CyberArk

Exam Questions PAM-DEF

CyberArk Defender - PAM

NEW QUESTION 1
Which accounts can be selected for use in the Windows discovery process? (Choose two.)

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

Answer: AB

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

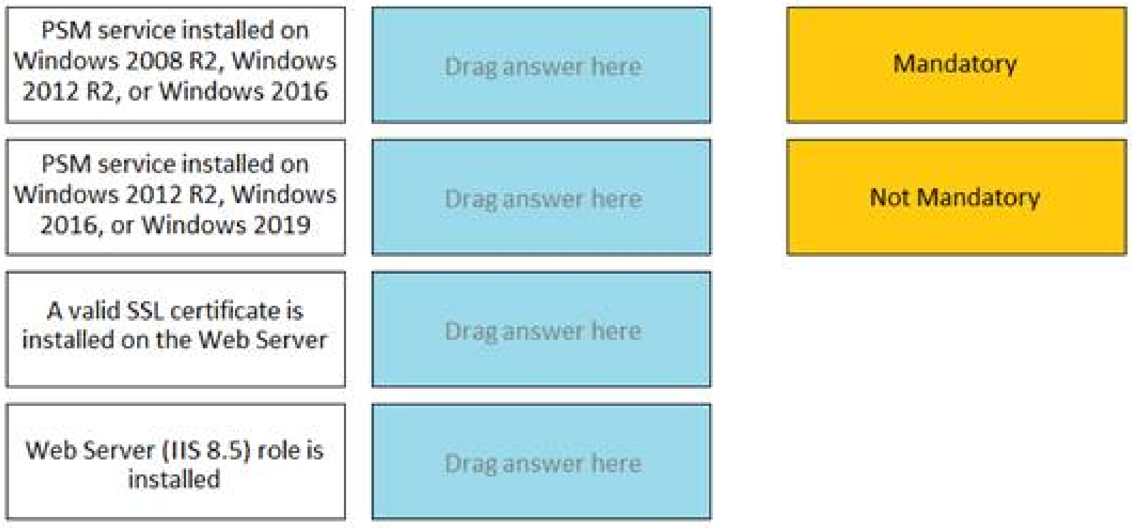
NEW QUESTION 2
Which of the following Privileged Session Management (PSM) solutions support live monitoring of active sessions?

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

Answer: D

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

NEW QUESTION 3
DRAG DROP
For each listed prerequisite, identify if it is mandatory or not mandatory to run the PSM Health Check.

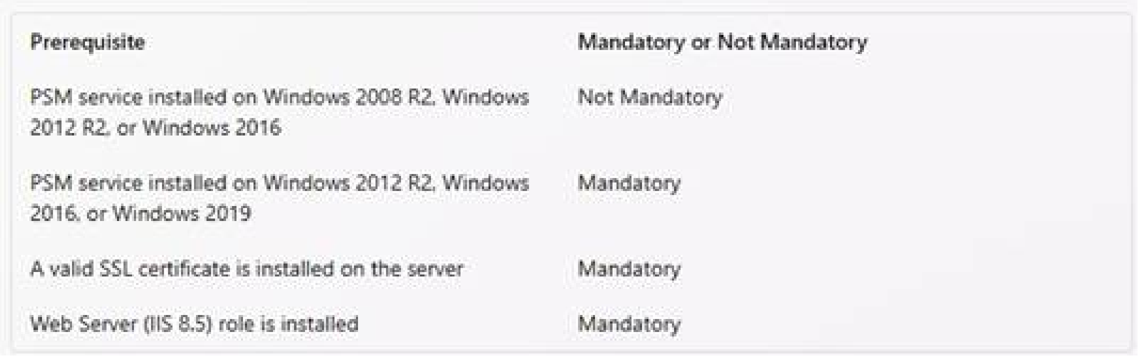


PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016	Drag answer here	Mandatory
PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019	Drag answer here	Not Mandatory
A valid SSL certificate is installed on the Web Server	Drag answer here	
Web Server (IIS 8.5) role 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 4
The vault supports Role Based Access Control.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 5
All of your Unix root passwords are stored in the safe UnixRoot. Dual control is enabled for some of the accounts in that safe. The members of the AD group UnixAdmins need to be able to use the show, copy, and connect buttons on those passwords at any time without confirmation. The members of the AD group Operations Staff need to be able to use the show, copy and connect buttons on those passwords on an emergency basis, but only with the approval of a member of Operations Managers never need to be able to use the show, copy or connect buttons themselves.
Which safe permission do you need to grant Operations Staff? Check all that apply.

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

Answer: AB

Explanation:
To use the show, copy, and connect buttons on the accounts in the safe UnixRoot, the Operations Staff need to have the Use Accounts permission, which allows them to request access to the accounts and perform actions on them. However, since dual control is enabled for some of the accounts, they also need to have the Retrieve Accounts permission, which allows them to view the password of the account after it is authorized by another user. The Authorize Password Requests permission is not needed, as it is only required for the users who can approve the requests, not the ones who make them. The Access Safe without Authorization permission is not needed, as it would bypass the dual control mechanism and allow the Operations Staff to access the accounts without approval. References:
? [Defender PAM Sample Items Study Guide], page 10, question 5
? [CyberArk Privileged Access Security Implementation Guide], page 30, table 2-1
? [CyberArk Privileged Access Security Administration Guide], page 43, section 3.2.2.1

NEW QUESTION 6
When the CPM connects to a database, which interface is most commonly used?

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

Answer: B

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

NEW QUESTION 7
What is the purpose of a linked account?

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

Answer: D

Explanation:
A linked account is an account that is associated with another account to enable the password management process. A linked account can be used for various purposes, such as logging on to a target system, changing the password of another account, or enabling privileged commands. A linked account can be defined either on the platform level or on the account level, depending on the type and scope of the linked account. The types of linked accounts that are supported by CyberArk are1:
? Logon account: An account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the CPM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the CPM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account.
? Reconcile account: An account that contains the password used in reconciliation processes. Reconciliation is a process that restores the password of a privileged account to the value that is stored in the Vault, in case it is changed or out of sync. A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the target account, the CPM can use the reconcile account to

restore the password of the target account, in case it is changed or out of sync.
? Other additional accounts: Additional accounts can be used in various cases. For example:
The other options are not the purpose of a linked account, because:
? A. To ensure that a particular collection of accounts all have the same password.
This is not the purpose of a linked account, but of a group account. A group account is an account that is associated with multiple target systems that share the same credentials. A group account allows the CPM to manage the password of multiple systems with a single password object in the Vault2.
? B. To ensure a particular set of accounts all change at the same time. This is not the purpose of a linked account, but of a password change schedule. A password change schedule is a feature that allows the administrator to define a time frame for changing the passwords of a set of accounts. A password change schedule can be configured either in the Master Policy or in the Platform settings3.
? C. To connect the CPNI to a target system. This is not the purpose of a linked account, but of a service account. A service account is an account that is used by a service or an application to connect to a target system. A service account can be managed by the Central Credential Provider (CCP), which is a component that provides applications and services with the credentials they need to access target systems4.
References:
? 1: Linked Accounts
? 2: Group Accounts
? 3: Password Change Schedule
? 4: Service Accounts

NEW QUESTION 8
A user is receiving the error message “ITATS006E Station is suspended for User jsmith” when attempting to sign into the Password Vault Web Access (PVWA). Which utility would a Vault administrator use to correct this problem?

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

Answer: C

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

NEW QUESTION 9
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
In a rule using “Privileged Session Analysis and Response” in PTA, which session options are available to configure as responses to activities?

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

Answer: A

Explanation:
https://docs.cyberark.com/Product- Doc/OnlineHelp/PAS/Latest/en/Content/PTA/Security- Configuration.htm?TocPath=End%20User%7CSecurity%20Events%7C3
These are the session response options that can be configured in a rule using Privileged Session Analysis and Response in PTA. These options determine how PTA reacts to suspicious activities detected in a privileged session. Suspend means that the session is paused and the user is notified. Terminate means that the session is ended and the user is disconnected. None means that no action is taken on the session, but the event is still recorded and reported. You can find more information about these options and how to configure them in the reference below.
Reference:
Configure security events

NEW QUESTION 10
A logon account can be specified in the platform settings.

A. True
B. False

Answer: A

Explanation:
A logon account can be specified in the platform settings of CyberArk, a security software that manages privileged accounts and credentials. According to the CyberArk documentation1, "In the Account Details window, in the CPM pane, in the accounts section, you can associate either a logon account or a reconciliation account. If a default logon account has been configured for the platform that manages this account, that account is listed. You can associate another logon account or leave the default account as it is."1 A logon account is an account that is used to log on to a target system and perform password management operations on other accounts. A reconciliation account is an account that is used to restore access to a target system when the logon account fails.

NEW QUESTION 12
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 17
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 19
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 22
When are external vault users and groups synchronized by default?

A. They are synchronized once every 24 hours between 1 AM and 5 A
B. Most Voted

C. They are synchronized once every 24 hours between 7 PM and 12 AM.
D. They are synchronized every 2 hours.
E. They are not synchronized according to a specific schedule.

Answer: A

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

NEW QUESTION 25
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 29
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 34
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 35
You are onboarding 5,000 UNIX root accounts for rotation by the CPM. You discover that the CPM is unable to log in directly with the root account and will need to use a secondary account.
How should this be configured to allow for password management using least privilege?

A. Configure each CPM to use the correct logon account.
B. Configure each CPM to use the correct reconcile account.
C. Configure the UNIX platform to use the correct logon account.
D. Configure the UNIX platform to use the correct reconcile account.

Answer: C

Explanation:
When onboarding a large number of UNIX root accounts for password rotation by the Central Policy Manager (CPM), and the CPM cannot log in directly with the root account, it is necessary to configure the UNIX platform to use a secondary logon account that has the appropriate privileges. This secondary account should have the minimum necessary permissions to perform password management tasks, adhering to the principle of least privilege1. By configuring the UNIX platform with the correct logon account, the CPM can use this account to manage the root accounts securely and efficiently.
References:
? CyberArk's official documentation on Least Privileges and Privileged Access Manager provides guidance on configuring on-demand privileges for UNIX environments, which includes setting up the correct logon account for tasks that require elevated privileges1.
? Additional information on managing UNIX and Linux accounts, including the configuration of logon and reconcile accounts, can be found in the Unix plugin documentation for CyberArk

NEW QUESTION 36
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 38
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 39
Which master policy settings ensure non-repudiation?

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

Answer: B

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

NEW QUESTION 42
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.

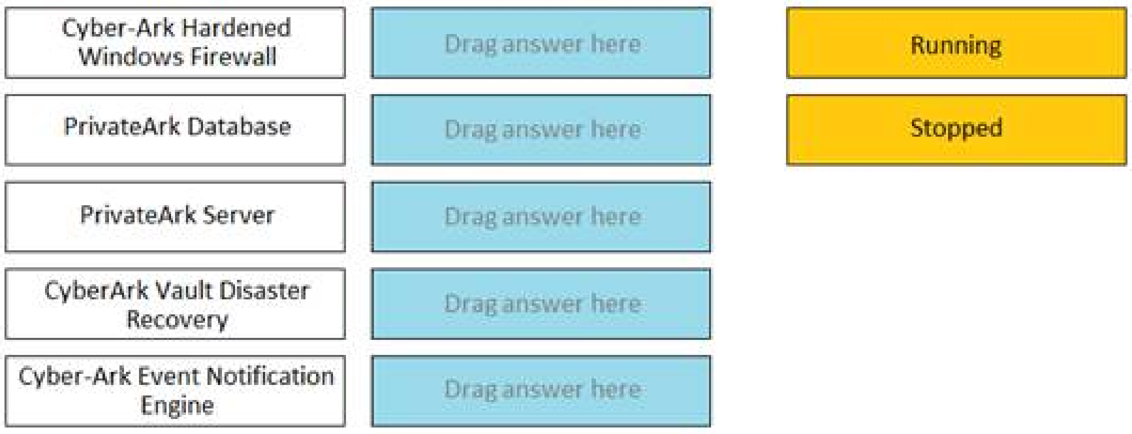
NEW QUESTION 47
If a password is changed manually on a server, bypassing the CPM, how would you configure the account so that the CPM could resume management automatically?

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

Answer: B

Explanation:
A reconcile account is a privileged account that has the permission to reset the password of another account on the target system. By associating a reconcile account with the account that has been changed manually, the CPM can use the reconcile account to restore the password of the account to the value that is stored in the Vault, in case it is changed or out of sync. This process is called password reconciliation and it ensures that the passwords are synchronized and available for use. To configure the account so that the CPM can resume management automatically, the platform that the account belongs to must have the following parameters set1:
? RCAutomaticReconcileWhenUnsynched: This parameter determines whether passwords will be reconciled automatically after the CPM detects a password on a remote machine that is not synchronized with its corresponding password in the Vault. The acceptable values are Yes or No.
? RCReconcileReasons: This parameter determines the codes that represent the CPM plugin errors that will launch a reconciliation process. The acceptable values are plug-in return codes separated by a comma.
? RCFromHour, RCToHour: These parameters determine the time frame in hours during which the CPM can reconcile passwords, either manually or automatically. The acceptable values are 0-23 or -1 for none.
? RCExecutionDays: This parameter determines the days of the week when the CPM will reconcile passwords. The acceptable values are days of the week, separated by commas.
References:
? 1: Password Reconciliation

NEW QUESTION 48
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
PrivateArk Database | Drag answer here
PrivateArk Server | Drag answer here
CyberArk Vault Disaster Recovery | Drag answer here
Cyber-Ark Event Notification Engine | Drag answer here

Running
Stopped

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 49
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 53
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 57
What are the minimum permissions to add multiple accounts from a file when using PVWA bulk-upload? (Choose three.)

A. add accounts
B. rename accounts
C. update account content
D. update account properties
E. view safe members
F. add safes

Answer: ACD

Explanation:
When using PVWA bulk-upload to add multiple accounts from a file, the minimum permissions required are to add accounts, update account content, and update account properties. These permissions ensure that the user has the ability to create new accounts in the Vault, modify the content of the accounts, and change their properties as necessary during the bulk-upload process1.
References:
? CyberArk Docs - Add multiple accounts from a file in V10 Interface

NEW QUESTION 58
How does the Vault administrator apply a new license file?

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

Answer: C

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

NEW QUESTION 59
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 63
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 68
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 69
Which of the following properties are mandatory when adding accounts from a file? (Choose three.)

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

Answer: ABC

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

NEW QUESTION 72
You have been asked to create an account group and assign three accounts which belong to a cluster. When you try to create a new group, you receive an unauthorized error; however, you are able to edit other aspects of the account properties.
Which safe permission do you need to manage account groups?

A. create folders
B. specify next account content
C. rename accounts
D. manage safe

Answer: D

Explanation:
To manage account groups, you need the manage safe permission, which allows you to create, update, and delete account groups in a safe. The other permissions are not related to account groups. The create folders permission allows you to create folders in a safe. The specify next account content permission allows you to specify the next password or SSH key for an account. The rename accounts permission allows you to rename accounts in a safe. References: Manage account groups, Safe member permissions

NEW QUESTION 76
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 78
An auditor initiates a live monitoring session to PSM server to view an ongoing live session. When the auditor’s machine makes an RDP connection the PSM server, which user will be used?

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

Answer: A

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

NEW QUESTION 81
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 82
Vault admins must manually add the auditors’ group to newly created safes so auditors will have sufficient access to run reports.

A. TRUE
B. FALSE

Answer: B

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

NEW QUESTION 86
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 91
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 92
PSM captures a record of each command that was executed in Unix.

A. TRIE
B. FALSE

Answer: A

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

NEW QUESTION 93
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 98
What is the configuration file used by the CPM scanner when scanning UNIX/Linux devices?

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

Answer: A

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

NEW QUESTION 102
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 106
For an account attached to a platform that requires Dual Control based on a Master Policy exception, how would you configure a group of users to access a password without approval.

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

Answer: D

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

NEW QUESTION 108
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 109
The vault supports Subnet Based Access Control.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 113
Where can you check that the LDAP binding is using TCP/636?

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

Answer: D

Explanation:
To check that the LDAP binding is using TCP/636, you can use the Test- NetConnection cmdlet from the PVWA to connect to the domain controller on Port 636. This method allows you to verify that the LDAP service is listening on the secure port and that the connection can be established using SSL/TLS, which is typically associated with port 6361.
References:
? CyberArk Docs - LDAP Integration2
? CyberArk Knowledge Article - How to test outgoing LDAP external directory connectivity to the vault

NEW QUESTION 116
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 118
Which parameter controls how often the CPM looks for Soon-to-be-expired Passwords that need to be changed.

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

Answer: A

NEW QUESTION 121
Can the 'Connect' button be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied?

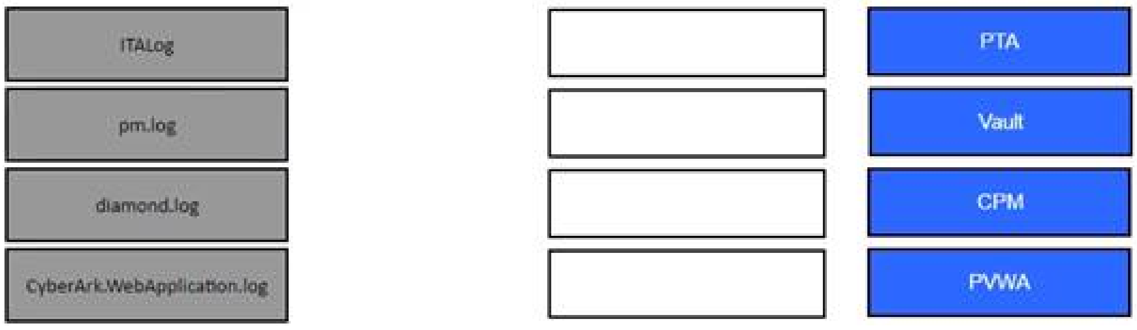
A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction.
B. Yes, only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component.
C. Yes, if a logon account is associated with the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

Answer: B

Explanation:
The ‘Connect’ button is a feature of the PVWA that allows users to initiate a privileged session to a target system through PSM without revealing the account credentials. The ‘Connect’ button can be used to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, but only if a logon account is associated with the root account and the user connects through the PSM-SSH connection component. A logon account is a linked account that contains the password required to log on to a remote machine in order to perform a task using the regular account. A common use case for using a logon account is managing root accounts on a Unix system. The best practice for Unix systems is to disallow the root user from logging in using SSH. However, SSH is what the PSM uses to sign in to a system to manage the password. To manage the root password without violating this practice, the PSM establishes the session with a non-root account and then SUs to root (the target account). This is done using a linked account called a logon account. The PSM-SSH connection component is a predefined connection component that enables users to connect to Unix systems through PSM using SSH. The PSM-SSH connection component supports the use of logon accounts to access root accounts on Unix systems1.

The other options are not correct, because:
? A. Yes, when using the connect button, CyberArk uses the PMTerminal.exe process which bypasses the root SSH restriction. This is not correct, because PMTerminal.exe is a process that is used by the PSM-RDP connection component, not the PSM-SSH connection component. PMTerminal.exe is a terminal emulator that enables users to connect to Windows systems through PSM using RDP. PMTerminal.exe does not bypass the root SSH restriction, but rather uses the credentials stored in the Vault to authenticate to the target system2.
? C. Yes, if a logon account is associated with the root account. This is not correct, because a logon account alone is not sufficient to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied. The user also needs to connect through the PSM-SSH connection component, which supports the use of logon accounts to access root accounts on Unix systems1.
? D. No, it is not possible. This is not correct, because it is possible to initiate an SSH connection, as root, to a Unix system when SSH access for root is denied, as explained in option B.
References:
? 1: Logon Accounts for SSH and Telnet Connections
? 2: Connect through PSM for SSH

NEW QUESTION 123
DRAG DROP
Match the log file name with the CyberArk Component that generates the log.



ITALog
pm.log
diamond.log
CyberArk.WebApplication.log

PTA
Vault
CPM
PVWA

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 124
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 125
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 128
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 131
You are creating a Dual Control workflow for a team's safe. Which safe permissions must you grant to the Approvers group?

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

Answer: C

Explanation:
When setting up a Dual Control workflow for a team's safe in CyberArk's Privileged Access Management (PAM), the Approvers group must be granted specific permissions to function effectively within the workflow. The permissions required for the Approvers group are to 'Retrieve accounts' and 'Authorize account request'. This allows the Approvers to retrieve the necessary account details and also to authorize requests for access as part of the dual control mechanism. These permissions ensure that the workflow operates smoothly and securely, with the Approvers having the ability to review and approve access requests as needed.
References: The answer is derived from the best practices and guidelines provided in the CyberArk Defender PAM course and learning resources, which include the official CyberArk documentation and study guides. Specifically, the CyberArk documentation outlines the importance of the 'Retrieve accounts' and 'Authorize account request' permissions for Approvers in a Dual Control workflow

NEW QUESTION 134
A newly created platform allows users to access a Linux endpoint. When users click to connect, nothing happens.
Which piece of the platform is missing?

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

Answer: A

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

NEW QUESTION 136
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 139
Via Password Vault Web Access (PVWA), a user initiates a PSM connection to the target Linux machine using RemoteApp. When the client's machine makes an RDP connection to the PSM server, which user will be utilized?

A. Credentials stored in the Vault for the target machine
B. Shadowuser

C. PSMConnect
D. PSMAdminConnect

Answer: C

Explanation:
According to the CyberArk Defender PAM documentation1, when a user initiates a PSM connection to the target Linux machine using RemoteApp via PVWA, the client's machine makes an RDP connection to the PSM server using the PSMConnect user. The PSMConnect user is a local or domain user that starts PSM sessions on the PSM machine. The PSMConnect user has limited permissions and access rights on the PSM server, and its credentials are managed by the CPM. The PSMConnect user retrieves the credentials of the target account from the vault and uses them to establish a secure connection to the target machine. The user can then interact with the target machine through the PSM session, while the PSM server records and audits the session activity.

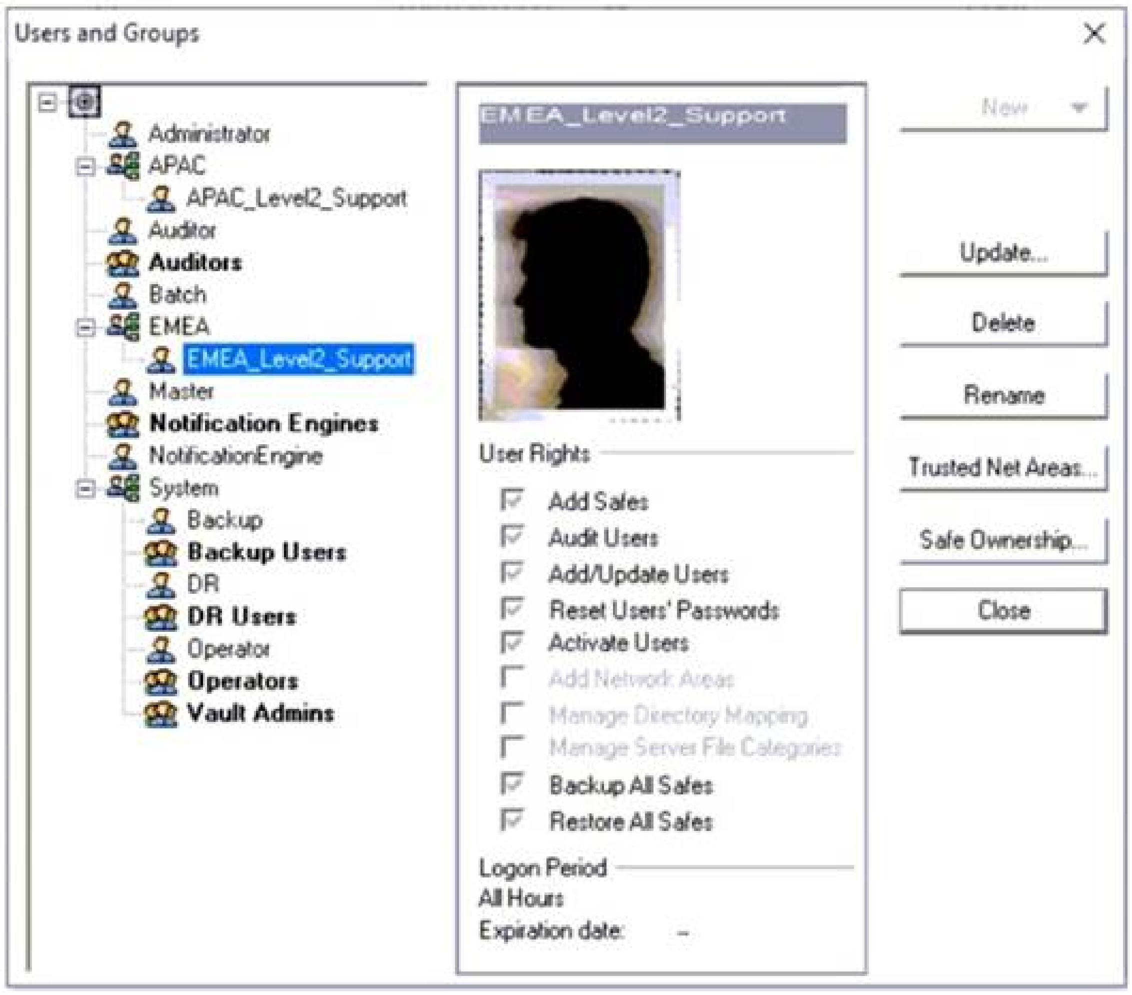
NEW QUESTION 140
What is the purpose of the CyberArk Event Notification Engine service?

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

Answer: B

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

NEW QUESTION 145
Refer to the exhibit.


Users and Groups

- Administrator
- APAC
  - APAC_Level2_Support
- Auditor
- **Auditors**
- Batch
- EMEA
  - EMEA_Level2_Support
- Master
- **Notification Engines**
- NotificationEngine
- System
  - Backup
  - **Backup Users**
  - DR
  - **DR Users**
  - Operator
  - **Operators**
  - **Vault Admins**

EMEA_Level2_Support

User Rights
☑ Add Safes
☑ Audit Users
☑ Add/Update Users
☑ Reset Users' Passwords
☑ Activate Users
☐ Add Network Areas
☐ Manage Directory Mapping
☐ Manage Server File Categories
☑ Backup All Safes
☑ Restore All Safes

Logon Period
All Hours
Expiration date: –

Why is user "EMEALevel2Support" unable to change the password for user "Operator"?

A. EMEALevel2Support's hierarchy level is not the same or higher than Operator.
B. EMEALevel2Support does not have the "Manage Directory Mapping" role.
C. Operator can only be reset by the Master user.
D. EMEALevel2Support does not have rights to reset passwords for other users.

Answer: D

Explanation:
The image description indicates that "EMEALevel2Support" has the following rights: Add/Update Users, Manage Server File Categories, Manage Directory Mapping, Backup All Files, Restore All Files. Since there is no mention of the right to reset passwords for other users, this suggests that "EMEALevel2Support" lacks the necessary permission to change the password for "Operator".

NEW QUESTION 149
Within the Vault each password is encrypted by:

A. the server key
B. the recovery public key
C. the recovery private key

D. its own unique key

Answer: D

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

NEW QUESTION 154
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.

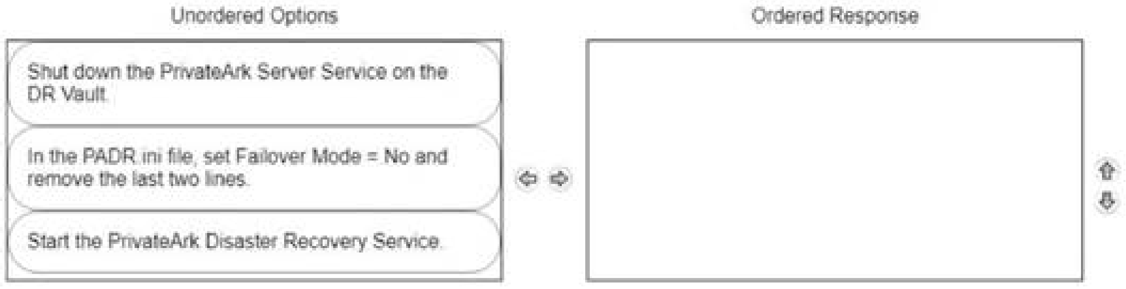
NEW QUESTION 155
To manage automated onboarding rules, a CyberArk user must be a member of which
group?

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

Answer: A

Explanation:
To manage automated onboarding rules in CyberArk, a user must be a member of the Vault Admins group. This group has the necessary permissions to create and manage predefined rules that automatically onboard newly discovered accounts, which helps minimize the time it takes to onboard and securely manage accounts, reduces the time spent on reviewing pending accounts, and prevents human errors that may occur during manual onboarding1.
References:
? CyberArk's official documentation on onboarding rules provides detailed information on the groups required to manage these rules, including the Vault Admins group1.

NEW QUESTION 159
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.



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.

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 164
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 169
Your customer, ACME Corp, wants to store the Safes Data in Drive D instead of Drive C. Which file should you edit?

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

Answer: A

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

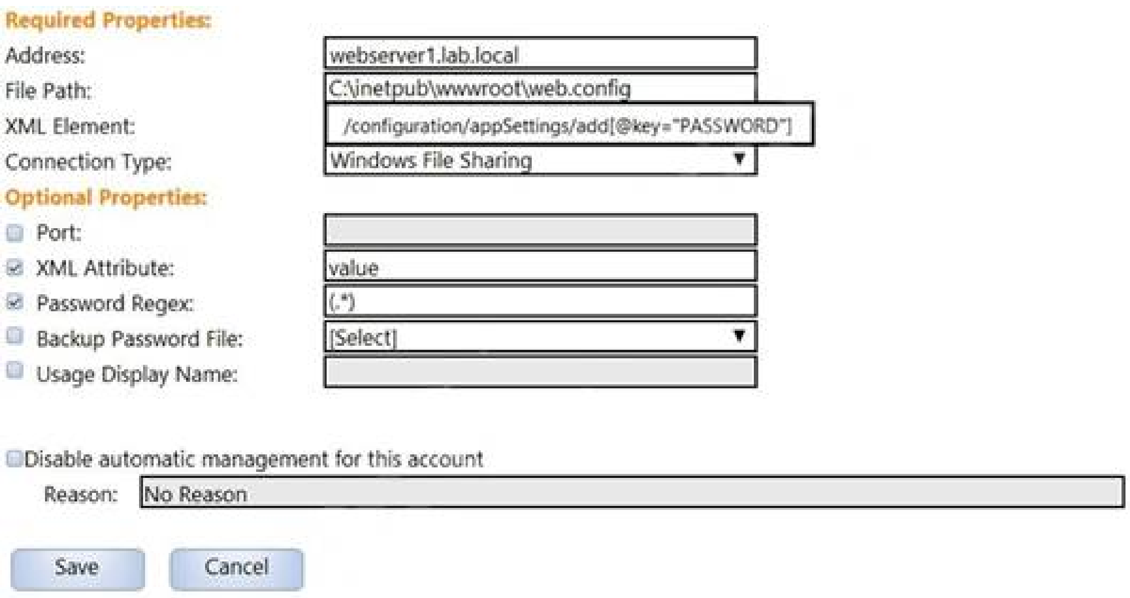
NEW QUESTION 174
When should vault keys be rotated?

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 178
In the screenshot displayed, you just configured the usage in CyberArk and want to update its password.
What is the least intrusive way to accomplish this?



Required Properties:

Address: webserver1.lab.local

File Path: C:\inetpub\wwwroot\web.config

XML Element: /configuration/appSettings/add[@key="PASSWORD"]

Connection Type: Windows File Sharing ▼

Optional Properties:

□ Port:

☑ XML Attribute: value

☑ Password Regex: (.*)

□ Backup Password File: [Select] ▼

□ Usage Display Name:

□ Disable automatic management for this account

Reason: No Reason

A. Use the “change” button on the usage’s details page.
B. Use the “change” button on the parent account’s details page.
C. Use the “sync” button on the usage’s details page.
D. Use the “reconcile” button on the parent account’s details page.

Answer: C

Explanation:
A usage is a configuration that allows CyberArk to manage passwords for files, such as XML or INI files, that are stored on remote machines. A usage is associated with a parent account, which is the account that has access to the file. To update the password of a usage, the least intrusive way is to use the “sync” button on the usage’s details page. This will synchronize the password value between the Vault and the file, without changing the actual password. The “change” button will initiate a password change process by the CPM, which will generate a new random password for the usage and the file. The “reconcile” button will initiate a password reconcile process by the CPM, which will use a reconcile account to reset the password of the usage and the file to the value stored in the Vault. References: Usages, Manage passwords for usages

NEW QUESTION 182
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 185
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 190
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 192

When managing SSH keys, the CPM stores the Public Key

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

Answer: B

Explanation:
When managing SSH keys, the CPM stores the public key on the target server. The CPM generates a new random SSH key pair and updates the public SSH key on the target machine. The public SSH key is stored in the home directory of the privileged user on the target machine, usually in the file ~/.ssh/authorized_keys. The public SSH key is not stored in the Vault, as this would be redundant and unnecessary. The public SSH key cannot be generated from the private key, as this would defeat the purpose of asymmetric encryption. References:
? Manage SSH Keys
? SSH Key Manager
? Use SSH Keys

NEW QUESTION 197
A Reconcile Account can be specified in the Master Policy.

A. TRUE
B. FALSE

Answer: B

Explanation:
A Reconcile Account is not specified in the Master Policy, but in the Platform settings. The Master Policy defines the general password management settings for all the accounts in the Vault, such as the frequency of password rotation and verification. The Platform settings define the specific password management settings for each type of target system, such as the password complexity and the Reconcile Account. References:
? Defender PAM course, Module 2: Password Management, Lesson 2: Master Policy and Platforms, slide 8
? Defender PAM course, Module 2: Password Management, Lesson 3: Reconcile and Logon Accounts, slide 2
? Defender PAM Sample Items Study Guide, Question 37
? CyberArk Privileged Access Security Documentation, Password Management - Master Policy
? CyberArk Privileged Access Security Documentation, Password Management - Platforms

NEW QUESTION 201
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 206
The Password upload utility can be used to create safes.

A. TRUE
B. FALSE

Answer: A

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

NEW QUESTION 208
Which command generates a full backup of the Vault?

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

Answer: A

Explanation:
The command PAReplicate.exe with the /FullBackup option is used to generate a full backup of the CyberArk Vault. This command requires the Vault configuration file (typically Vault.ini) and a credential file (specified with /LogonFromFile) that contains the user's encrypted logon credentials. The /FullBackup option indicates that a full backup of the Vault is to be performed, as opposed to an incremental backup1. References:
? CyberArk Docs: Install the Vault Backup Utility2
? CyberArk Knowledge Article: PAReplicate Configuration and Usage

NEW QUESTION 212
Time of day or day of week restrictions on when password verifications can occur configured in .

A. The Master Policy
B. The Platform settings
C. The Safe settings
D. The Account Details

Answer: C

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

NEW QUESTION 215
You are creating a new Rest API user that utilizes CyberArk Authentication.
What is a correct process to provision this user?

A. Private Ark Client > Tools > Administrative Tools > Users and Groups > New > User
B. Private Ark Client > Tools > Administrative Tools > Directory Mapping > Add
C. PVWA > User Provisioning > LDAP Integration > Add Mapping
D. PVWA > User Provisioning > Users and Groups > New > User

Answer: D

Explanation:
To provision a new Rest API user that utilizes CyberArk Authentication, the correct process involves using the PVWA (Password Vault Web Access). You would navigate to the User Provisioning section, then to Users and Groups, and select New > User. This allows you to create a new user that can be configured for Rest API access with the appropriate authentication method1.
References:
? CyberArk's official documentation on implementing Privileged Account Security Web Services provides information on using REST APIs to create, list, modify, and delete entities in PAM - Self-Hosted from within programs and scripts, which includes user provisioning1.
? Additional details on the process and best practices for creating Rest API users can be found in the CyberArk Privileged Access Manager documentation and training resources

NEW QUESTION 219
A user requested access to view a password secured by dual-control and is unsure who to contact to expedite the approval process. The Vault Admin has been asked to look at the account and identify who can approve their request.
What is the correct location to identify users or groups who can approve?

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

Answer: B

Explanation:
In CyberArk's Privileged Access Management (PAM), the correct location to identify users or groups who can approve a dual-control request is within the Password Vault Web Access (PVWA). Specifically, you would navigate to the 'Policies' section, then to 'Access Control (Safes)', and within a safe, you would go to 'Safe Members'. Here, under the 'Workflow' tab, there is an option to 'Authorize Password Requests'. This is where the Vault Admin can identify which users or groups are authorized to approve requests for viewing passwords secured by dual-control.
References: The information is based on the best practices and guidelines provided in the CyberArk Defender PAM course and learning resources, which include the official CyberArk documentation and study guides.

NEW QUESTION 222
You have been asked to secure a set of shared accounts in CyberArk whose passwords will need to be used by end users. The account owner wants to be able to track who was using an account at any given moment.
Which security configuration should you recommend?

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

Answer: C

Explanation:
One-time passwords and exclusive access are security features that can be configured for a platform in the Master Policy. These features enhance the security and accountability of shared accounts by ensuring that each password is used only once and by only one user at a time. One-time passwords generate a new password for each check- out and check-in of an account, preventing password reuse and exposure. Exclusive access prevents multiple users from accessing the

same account simultaneously, avoiding conflicts and confusion. By configuring both one-time passwords and exclusive access for the appropriate platform, the account owner can track who was using an account at any given moment and ensure that the passwords are always secure and unique. References
: One-Time Passwords, Exclusive Access, Master Policy

NEW QUESTION 227
Users are unable to launch Web Type Connection components from the PSM server. Your manager asked you to open the case with CyberArk Support.
Which logs will help the CyberArk Support Team debug the issue? (Choose three.)

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

Answer: ACD

Explanation:
When users are unable to launch Web Type Connection components from the PSM server, the CyberArk Support Team will require specific logs to debug the issue. The logs that are typically helpful in such cases include:
? PSMConsole.log: This log file contains informational messages and errors related to the PSM function, which can help identify issues with the PSM server's operation1.
? PSMTrace.log: This log file includes errors and trace messages, which can provide detailed insights into the issues occurring during the PSM server's processes1.
? <Session_ID>.Component.log: This log file contains errors and trace messages related to the connection component, which can be crucial for troubleshooting issues with launching Web Type Connection components1.
These logs can provide the necessary information to understand the problem and assist the support team in resolving the issue effectively.
References:
? CyberArk's official documentation on PSM for Web Troubleshooting, which outlines the types of logs available and their purposes in the troubleshooting process1.
? Additional resources on managing and interpreting PSM logs, which provide guidance on using logs for diagnosing and resolving issues with the PSM server2

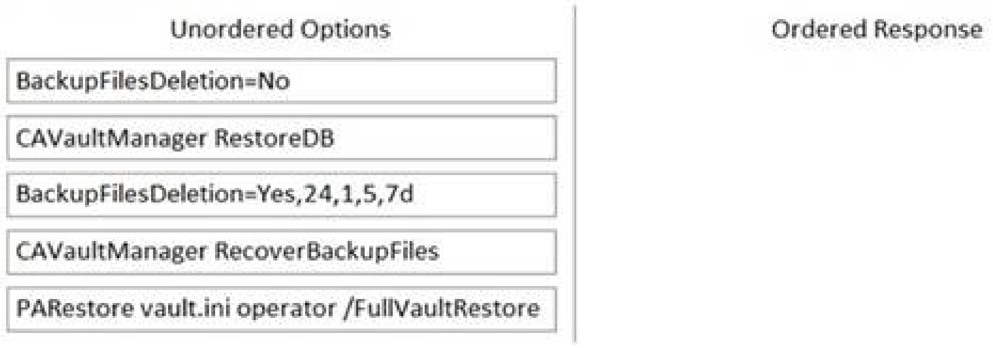
NEW QUESTION 231
PTA can automatically suspend sessions if suspicious activities are detected in a privileged session, but only if the session is made via the CyberArk PSM.

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

Answer: B

Explanation:
The PTA can automatically suspend sessions if suspicious activities are detected in a privileged session, regardless of the session method. The PTA can suspend sessions that are made via the PSM, the PVWA, or directly to the target system. The PTA can also suspend sessions that are made via SSH, RDP, or other protocols. References:
? Defender PAM Sample Items Study Guide, page 24
? PTA User Guide, page 17

NEW QUESTION 232
DRAG DROP
Arrange the steps to restore a Vault using PARestore for a Backup in the correct sequence.



Unordered Options

BackupFilesDeletion=No

CAVaultManager RestoreDB

BackupFilesDeletion=Yes,24,1,5,7d

CAVaultManager RecoverBackupFiles

PARestore vault.ini operator /FullVaultRestore

Ordered Response

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 234
What is required to manage loosely connected devices?

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

Answer: B

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

NEW QUESTION 235
Which report provides a list of account stored in the vault.

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

Answer: A

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

NEW QUESTION 238
......