and not all platforms support automatic reconciliation. References:
? Accounts Feed - CyberArk
? CyberArk University
? [Defender-PAM Sample Items Study Guide]

NEW QUESTION 84
A password compliance audit found:
1) One-time password access of 20 domain accounts that are members of Domain Admins group in Active Directory are not being enforced.
2) All the sessions of connecting to domain controllers are not being recorded by CyberArk PSM.
What should you do to address these findings?

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

Answer: A

Explanation:
To address the findings of the password compliance audit, you should edit the Master Policy in CyberArk Privileged Access Manager. The Master Policy is where you can enforce one-time password access and record session activity. One-time password access ensures that each password is used only once and then changed, which is a security measure to prevent unauthorized reuse of passwords1. Recording session activity is a feature of the Privileged Session Manager (PSM) that allows all activities during a session to be recorded for auditing purposes2. By enabling these settings in the Master Policy, you ensure that the domain accounts have one-time password access enforced and that all sessions connecting to domain controllers are recorded by CyberArk PSM. References:
? CyberArk Docs: One-time passwords and exclusive accounts1

NEW QUESTION 87
You have been asked to turn off the time access restrictions for a safe. Where is this setting found?

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

Answer: C

Explanation:
The setting to turn off the time access restrictions for a safe is found in the Password Vault Web Access (PVWA). The PVWA provides a web interface through which users can manage safes, including setting and modifying various safe properties such as access restrictions. By accessing the safe settings in the PVWA, you can adjust the time access restrictions as required1.
References:
? CyberArk Docs: Safe Settings1

NEW QUESTION 90
A Logon Account can be specified in the Master Policy.

A. TRUE
B. FALSE

Answer: B

Explanation:
A Logon Account cannot be specified in the Master Policy. The Master Policy is a set of rules that define the security and compliance policy of privileged accounts in the organization, such as access workflows, password management, session monitoring, and auditing1. The Master Policy does not include any technical settings that determine how the system manages accounts on various platforms1. A Logon Account is a technical setting that defines the account that the CPM uses to log on to a target system and perform password management tasks, such as changing, verifying, or reconciling passwords2. A Logon Account can be specified in the Platform Management settings, which are configured by the IT administrator for each platform2. The Platform Management settings are independent of the Master Policy and can be customized according to the organization’s environment and security policies1. References:
? The Master Policy
? [Platform Management]

NEW QUESTION 93
When running a “Privileged Accounts Inventory” Report through the Reports page in PVWA on a specific safe, which permission/s are required on that safe to show complete account inventory information?

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

Answer: A

Explanation:
The Privileged Accounts Inventory Report provides information about all the privileged accounts in the system, based on different filters, such as safe, platform, policy, and owner. To run this report through the Reports page in PVWA on a specific safe, the user needs to have the following permissions on that safe:
? List Accounts: This permission allows the user to view the accounts in the safe and their properties, such as name, address, platform, and policy.
? View Safe Members: This permission allows the user to view the members of the safe and their authorizations, such as owners, users, and groups.
These permissions are required to show complete account inventory information for the specific safe. Other permissions, such as Manage Safe Owners, Access Safe without confirmation, Manage Safe, and View Audit, are not relevant for this report. References: Reports and Audits - CyberArk, Safe Member Authorizations

NEW QUESTION 94
For a safe with Object Level Access enabled you can turn off Object Level Access Control when it no longer needed on the safe.

A. TRUE
B. FALSE

Answer: B

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

NEW QUESTION 95
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 96
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 100
What is the easiest way to duplicate an existing platform?

A. From PrivateArk, copy/paste the appropriate Policy.ini file; then rename it.
B. From the PVWA, navigate to the platforms page, select an existing platform that is similar to the new target account platform and then click Duplicate; name the new platform.
C. From PrivateArk, copy/paste the appropriate settings in PVConfiguration.xml; then update the policyName variable.
D. From the PVWA, navigate to the platforms page, select an existing platform that is similar to the new target account platform, manually update the platform settings and click "Save as" INSTEAD of save to duplicate and rename the platform.

Answer: B

Explanation:
The easiest way to duplicate an existing platform is to use the PVWA, which is the web interface that allows users to access and manage the CyberArk Defender PAM system. The PVWA has a platforms page that displays all the platforms that are available in the system, categorized by platform types. Users can duplicate an existing platform by selecting it, clicking the ellipsis button next to it, and then clicking Duplicate. This will create a copy of the platform with the same settings and properties, which can be customized according to the user's needs. Users can name the new platform and save it in the system.
References: Manage platforms - CyberArk

NEW QUESTION 104
The Active Directory User configured for Windows Discovery needs which permission(s) or membership?

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

Answer: D

Explanation:
The Active Directory User configured for Windows Discovery requiresRead Only Permissions. This level of permission allows the user to query and discover objects within the Active Directory without the ability to modify any objects or settings. Having read- only access is sufficient for discovery purposes, as it enables the user to retrieve necessary information without posing a risk of unintended changes to the directory1.
References:
? Microsoft Learn: Configure discovery methods1

NEW QUESTION 105
Which of the following files must be created or configured m order to run Password Upload Utility? Select all that apply.

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

Answer: ACD

Explanation:
To run the Password Upload Utility, you need to create or configure the following files:
? A comma delimited upload file: This is a text file that contains the passwords and
their properties that will be uploaded to the Vault. The file must have a .csv extension and follow a specific format. The first line in the file defines the names of the password properties as specified in the Password Vault. Every other line represents a single password object and its property values, according to the properties specified in the first line1.
? PACli.ini: This is a configuration file that stores the parameters for the PACli, which
is a command-line interface that enables communication between the Password Upload Utility and the Vault. The PACli.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: Vault, User, Password, and LogFile2.
? conf.ini: This is a configuration file that stores the parameters for the Password
Upload Utility. The conf.ini file must be located in the same folder as the Password Upload Utility executable file. The file must contain the following parameters: InputFile, LogFile, and ErrorFile3.
You do not need to create or configure the following file to run the Password Upload Utility:
? Vault.ini: This is a configuration file that stores the parameters for the Vault server, such as the database name, port, and password. This file is not used by the Password Upload Utility, and it is not located in the same folder as the Password Upload Utility executable file. The Vault.ini file is located in the Vault installation folder, and it is used by the Vault service and the PrivateArk Client4. References:
? 1: Create the Password File
? 2: PACli.ini
? 3: Password Upload Utility Parameter File (conf.ini)
? 4: [CyberArk Privileged Access Security Implementation Guide], Chapter 2: Installing the Vault, Section: Configuring the Vault, Subsection: Vault.ini

NEW QUESTION 106
You are configuring CyberArk to use HTML5 gateways exclusively for PSM connections. In the PVWA, where do you set DefaultConnectionMethod to HTML5?

A. Options > Privileged Session Management UI
B. Options > Privileged Session Management
C. Options > Privileged Session Management Defaults
D. Options > Privileged Session Management Interface

Answer: A

Explanation:
To configure CyberArk to use HTML5 gateways exclusively for PSM connections, you need to set the DefaultConnectionMethod to HTML5 in the PVWA. This is done by logging in to the PVWA with an administrative user, navigating to Options > Privileged Session Management UI, and setting the DefaultConnectionMethod to HTML51. This configuration ensures that HTML5 sessions are triggered only for PSM machines associated with the HTML5 Gateway1.
References:
? CyberArk Docs - Secure Access with an HTML5 Gateway1

NEW QUESTION 111
Ad-Hoc Access (formerly Secure Connect) provides the following features. Choose all that apply.

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

Answer: ABC

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

NEW QUESTION 115
Where can PTA be configured to send alerts? (Choose two.)

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

Answer: AB

Explanation:
CyberArk’s Privileged Threat Analytics (PTA) can be configured to send alerts to a Security Information and Event Management (SIEM) system and via Email. SIEM systems are used for real-time analysis of security alerts generated by applications and network hardware, while email alerts can be sent to individual or group email addresses for immediate notification1.
References:
? CyberArk Docs: Send PTA Alerts to Email1

NEW QUESTION 118
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 121
Which of the following are secure options for storing the contents of the Operator CD, while still allowing the contents to be accessible upon a planned Vault restart? (Choose three.)

A. Store the CD in a physical safe and mount the CD every time Vault maintenance is performed
B. Copy the entire contents of the CD to the system Safe on the Vault
C. Copy the entire contents of the CD to a folder on the Vault Server and secure it with NTFS permissions
D. Store the server key in a Hardware Security Module (HSM) and copy the rest the keys from the CD to a folder on the Vault Server and secure it with NTFS permissions

Answer: ABD

Explanation:
? A. Store the CD in a physical safe and mount the CD every time Vault maintenance is performed. This option ensures that the CD is kept in a secure location when not in use, and that the keys are available when needed. This is the default option suggested by CyberArk1.
? B. Copy the entire contents of the CD to the system Safe on the Vault. This option allows the Vault to access the keys from the system Safe, which is a special Safe that stores the Vault configuration files and keys. The system Safe is encrypted and protected by the Vault, and can only be accessed by authorized users2.
? D. Store the server key in a Hardware Security Module (HSM) and copy the rest the keys from the CD to a folder on the Vault Server and secure it with NTFS permissions. This option provides an additional layer of security for the server key, which is the most critical key for the Vault. An HSM is a physical device that stores and manages cryptographic keys in a tamper-resistant and isolated environment. The Vault can integrate with an HSM to store and retrieve the server key3. The rest of the keys can be stored in a folder on the Vault Server and secured with NTFS permissions, which restrict access to authorized users and groups.
The following option is not secure and should be avoided:
? C. Copy the entire contents of the CD to a folder on the Vault Server and secure it with NTFS permissions. This option exposes the keys to potential risks, such as unauthorized access, data corruption, or deletion. NTFS permissions are not sufficient to protect the keys from malicious or accidental actions. Moreover, this option does not comply with the CyberArk best practices, which recommend to store the keys on a removable media or an HSM

NEW QUESTION 126
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 130
When creating an onboarding rule, it will be executed upon .

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

Answer: C

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

NEW QUESTION 135
What is the primary purpose of One Time Passwords?

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

Answer: A

Explanation:
One Time Passwords (OTPs) are passwords that are valid for only one use or a limited time period. The primary purpose of OTPs is to reduce the risk of credential theft, which is a common attack vector for hackers and malicious insiders. By using OTPs, the exposure of the credentials is minimized, and the attacker cannot reuse the stolen password to access the target system. OTPs also enhance the security of the authentication process, as they add an extra layer of verification to the user’s identity. OTPs can be generated by various methods, such as SMS, email, hardware tokens, software tokens, etc1.
The other options are not the primary purpose of OTPs, because:
? B. More frequent password changes. This is not the primary purpose of OTPs, but a consequence of using them. OTPs require more frequent password changes, as they expire after one use or a limited time period. However, this is not the main goal of using OTPs, but rather a means to achieve the goal of reducing the risk of credential theft.
? C. Non-repudiation (individual accountability). This is not the primary purpose of
OTPs, but a benefit of using them. Non-repudiation means that the user cannot deny performing an action or accessing a resource, as there is sufficient evidence to prove their identity and activity. OTPs can help achieve non-repudiation, as they are unique and personal to each user, and can be traced back to the user’s device or account. However, this is not the main goal of using OTPs, but rather an advantage of using them.
? D. To force a ‘collusion to commit’ fraud ensuring no single actor may use a
password without authorization. This is not the primary purpose of OTPs, but a feature of using them. OTPs can help prevent unauthorized access to privileged accounts, as they require the user to have both the OTP and the regular password to access the target system. This means that no single actor can use the password without authorization, as they would need the cooperation of another actor who has the OTP. However, this is not the main goal of using OTPs, but rather a capability of using them.
References:
? 1: One-time password

NEW QUESTION 140
VAULT authorizations may be granted to .

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

Answer: AC

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

NEW QUESTION 143
According to the DEFAULT Web Options settings, which group grants access to the REPORTS page?

A. PVWAUsers
B. Vault Admins
C. Auditors
D. PVWAMonitor

Answer: C

Explanation:
According to the CyberArk Defender-PAM study guide, the REPORTS page is used to generate reports on various aspects of the CyberArk Privileged Access Management Solution, such as user activity, password usage, and compliance status. The default group that grants access to the REPORTS page is the Auditors group, which is a built-in group in the Vault that has the AuditUsers authorization. Members of the Auditors group can view and generate reports, but cannot modify them. References:
? CyberArk Defender-PAM study guide, page 17, section 3.2.1
? CyberArk Privileged Access Security Documentation, page 48, section 2.3.2.1

NEW QUESTION 145
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 149
In order to connect to a target device through PSM, the account credentials used for the connection must be stored in the vault?

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

Answer: B

Explanation:
In order to connect to a target device through PSM, the account credentials used for the connection do not necessarily have to be stored in the vault. The user can also enter credentials manually using Secure Connect, which is a feature that enables users to connect to target systems through PSM without storing the account credentials in the vault. Secure Connect allows users to provide their own credentials at the time of connection, and these credentials are not saved or managed by CyberArk. Secure Connect can be used with any connection component that supports PSM, such as RDP, SSH, WinSCP, etc. To use Secure Connect, the user needs to specify the target system address and the connection component ID in the URL, and then enter the credentials in the PSM login screen1.
The other options are not correct, because:
? A. True. This is not correct, because as explained above, the user can also enter credentials manually using Secure Connect.
? C. False. Because if credentials are not stored in the vault, the PSM will log into the target device as PSM Connect. This is not correct, because PSM Connect is a predefined user that is created on the PSM server during the installation. This user is used to establish the connection between the PSM server and the target server, and to run the PSM processes. The PSM Connect user is not used to log into the target device as the end user2.
? D. False. Because if credentials are not stored in the vault, the PSM will prompt for credentials. This is not correct, because this option is essentially the same as Secure Connect, which is the correct answer.
References:
? 1: Secure Connect
? 2: PSMConnect and PSMAdminConnect

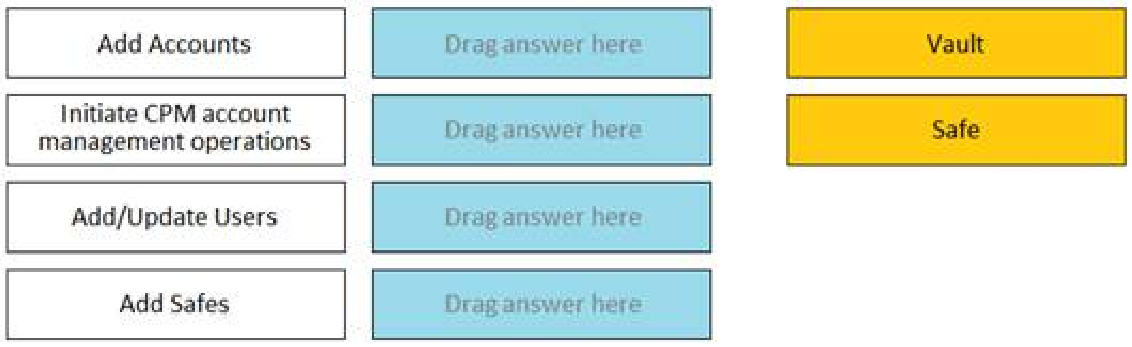
NEW QUESTION 154
Which of the following components can be used to create a tape backup of the Vault?

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

Answer: C

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

NEW QUESTION 158
DRAG DROP
Match each permission to where it can be found.



Add Accounts
Initiate CPM account management operations
Add/Update Users
Add Safes

Drag answer here
Drag answer here
Drag answer here
Drag answer here

Vault
Safe

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 163
You created a new safe and need to ensure the user group cannot see the password, but can connect through the PSM.
Which safe permissions must you grant to the group? (Choose two.)

A. List Accounts Most Voted
B. Use Accounts Most Voted
C. Access Safe without Confirmation
D. Retrieve Files
E. Confirm Request

Answer: BD

Explanation:
To ensure that a user group can connect through the Privileged Session Manager (PSM) without seeing the password, you must grant the Use Accounts and Retrieve Files permissions to the group for the safe. TheUse Accounts permission allows users to initiate sessions using accounts without viewing the account details or
passwords. TheRetrieve Files permission enables users to retrieve files during PSM sessions without having access to the passwords1.
References:
? CyberArk Docs - Safe Permissions

NEW QUESTION 168
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 170
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 172
What can you do to ensure each component server is operational?

A. Logon to PVWA with v10 UI, navigate to Healthcheck, and validate each component server is connected to the Vault.
B. Ping each component server to ensure connectivity.
C. Use the PrivateArk client to connect to the Vault server and validate all the services are running.

D. Install the Vault Server interface on a remote machine to avoid interactive logon to the Vault OS and review the ITALog.log through the Vault Server interface.

Answer: A

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

NEW QUESTION 175
Where can a user with the appropriate permissions generate a report? (Choose two.)

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

Answer: AB

Explanation:
A user with the appropriate permissions can generate a report in the PVWA (Privileged Vault Web Access) under theReports section1. Users who belong to the group specified in the ManageReportsGroup parameter in the Reports section of the Web Access Options in the System Configuration page are able to generate reports in the PVWA. By default, this group is the PVWAMonitor group1. Additionally, reports can be generated using the PrivateArk Client, which is a desktop application that provides a direct interface to manage the CyberArk Vault and its contents, including the generation of
reports2.
References:
? CyberArk Docs - Reports in PVWA1
? CyberArk Docs - Generate the Report2

NEW QUESTION 176
In addition to add accounts and update account contents, which additional permission on the safe is required to add a single account?

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

Answer: C

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

NEW QUESTION 177
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 180
Your organization requires all passwords be rotated every 90 days. Where can you set this regulatory requirement?

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

Answer: D

Explanation:

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

NEW QUESTION 181
Which CyberArk group does a user need to be part of to view recordings or live monitor sessions?

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

Answer: A

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

NEW QUESTION 186
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 190
The Accounts Feed contains:

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

Answer: B

Explanation:
The Accounts Feed is a feature of the CyberArk Privileged Access Security Solution that enables the discovery and provisioning of privileged accounts in the environment. The Accounts Feed contains the accounts that were discovered by CyberArk that have not yet been onboarded to the Vault. These accounts are displayed in the Pending Accounts page in the PVWA, where the user can view, analyze, and onboard them according to various criteria. The Accounts Feed helps the user to identify and manage the unmanaged privileged accounts that pose a security risk1.
The other options are not correct, because:
? A. Accounts that were discovered by CyberArk in the last 30 days. This is not correct, because the Accounts Feed does not contain all the accounts that were discovered by CyberArk in the last 30 days, but only the ones that have not yet been onboarded. The accounts that were already onboarded to the Vault are not part of the Accounts Feed, but are displayed in the Accounts page in the PVWA1.
? C. All accounts added to the vault in the last 30 days. This is not correct, because the Accounts Feed does not contain the accounts that were added to the Vault, but the ones that are waiting to be onboarded. The accounts that were added to the Vault are not part of the Accounts Feed, but are displayed in the Accounts page in the PVWA1.
? D. All users added to CyberArk in the last 30 days. This is not correct, because the Accounts Feed does not contain the users that were added to CyberArk, but the accounts that are waiting to be onboarded. The users that were added to CyberArk are not part of the Accounts Feed, but are displayed in the Users page in the PVWA1.
References:
? 1: Accounts Feed

NEW QUESTION 194
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 196
Select the best practice for storing the Master CD.

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

Answer: C

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

NEW QUESTION 199
Which change could CyberArk make to the REST API that could cause existing scripts to fail?

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

Answer: C

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

NEW QUESTION 203
In PVWA, you are attempting to play a recording made of a session by user jsmith, but there is no option to “Fast Forward” within the video. It plays and only allows you to skip between commands instead. You are also unable to download the video.
What could be the cause?

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

Answer: A

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

NEW QUESTION 207
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

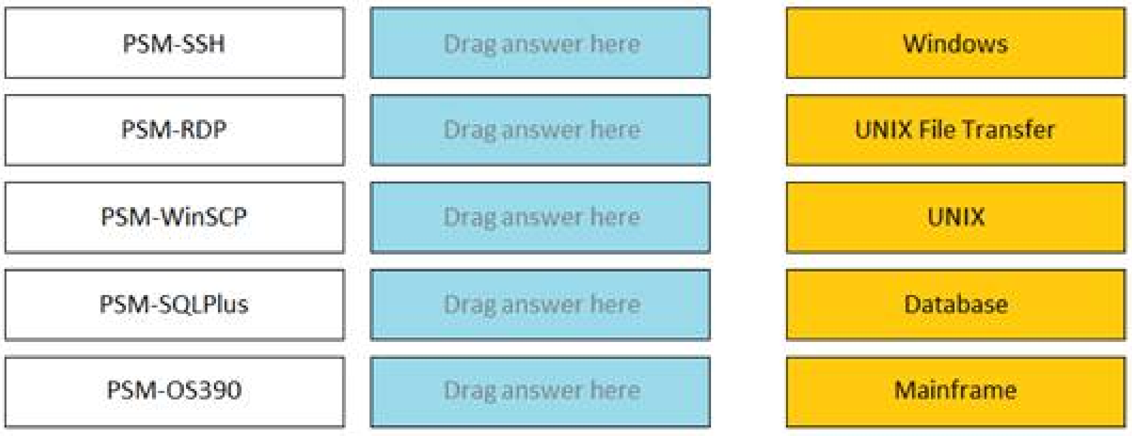
NEW QUESTION 209
tsparm.ini is the main configuration file for the Vault.

A. True
B. False

Answer: B

Explanation:
tsparm.ini isnot 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 mode. References:
? Defender PAM Sample Items Study Guide, page 9, question 92
? CyberArk Privileged Access Security Implementation Guide, page 75, section “DBParm.ini”
? CyberArk Vault Server Parameter Files, page 1, section “TSParm.ini”

NEW QUESTION 211
DRAG DROP
Match the connection component to the corresponding OS/Function.



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

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? A connection component is a set of parameters that defines how PSM connects to a target system using a specific protocol or application. Different connection components are suitable for different types of systems or functions. The correct matches are as follows:
? PSM-SSH: This connection component enables transparent connections to UNIX machines using the SSH protocol. It supports various UNIX flavors, such as Linux, Solaris, AIX, and HP-UX.
? PSM-RDP: This connection component enables transparent connections to Windows machines using the RDP protocol. It supports various Windows versions, such as Windows Server, Windows 10, and Windows 7.
? PSM-WinSCP: This connection component enables transparent connections to UNIX machines using the WinSCP application. It supports file transfer operations, such as upload, download, delete, and rename, between the local and remote machines.
? PSM-SQLPlus: This connection component enables transparent connections to Oracle databases using the SQL*Plus application. It supports various Oracle versions, such as Oracle 12c, Oracle 11g, and Oracle 10g.
? PSM-OS390: This connection component enables transparent connections to IBM mainframes using the OS/390 protocol. It supports various mainframe applications, such as TSO, CICS, and IMS.
References: Connection Components, Connection Component Parameters

NEW QUESTION 212
Users 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:
Users 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 is a special permission that allows a user to bypass the Dual control mechanism and access the accounts in the safe without requiring confirmation from other authorized users. This permission can be useful for emergency situations or trusted users who need immediate access to the accounts. However, this permission also increases the risk of unauthorized or malicious access, so it should be granted with caution and monitored closely1.
References:
? 1: Access without confirmation

NEW QUESTION 217

You created a new platform by duplicating the out-of-box Linux through the SSH platform.
Without any change, which Text Recorder Type(s) will the new platform support? (Choose two.)

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

Answer: AB

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

NEW QUESTION 220
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 225
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 226
When managing SSH keys, the CPM stored the Private Key

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

Answer: A

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

NEW QUESTION 228
You are troubleshooting a PVWA slow response. Which log files should you analyze first? (Choose two.)

A. ITALog.log
B. web.config

C. CyberArk.WebApplication.log
D. CyberArk.WebConsole.log

Answer: CD

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

NEW QUESTION 230
If the AccountUploader Utility is used to create accounts with SSH keys, which parameter do you use to set the full or relative path of the SSH private key file that will be attached to the account?

A. KeyPath
B. KeyFile
C. ObjectName
D. Address

Answer: B

Explanation:
When using the AccountUploader Utility to create accounts with SSH keys, the parameter used to set the full or relative path of the SSH private key file that will be attached to the account is KeyFile. This parameter specifies the location of the SSH private key file, which is then associated with the account being onboarded into the CyberArk Privileged Access Security system. The correct configuration of this parameter is crucial for the successful attachment of the SSH key to the account1.
References:
? CyberArk's official documentation on the AccountUploader Utility, which provides detailed information on the parameters and usage for onboarding accounts with SSH keys1.

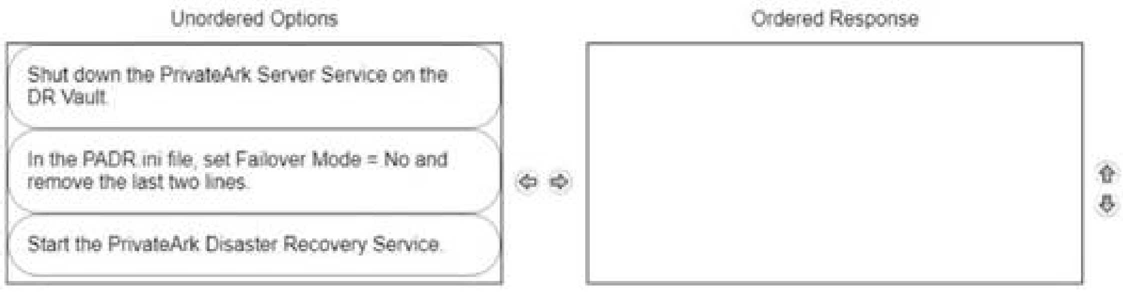
NEW QUESTION 234
Which built-in report from the reports page in PVWA displays the number of days until a password is due to expire?

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 237
DRAG DROP
ADR Vault became active due to a failure of the primary Vault. Service on the primary Vault has now been restored. Arrange the steps to return the DR vault to its normal standby mode in the correct sequence.



Unordered Options

Shut down the PrivateArk Server Service on the DR Vault.

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

Start the PrivateArk Disaster Recovery Service.

Ordered Response

A. Mastered
B. Not Mastered

Answer: A

Explanation:
? Shut down the PrivateArk Server Service on the DR Vault.
? In the PADR.ini file, set Failover Mode = No and remove the last two lines.
? Start the PrivateArk Disaster Recovery Service.
Comprehensive Explanation: When the primary Vault service has been restored and you need to return the DR Vault to its normal standby mode, the steps are as follows:
? Shut down the PrivateArk Server Service on the DR Vault to stop the Vault from being active.
? Modify the PADR.ini file by setting Failover Mode to No and removing the last two lines that were added during the failover process. This reconfigures the DR Vault to standby mode.
? Start the PrivateArk Disaster Recovery Service to complete the transition back to standby mode1.

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

NEW QUESTION 238
Which utilities could you use to change debugging levels on the vault without having to restart the vault. Select all that apply.

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

Answer: AB

Explanation:
To change debugging levels on the vault without having to restart the vault, you can use the following utilities:
? PAR Agent: This is a utility that runs on the vault server and allows you to change the debug level of the vault by editing the PARAgent.ini file. You can set the EnableTrace parameter to yes and specify the debug level in the DebugLevel parameter. The changes will take effect immediately without restarting the vault. The log file is located in the PARAgent.log file1.
? PrivateArk Server Central Administration: This is a graphical user interface that runs on the vault server and allows you to change the debug level of the vault by selecting the vault server and clicking the Debug button. You can choose the debug level from a list of predefined options or enter a custom value. The changes will take effect immediately without restarting the vault. The log files are located in the Trace.dX files, where X is a number from 0 to 42.
You cannot use the following utilities to change debugging levels on the vault without having to restart the vault:
? Edit DBParm.ini in a text editor: This is a configuration file that stores the vault parameters, such as the database name, port, and password. Editing this file does not affect the debug level of the vault, and requires restarting the vault for the changes to take effect3.
? Setup.exe: This is an installation program that runs on the vault server and allows you to install, upgrade, or uninstall the vault. It does not allow you to change the debug level of the vault, and requires restarting the vault for any changes to take effect4. References:
? 1: Configure Debug Levels, Vault section, PARAgent subsection
? 2: Configure Debug Levels, Vault section, PrivateArk Server Central Administration subsection
? 3: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault, Section: Configuring the Vault, Subsection: DBParm.ini
? 4: CyberArk Privileged Access Security Implementation Guide, Chapter 2: Installing the Vault, Section: Installing the Vault

NEW QUESTION 241
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 245
When should vault keys be rotated?

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

Answer: D

Explanation:
Vault keys should be rotated when there is a significant event that could potentially compromise the security of the keys, such as when migrating to a new data center. This is because the keys may be exposed to new environments and systems, and rotating them ensures that any potential exposure does not result in a security breach. Additionally, periodic rotation of encryption keys is recommended to maintain the integrity of the encryption and to adhere to best practices for security1. References:
? CyberArk Docs: Credentials Rotation Policy2
? HashiCorp Developer: Key Rotation

NEW QUESTION 248
What is the purpose of the PrivateArk Server service?

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

Answer: C

Explanation:
The purpose of the PrivateArk Server service is to make Vault data accessible to components, such as the PVWA, the CPM, the PSM, and the PTA, and handle

the requests from the clients and components. The PrivateArk Server service is a Windows service that runs the Vault and communicates with the PrivateArk Database service, which maintains the Vault metadata. The PrivateArk Server service can start automatically or manually depending on the Server's key configuration. The PrivateArk Server service can also be run in "console" mode for troubleshooting purposes1.
The other options are not the purpose of the PrivateArk Server service, although they may be related to other services or components of the Vault. The Central Policy Manager component is the component that executes password changes, verifications, and reconciliations for the accounts that are managed by the Vault. The Event Notification Engine service is the service that sends email alerts from the Vault, based on predefined events and recipients. The PrivateArk Client is a utility that allows the Vault administrator to access and manage the Vault data, users, groups, policies, and settings. References:
? Server Components - CyberArk, section "The PrivateArk Server process (Dbmain)"

NEW QUESTION 250
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 254
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 258
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 262
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 266
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 271
Which type of automatic remediation can be performed by the PTA in case of a suspected credential theft security event?

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

Answer: A

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

NEW QUESTION 275
You received a notification from one of your CyberArk auditors that they are missing Vault level audit permissions. You confirmed that all auditors are missing the Audit Users Vault permission.
Where do you update this permission for all auditors?

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

Answer: B

Explanation:
To update the Vault level audit permissions for all auditors, you would use the Private Ark Client. Specifically, you would navigate to the Tools menu, select Administrative Tools, then Users and Groups. Within the Users and Groups section, you would select the Auditors group and go to theAuthorizations tab. Here, you can manage and update the permissions for the Auditor group, including the Audit Users Vault permission. This ensures that all members of the Auditors group have the necessary permissions to perform their audit functions within the Vault1.
References:
? CyberArk’s official documentation on predefined users and groups, which includes information on the Auditor user and the permissions associated with this role1.
? Information on the administrative tools available in the Private Ark Client, which are used for managing users and groups, including auditors2.

NEW QUESTION 280
......