CyberArk PAM-DEF Exam Questions

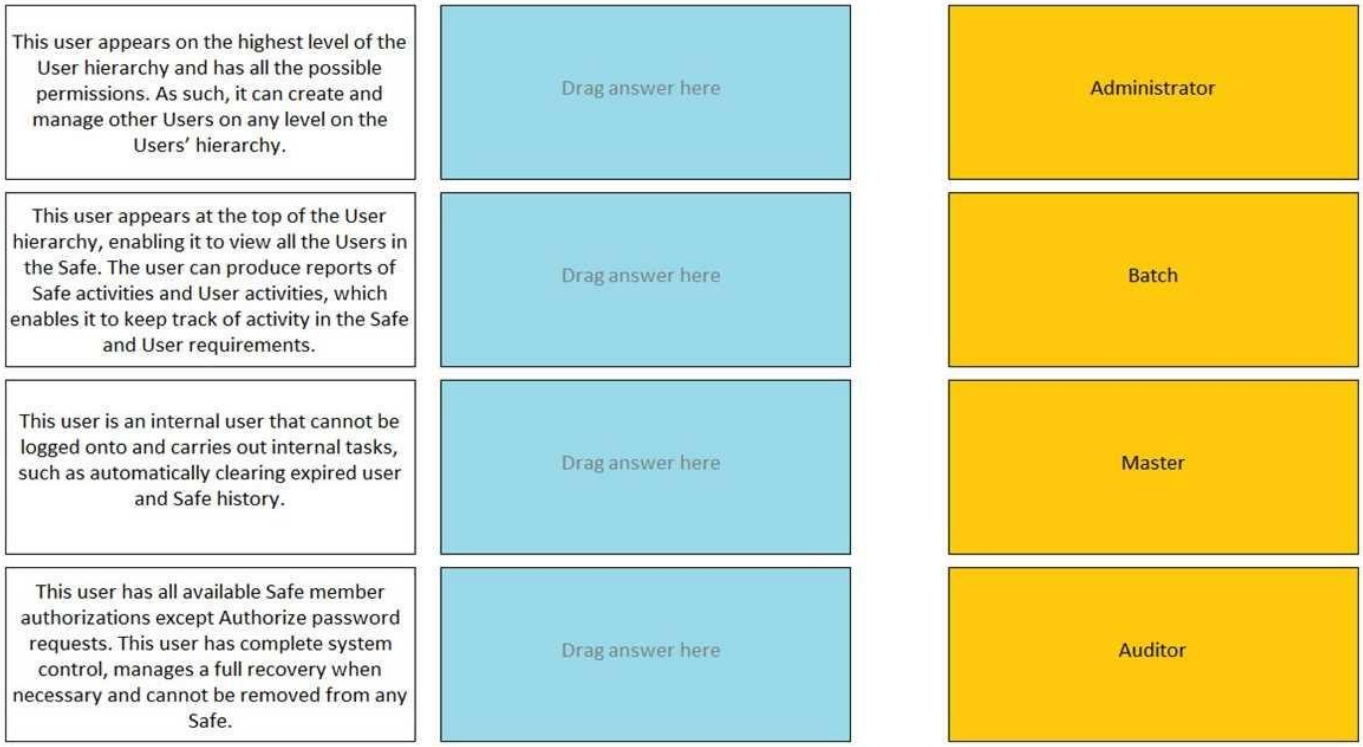
Total Questions: 220+
Demo Questions: 30
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit:
CyberArk PAM-DEF Exam Questions by Cert Empire

Question: 1

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



Answer:

Box 1: Master

Box 2: Auditor

Box 3: Batch

Box 4: Administrator

Explanation:

The question requires matching predefined CyberArk Vault users to their specific roles and permissions.

• The Master user is the ultimate superuser with all possible permissions, including the management of all other users, aligning with the first description.

• The Auditor user has system-wide, non-intrusive monitoring and reporting capabilities, matching the description of a user who views all activities to produce reports.

• The Batch user is a non-interactive internal account used for automated, background system tasks like clearing history, as described.

• The Administrator user holds high-level system control and recovery responsibilities and cannot be removed from Safes, fitting the final description. This user has extensive permissions but not the absolute power of the Master user.

References:

CyberArk Privileged Access Security System, Version 12.6, "Privileged Access Security Implementation Guide":
Master User: Section: "The Master User", Page 18 states, "The Master user has the highest level of authority in the system and can perform any task." It also notes the Master user can "add, delete, and manage all users in the Vault."
Administrator User: Section: "The Administrator User", Page 19 describes, "The Administrator user has complete system control... This user is responsible for the overall function of the system and manages a full system recovery when necessary."
Auditor Users: Section: "Auditor Users", Page 20 explains, "Auditor users can see all activity in the entire system... They generate reports about user and Safe activities..."
Batch User: Section: "The Batch User", Page 20 clarifies, "The Batch user is an internal user that carries out internal tasks, such as automatically clearing expired user and Safe history."

Question: 2

You are onboarding an account that is not supported out of the box. What should you do first to obtain a platform to import?

A. Create a service ticket in the customer portal explaining the requirements of the custom platform.

B. Search common community portals like stackoverflow, reddit, github for an existing platform.

C. From the platforms page, uncheck the "Hide non-supported platforms" checkbox and see if a platform meeting your needs appears.

D. Visit the CyberArk marketplace and search for a platform that meets your needs.

Answer:

D

Explanation:

The CyberArk Marketplace is the official and centralized repository for discovering, downloading, and deploying integrations and platforms developed by CyberArk, its partners, and the community. When a required account platform is not available "out of the box," the first and most appropriate step is to search the Marketplace. This ensures that any platform obtained is vetted and supported, reducing security risks and custom development effort. The Marketplace is specifically designed to extend the capabilities of the CyberArk Privileged Access Management solution with pre-built, downloadable components.

Why Incorrect Options are Wrong:

A. Creating a service ticket is for requesting support or custom development from CyberArk, which is not the first step when trying to find an existing, downloadable platform.
B. Searching community portals is highly discouraged for security platforms. Code from unverified sources can introduce significant vulnerabilities and is not supported by CyberArk.
C. This option unhides platforms that are already in the Vault but are inactive or deprecated. It does not help in obtaining a new platform for an unsupported account type.

References:

1. CyberArk Documentation - Manage account platforms: "You can import new platforms that you download from the CyberArk Marketplace, or platforms that you have created and exported from another environment." This document explicitly identifies the Marketplace as the primary source for new platforms. (CyberArk Privileged Access Management Documentation, Version 12.6, "Manage account platforms", Section: "Import a platform".)
2. CyberArk Marketplace - About Page: "The CyberArk Marketplace is a one-stop shop for our customers and partners to find and deploy integrations with the CyberArk Identity Security

Platform... It provides a centralized, comprehensive catalog of integrations and solutions..." This confirms the Marketplace's role as the official source for platform extensions. (Accessed via the official CyberArk website.)

3. CyberArk Documentation - Onboard and manage accounts: "Before you begin onboarding accounts, make sure that the relevant platform is active in your system. You can download additional platforms from the CyberArk Marketplace." This instruction places checking the Marketplace as a preliminary step to onboarding. (CyberArk Privileged Access Management Documentation, Version 12.6, "Onboard and manage accounts", Section: "Prerequisites".)

Question: 3

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

A. Vault Replicator

B. PAS Reporter

C. Remote Control Agent

D. Syslog

Answer:

C

Explanation:

The CyberArk Remote Control Agent (RCA) runs on the Vault server and polls the PrivateArk-related Windows services. It records whether each service is up or down, can restart failed services, and can alert administrators-making it the utility purposely designed for determining Vault-service status.

Why Incorrect Options are Wrong:

A. Vault Replicator - Copies data between production and DR Vaults; it neither queries nor reports service health.
B. PAS Reporter - Generates compliance and audit reports from Vault data; it does not monitor live service states.
D. Syslog - A generic logging protocol; CyberArk can forward events to it, but it is not a CyberArk utility for checking service status.

References:

1. CyberArk Privileged Access Security Installation Guide v12.1, "Install the Remote Control Agent," pp. 125-128: "The Remote Control Agent monitors Vault services, restarts them if necessary and sends status notifications."
2. CyberArk Privileged Access Security Hardening Guide v11.5, Section4.2 "Remote Control Agent (RCA)": "RCA continuously checks the PrivateArk Server, Event Notification Engine and other Vault services to verify they are running."
3. CyberArk Enterprise Password Vault Administrator Guide v10.7, Section11.2 "Remote Control Agent Service Monitoring," para 1-2: "Use the Remote Control Agent to view whether Vault services are up or down and to take corrective action."

Question: 4

You are logging into CyberArk as the Master user to recover an orphaned safe. Which items are required to log in as Master?

A. Master CD, Master Password, console access to the Vault server, Private Ark Client

B. Operator CD, Master Password, console access to the PVWA server, PVWA access

C. Operator CD, Master Password, console access to the Vault server, Recover.exe

D. Master CD, Master Password, console access to the PVWA server, Recover.exe

Answer:

A

Explanation:

Logging in as the Master user is a critical administrative function reserved for emergency or high-level configuration tasks. This process is intentionally restrictive and requires multiple security factors. The Master user can only log in from the Vault server console using the PrivateArk Client application. Authentication requires both the Master Password (something you know) and the Master CD, which contains the Master.key file (something you have). This combination ensures that only an authorized administrator with physical access to the Vault and possession of the secure credentials can perform these sensitive operations.

Why Incorrect Options are Wrong:

B: The Operator CD is used for starting the Vault service, not for Master user login. The Master user cannot log in through the PVWA.
C: The Operator CD is incorrect for Master login. Recover.exe is a specific disaster recovery utility, not the client used for managing safes.
D: The Master user must log in from the Vault server console, not the PVWA server. Recover.exe is the incorrect tool for this task.

References:

1. CyberArk Docs - Privileged Access Security v12.6: "Log on as the Master user". This document explicitly states the procedure: "The Master user can only log on to the Vault through the PrivateArk Administrative Client on the Vault server... In the Password box, specify the Master user's password... Click Keys on CD, and then specify the location of the Master key." This confirms the requirement for the PrivateArk Client, console access to the Vault server, the Master Password, and the Master CD (containing the key).
2. CyberArk Docs - Privileged Access Security v12.6: "Emergency Access". This section details scenarios requiring Master user access, reinforcing that such access is performed via the PrivateArk Administrative Client directly on the Vault server for tasks like recovering safes or

resetting user passwords when no other administrator can.
3. CyberArk Docs - Privileged Access Security v12.6: "Vault Keys". This documentation distinguishes between the Server Key, Master Key, and Operator Key. It clarifies that the Master Key (on the Master CD) is required for the Master user to log on and perform recovery activities, while the Operator Key (on the Operator CD) is used to open the Vault for regular operations.

Question: 5

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:

Platform Configuration is the specific location within CyberArk's Privileged Access Management (PAM) solution where password management policies are defined for different types of target systems (e.g., Windows, Linux, databases). This is where an administrator configures the detailed parameters for the Central Policy Manager (CPM), including the password rotation frequency. The "Perform periodic change" setting and its corresponding interval (e.g., 90 days) are set directly within the platform's policy settings.

Why Incorrect Options are Wrong:

A. Master Policy: The Master Policy sets high-level, mandatory security rules for the entire system, such as enforcing that periodic password changes must be enabled, but it does not define the specific interval (e.g., 90 days) for a given platform.
B. Safe Templates: Safe templates are used to pre-define properties and permissions for newly created Safes. They do not control the password management policies for the accounts that will be stored inside the Safe.
C. PVWAConfig.xml: This is a configuration file for the Password Vault Web Access (PVWA) interface. It controls web-related settings and behavior, not the backend password management policies executed by the CPM.

References:

1. CyberArk Docs - Privileged Access Manager - Self-Hosted (v12.6), "Manage Platforms": This document details the configuration of platforms. Under the "Automatic Password Management" section, it describes the "Perform periodic change" parameter: "Whether or not the CPM changes the password periodically. The frequency is determined by the value of the Password change interval (in days) parameter." This confirms that the specific rotation interval is set at the platform level.
2. CyberArk Docs - Privileged Access Manager - Self-Hosted (v12.6), "Master Policy": This

documentation explains the role of the Master Policy. It states, "The Master Policy is a list of high-level security and compliance policy rules that create a baseline of security for your entire privileged account security program." It shows rules like "Require password change every X days" can be enforced, compelling platforms to have this setting, but the value of 'X' is configured in the platform itself.
3. CyberArk Docs - Privileged Access Manager - Self-Hosted (v12.2), "Policy.ini": The underlying platform configuration file (Policy.ini) contains the parameter MinValidityPeriod. The documentation states, "The number of days that the password is valid for. After this number of days, the CPM will change the password." This parameter is a core part of the platform configuration.

Question: 6

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

A. List Accounts, View Safe members, Add accounts (includes update properties), Update Account
content, Update Account properties

B. List Accounts, Add accounts (includes update properties), Delete Accounts, Manage Safe

C. Add accounts (includes update properties), Update Account content, Update Account properties,
View Audit

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

Answer:

A

Explanation:

For Privileged Threat Analytics (PTA) to automatically add a discovered unmanaged account to the PasswordManagerpending safe, the designated PTAUser requires a specific set of minimum permissions. These permissions enable the user to create and populate the new account object within the safe. The required permissions are: List Accounts (to check for existing accounts), View Safe members (to validate safe context), Add accounts (the primary permission to create the account), and Update Account content/properties (to populate the details of the discovered account). This combination is the minimum required for the "Add to Pending" remediation action to function correctly.

Why Incorrect Options are Wrong:

B: This option includes Delete Accounts and Manage Safe, which are high-level administrative permissions not required for the specific task of adding a new account.
C: This option is missing the necessary List Accounts and View Safe members permissions and incorrectly includes View Audit, which is not needed for this action.
D: This option includes excessive permissions like Manage Safe and Access Safe without confirmation, which are unrelated to the automated onboarding of a pending account.

References:

1. CyberArk Privileged Threat Analytics (PTA) Documentation: In the section detailing the setup for automatic remediation, the specific permissions for the PTAUser on the PasswordManagerpending safe are explicitly listed. The required permissions are: List Accounts, Add accounts, Update account properties, Update account content, and View Safe Members. Source: CyberArk Docs: Privileged Threat Analytics (PTA) - Self-Hosted Configure PTA Remediate security events Configure automatic remediation. (Refer to the table "Permissions on the PasswordManagerpending Safe").

Question: 7

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

A. PrivateArk

B. RestAPI

C. Password Vault Web Access (PVWA)

D. Vault

Answer:

A

Explanation:

The PrivateArk Administrative Client is the primary thick-client interface for performing core administrative tasks directly on the CyberArk Vault. This includes the creation and comprehensive management of Safes and their properties. The time access restrictions for a Safe are configured within the Safe's properties, specifically under the "Time Restriction" tab, which is directly accessible through the PrivateArk Client. While modern versions of the PVWA also offer this capability, the PrivateArk Client is the foundational tool for low-level Vault and Safe administration.

Why Incorrect Options are Wrong:

B. RestAPI: This is a programmatic interface used for automation and integration, not a graphical user interface where an administrator would typically "find" and configure such a setting.
C. Password Vault Web Access (PVWA): Although modern PVWA versions allow administrators to manage Safe properties, including time restrictions, the PrivateArk Client is the original and most direct administrative tool for core Vault configurations.
D. Vault: The Vault is the secure server and storage component of the CyberArk solution; it is not a user interface used for configuration. One interacts with the Vault via a client like PrivateArk or PVWA.

References:

1. CyberArk Privileged Access Security Documentation v12.6: In the section "Manage Safes with the PrivateArk Administrative Client," the procedure to "Edit a Safe's properties" is detailed. It explicitly lists the "Time Restriction" tab within the Safe Properties window as the location to "specify the hours during which this Safe can be accessed." (CyberArk Docs Administration Manage Safes Edit a Safe's properties).
2. CyberArk Privileged Access Security Documentation v12.6: The "System and Architecture Guide" describes the roles of different components. It defines the PrivateArk Client (or Administrative Client) as the interface for "advanced administrative operations in the Vault," which

includes detailed Safe property management. (CyberArk Docs Get Started Privileged Access Security (PAS) system architecture CyberArk components).

Question: 8

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 Central Policy Manager (CPM) uses a set of platform-specific files to manage credentials on target systems. For UNIX/Linux devices, the UnixPrompts.ini file is used to define the command-line prompts that the CPM expects to encounter during a session (e.g., 'login:', 'password:', '$', '#'). The CPM scanner uses this file to correctly interpret the state of the remote shell and provide the appropriate responses to log in, execute commands, and manage passwords. This file is crucial for ensuring compatibility across different UNIX/Linux distributions and custom shell configurations.

Why Incorrect Options are Wrong:

B. plink.exe: This is an executable SSH client, a tool used for establishing the connection, not the configuration file that defines the interaction logic.
C. dbparm.ini: This is the core configuration file for the CyberArk Vault Server, containing database and security parameters, unrelated to CPM scanning.
D. PVConfig.xml: This is the main configuration file for the Password Vault Web Access (PVWA) user interface, not for backend CPM processes.

References:

1. CyberArk Privileged Access Manager Documentation (v12.6): "UNIX Account Management". This section details the files used for UNIX platform management. It states, "The following files are used to define the password management process for UNIX systems: ... UnixPrompts.ini - This file contains the prompts that are used in the process file." This confirms that UnixPrompts.ini is the configuration file for prompts.
2. CyberArk Privileged Access Manager Documentation (v12.6): "Central Policy Manager CPM Plugins". The documentation for developing and configuring CPM plugins for UNIX-like systems explicitly references the prompts and process files as the core mechanism for defining the command-and-response workflow, with UnixPrompts.ini being the default implementation for standard UNIX platforms.

Question: 9

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:

To meet the requirement of tracking who uses a shared account at any given moment, a combination of exclusive access and one-time passwords is the most effective configuration. Exclusive access ensures that only one user can check out and use an account's password at a time, preventing concurrent sessions. One-time passwords enforce that the password is automatically changed after each use. This combination creates a clear and unambiguous audit trail, definitively linking each specific usage session to the individual user who retrieved the password, thereby providing precise accountability.

Why Incorrect Options are Wrong:

A. Configure one-time passwords for the appropriate platform in Master Policy.
This is insufficient because it does not prevent multiple users from retrieving the password concurrently, which would disrupt sessions and complicate tracking active use.
B. Configure shared account mode on the appropriate safe.
"Shared account mode" is not a specific configuration setting in CyberArk. Safes are inherently designed to manage access to shared accounts among authorized members.
D. Configure object level access control on the appropriate safe.
This controls who has permission to access an account (the "object") but does not manage concurrent usage or enforce password rotation policies for accountability.

References:

1. CyberArk Privileged Access Security Documentation - Master Policy settings:
Section: Manage platforms Master Policy settings
Content: The documentation details platform-level policies that can be enforced through the Master Policy. It lists "Require exclusive password access" and "Generate one-time password access" as key security controls. This confirms that both are configured at the platform level and are part of the Master Policy framework.
2. CyberArk Privileged Access Security Documentation - Password Management:
Section: Work with accounts Exclusive accounts
Content: "To make sure that only one user can use an account at any given time, you can require users to retrieve passwords for exclusive use. When a password is used exclusively, it is locked and no other user can retrieve it." This directly supports the need for exclusive access to track usage "at any given moment."
3. CyberArk Privileged Access Security Documentation - One-time password access:
Section: Work with accounts One-time password access
Content: "For high security accounts, you can configure one-time password access... The password is changed on the remote machine immediately after it has been used." This supports the use of OTP for creating a unique credential for each session, enhancing accountability.

Question: 10

In your organization the "click to connect" button is not active by default. How can this feature be activated?

A. Policies Master Policy Allow EPV transparent connections Inactive

B. Policies Master Policy Session Management Require privileged session monitoring and isolation Add Exception

C. Policies Master Policy Allow EPV transparent connections Active

D. Policies Master Policy Password Management

Answer:

C

Explanation:

The "click to connect" functionality, which enables users to initiate a privileged session without viewing the password, is known as a transparent connection. This feature is governed globally by the Master Policy. To enable it across the environment, the "Allow EPV transparent connections" rule within the Master Policy must be set to "Active". This setting makes the "Connect" button available in the PVWA interface for accounts that are configured for PSM connections, allowing for secure and isolated session initiation.

Why Incorrect Options are Wrong:

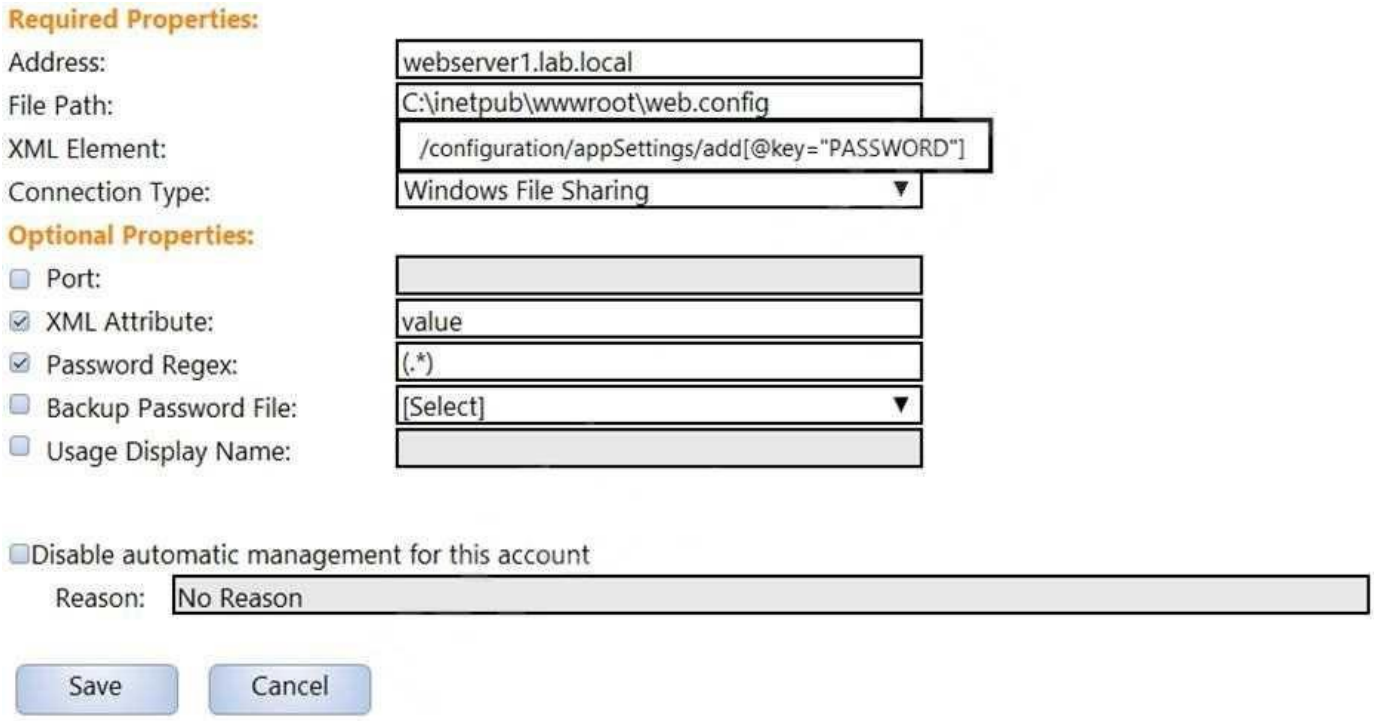
A. Setting "Allow EPV transparent connections" to "Inactive" explicitly disables the "click to connect" feature, which is the opposite of the required action.
B. This policy enforces PSM sessions for password access. Adding an exception bypasses session monitoring, it does not enable the connection button itself.
D. The "Password Management" section of the Master Policy controls password rotation, verification, and complexity, not session initiation methods.

References:

1. CyberArk Privileged Access Manager Documentation (v12.6), "Master Policy settings", Section: "Session Management". The documentation states: "Allow EPV transparent connections - Determines whether users can initiate privileged sessions transparently without seeing the password. When this is active, users can click Connect to open a privileged session."
2. CyberArk Privileged Access Manager Documentation (v12.6), "Configure the Master Policy", Section: "Activate a Master Policy rule". The procedure for activating policies is outlined here, confirming that setting a rule to "Active" is the method for enabling its corresponding feature. This applies directly to "Allow EPV transparent connections".

Question: 11

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?



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:

The "Sync" (Synchronize) function is designed specifically for dependent accounts, also known as usages. This operation updates the password on the dependent target system using the parent account's current password stored in the Vault. It does not initiate a password change or reconcile action on the parent account itself. Therefore, it is the least intrusive method because it isolates the update to only the out-of-sync usage without affecting the parent account or any other services that rely on it. This avoids a full password rotation cycle, which would be more disruptive.

Why Incorrect Options are Wrong:

A. A "change" button is not a feature on a usage's details page; password management actions are initiated from the parent account.
B. Using the "change" button on the parent account is highly intrusive as it forces a password rotation for the primary account.
D. The "reconcile" button on the parent account is also highly intrusive, used to forcibly reset a password that is out of sync.

References:

1. CyberArk Privileged Access Manager Documentation - v12.6, "Manage dependent accounts". In the section "Manually synchronize a dependent account password," the documentation states: "This synchronizes the password on the dependent account with the password of the main account that is stored in the Vault." This confirms the action's purpose is to update the usage without altering the parent account's password.
2. CyberArk Privileged Access Manager Documentation - v12.6, "Manage accounts". The descriptions for "Change Password" and "Reconcile Password" detail actions that actively alter the password on the remote machine for the primary account. This contrasts with the "Sync" function, which only propagates an existing password to a dependency, highlighting why "Sync" is the least intrusive option for the specified task.

Question: 12

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

A. PVWA User Provisioning LDAP Integration Mapping Criteria

B. PVWA User Provisioning LDAP Integration Map Name

C. PVWA Administration LDAP Integration Mappings

D. PVWA Administration LDAP Integration AD Groups

Answer:

C

Explanation:

The issue described is a classic authorization problem where a user authenticates successfully via LDAP but does not receive the correct permissions. This is typically caused by an incorrect directory mapping. In CyberArk, directory mappings link an external directory group (e.g., an Active Directory group) to an internal Vault group (e.g., the built-in Vault Admins group). The PVWA interface for managing these system-level integrations is located under the Administration section. The specific area to create, view, and edit these mappings is found within the LDAP Integration settings.

Why Incorrect Options are Wrong:

A. PVWA User Provisioning LDAP Integration Mapping Criteria: The "User Provisioning" section is not the correct location for managing core LDAP directory mappings; this is handled under "Administration".
B. PVWA User Provisioning LDAP Integration Map Name: This path is incorrect. System-wide LDAP integration settings are configured under the "Administration" tab, not "User Provisioning".
D. PVWA Administration LDAP Integration AD Groups: This is not a valid path within the PVWA interface. The AD group information is a component within a specific directory mapping, not a separate section.

References:

1. CyberArk Privileged Access Manager - Self-Hosted Documentation (v13.2), "Integrate with LDAP," Section: "Define a Directory Map." The procedure explicitly states: "In the PVWA, go to Administration LDAP Integration." This section details how to view and manage the list of directory mappings that link directory groups to Vault groups.
2. CyberArk Privileged Access Manager - Self-Hosted Documentation (v12.6), "LDAP Integration," Section: "Manage LDAP integration." The documentation guides administrators to

the Administration LDAP Integration page to configure directories and their corresponding mappings. This is the central location for verifying that an AD group is correctly mapped to the Vault Admins safe.

Question: 13

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 CyberArk platform dictates how the Privileged Session Manager (PSM) connects to a target system. For a Linux endpoint, the standard connection protocol is SSH. The PSM-SSH Connection Component is the specific module that the PSM uses to initiate and manage this type of session. If this component is not associated with the platform, the PSM does not know how to handle the connection request from the PVWA. As a result, when a user clicks the "Connect" button, the action fails without initiating a session, which manifests as "nothing happens."

Why Incorrect Options are Wrong:

B. UnixPrompts.ini: This is a Central Policy Manager (CPM) configuration file that defines expected command prompts for password management operations on Unix/Linux systems, not for user session connections.
C. UnixProcess.ini: This is a Central Policy Manager (CPM) file that defines the sequence of commands for password management processes (e.g., verify, change, reconcile) on Unix/Linux systems.
D. PSM-RDP Connection Component: This component is used for establishing connections to Windows systems via the Remote Desktop Protocol (RDP), not for connecting to Linux endpoints which typically use SSH.

References:

1. CyberArk Privileged Access Manager Documentation - Self-Hosted v12.6: "Platforms and service account platforms" "Target Account Platforms" "Connection Components".
Section: Connection Components
Content: This section explicitly states, "Connection Components are the PSM connectors that can be used to connect to remote machines." It lists PSM-SSH as the out-of-the-box component for connecting to Unix systems. This confirms that a connection component is required for the "Connect" button to function.

2. CyberArk Privileged Access Manager Documentation - Self-Hosted v12.6: "Privileged Session Manager" "Configure PSM" "Connection Components" "PSM-SSH".
Section: Configure the PSM-SSH connection component
Content: The documentation details that "The PSM-SSH connection component enables PSM to securely connect to SSH-based systems...". This directly links the PSM-SSH component to connecting to Linux/Unix endpoints.
3. CyberArk Privileged Access Manager Documentation - Self-Hosted v12.6: "Central Policy Manager" "CPM plugins" "Developing CPM plugins".
Section: Process and Prompts files
Content: This section describes the function of the Process.ini and Prompts.ini files, clarifying their role in CPM's password management workflows, which is distinct from PSM's session initiation. This supports why options B and C are incorrect.

Question: 14

Which CyberArk utility allows you to create lists of Master Policy Settings, owners and safes for output to text files or MSSQL databases?

A. Export Vault Data

B. Export Vault Information

C. PrivateArk Client

D. Privileged Threat Analytics

Answer:

B

Explanation:

The ExportVaultInformation (EVI) utility is a command-line tool specifically designed for extracting Vault configuration metadata. Its primary function is to create comprehensive lists of Master Policy settings, Safe owners, and Safe configurations. This utility provides the flexibility to output the extracted information into structured formats, such as text files for simple reporting or directly into an MSSQL database for more complex analysis and integration. This capability is crucial for auditing, reporting, and maintaining an overview of the Vault's security posture and configuration.

Why Incorrect Options are Wrong:

A. Export Vault Data: This utility is used to export the contents of Safes (e.g., passwords, files), not the Vault's configuration metadata like Master Policy settings.
C. PrivateArk Client: This is the graphical user interface for Vault administration. While it can be used to view configurations, it is not the specific utility for bulk exporting this data to text files or a database.
D. Privileged Threat Analytics: This is a security monitoring and analytics component that detects and alerts on anomalous privileged user behavior; it does not export configuration lists.

References:

1. CyberArk Privileged Access Security Documentation, Version 12.6, "ExportVaultInformation Utility".
Section: Server Post-Installation Tasks ExportVaultInformation Utility.
Content: "The ExportVaultInformation utility enables you to create lists of Master Policy settings, Owners and Safes, and output them to text files or to an MSSQL database." This directly confirms the utility's purpose as described in the question.
2. CyberArk Privileged Access Security Documentation, Version 12.6, "Export Vault Data".
Section: Utilities Export Vault Data.
Content: "The Export Vault Data utility (EVD) enables you to export data from Safes in the Vault

to a target location." This distinguishes its function from exporting metadata.
3. CyberArk Privileged Access Security Documentation, Version 12.6, "Privileged Threat Analytics".
Section: Introduction to PTA PTA components.
Content: Describes PTA's role in "detecting, alerting on, and responding to the highest-risk privileged activity." This confirms it is a security analytics tool, not a data export utility.

Question: 15

Which PTA sensors are required to detect suspected credential theft?

A. Logs, Vault Logs

B. Logs, Network Sensor, Vault Logs

C. Logs, PSM Logs, CPM Logs

D. Logs, Network Sensor, EPM

Answer:

B

Explanation:

To detect suspected credential theft, such as Pass-the-Hash (PtH) or Pass-the-Ticket (PtT) attacks, Privileged Threat Analytics (PTA) requires multiple data sources for a comprehensive analysis. It correlates information from the CyberArk Vault to understand legitimate privileged account activity, analyzes network traffic for anomalous authentication patterns, and ingests security event logs from sources like Domain Controllers. This combination allows PTA to build a baseline of normal behavior and accurately identify deviations that indicate a credential has been compromised and is being used maliciously on the network.

Why Incorrect Options are Wrong:

A. Logs, Vault Logs: This option is incomplete. Without the Network Sensor, PTA cannot capture and analyze the network authentication traffic (e.g., NTLM, Kerberos) where attacks like Pass-the-Hash are visible.
C. Logs, PSM Logs, CPM Logs: This is incorrect because PSM and CPM logs detail activities within the CyberArk environment (session activity, password management), not the malicious use of stolen credentials on the broader network.
D. Logs, Network Sensor, EPM: While EPM is a powerful sensor for detecting credential theft attempts on the endpoint, Vault logs are a more fundamental requirement for PTA to correlate network events with the specific privileged accounts managed by CyberArk.

References:

1. CyberArk Privileged Threat Analytics Documentation - "Data Sources": The official documentation specifies the data sources PTA uses for its security algorithms. It explicitly lists Vault traffic and logs, network traffic captured via a network sensor (or port mirroring), and log data from SIEMs or directly from Domain Controllers as key inputs for detecting credential theft. Reference: CyberArk Privileged Threat Analytics (PTA) Implementation Guide, Version 12.x, Chapter: "System Architecture and Components", Section: "Data Sources". This section details

that PTA receives Vault syslog records, Windows event logs from Domain Controllers, and network traffic data to detect threats.
2. CyberArk Privileged Threat Analytics Documentation - "Credential Theft": The documentation on specific threat detection scenarios highlights that detecting Pass-the-Hash and Overpass-the-Hash requires analyzing network traffic. PTA's Network Sensor is designed for this purpose, capturing authentication packets and forwarding them for analysis. The correlation with Vault data is essential to distinguish privileged from non-privileged activity.
Reference: CyberArk Privileged Threat Analytics (PTA) Security Fundamentals Guide, Version 12.x, Chapter: "PTA Detections", Section: "Suspected Credential Theft". This section explains that the detection algorithm relies on analyzing authentication traffic from the network and correlating it with user activity data from the Vault and Windows Events.

Question: 16

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:

To generate a "Privileged Accounts Inventory" report with complete information, a user requires a combination of permissions. The fundamental permission is List Accounts, which allows the user to see the accounts stored within the safe. To provide a complete inventory, which includes the context of who has access to these accounts, the View Safe Members permission is also required. This permission allows the reporting engine to retrieve the list of users and groups who are members of the safe, thereby presenting a full picture of the privileged accounts and their associated entitlements.

Why Incorrect Options are Wrong:

B. Manage Safe Owners is an excessive administrative permission for adding/removing owners and is not required for a read-only inventory report.
C. Access Safe without confirmation is a permission related to specific password access workflows (dual control) and is irrelevant to generating reports.
D. Manage Safe allows modification of safe properties, and View Audit is for viewing activity logs; neither is used for listing account inventory.

References:

1. CyberArk Privileged Access Manager Documentation v12.6, "Reports in PVWA": This section details the reports available in the PVWA. It specifies that the "Privileged Accounts Inventory" report "generates a list of all accounts and their properties." The baseline permission for this is List accounts.
2. CyberArk Privileged Access Manager Documentation v12.6, "Reports in PVWA": The documentation for the "Entitlements report" states that it "generates a list of all Safe members and their permissions" and requires the View Safe Members authorization. For an "account inventory" report to be considered "complete," it must include this entitlement data, thus requiring both

permissions.
3. CyberArk Privileged Access Manager Documentation v12.6, "Safe Members": This page defines the authorizations for safe members. It confirms that List Accounts "Enables users to see the accounts in the Safe" and View Safe Members "Enables users to see the other members of the Safe." The combination of these two permissions provides the data needed for a complete inventory report as described in the question.

Question: 17

Which usage can be added as a service account platform?

A. Kerberos Tokens

B. IIS Application Pools

C. PowerShell Libraries

D. Loosely Connected Devices

Answer:

B

Explanation:

CyberArk Privileged Access Management (PAM) provides dedicated platforms to manage the credentials of service accounts used by various applications and services. An IIS Application Pool is a classic example of such a "usage." CyberArk's Central Policy Manager (CPM) has a specific plugin designed to automatically manage the lifecycle of passwords for accounts that run IIS Application Pools. This process includes password rotation in the Vault and updating the password directly in the IIS configuration, ensuring service continuity without manual intervention.

Why Incorrect Options are Wrong:

A. Kerberos Tokens: Kerberos tokens are temporary authentication credentials generated during a session; they are not a service account or a platform usage that requires password management by the CPM.
C. PowerShell Libraries: PowerShell libraries are collections of code (cmdlets/functions). They do not run under a specific service identity and are not a manageable usage type for a service account platform.
D. Loosely Connected Devices: This term typically refers to endpoints managed by CyberArk's Endpoint Privilege Manager (EPM), not a type of service account usage managed by core PAM platforms like the CPM.

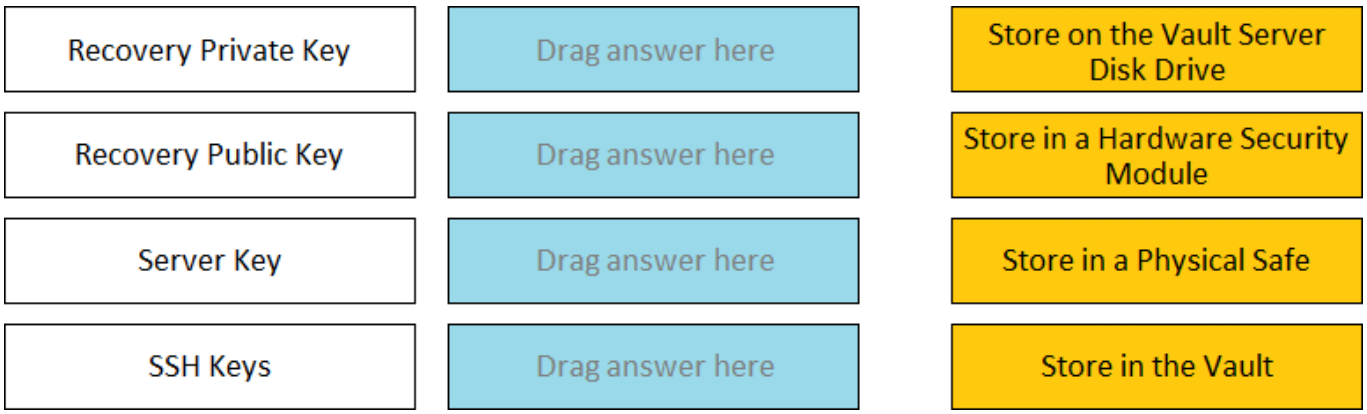
References:

1. CyberArk Privileged Access Management Documentation, Version 12.6: "Manage IIS application pool passwords". This section explicitly details the CPM's capability to manage passwords for accounts used by both IIS application pools and virtual directories. It states, "The CPM can manage passwords for the following types of accounts: Accounts used by IIS application pools."
2. CyberArk Privileged Access Management Documentation, Version 12.6: "CPM Plugins". The documentation lists the "CyberArk.Extensions.IISAppPool.dll" and "CyberArk.Extensions.IISAdminDirectory.dll" as the core components of the CPM plugin

responsible for managing IIS Application Pool and virtual directory credentials, confirming it is a supported service account usage.

Question: 18

DRAG DROP Match each key to its recommended storage location.



Answer:

Recovery Private Key: Store in a Physical Safe

Recovery Public Key: Store on the Vault Server Disk Drive

Server Key: Store in a Hardware Security Module

SSH Keys: Store in the Vault

Explanation:

This question assesses knowledge of best practices for storing various cryptographic keys within a secrets management architecture, likely HashiCorp Vault.

• The Recovery Private Keys (unseal keys) are the most critical components for accessing a sealed Vault. They are part of Shamir's Secret Sharing scheme and must be stored offline in a highly secure location, making a physical safe the appropriate choice.

• The Server Key, likely referring to the Vault's master encryption key or a critical TLS key, should be protected with the highest level of security. An HSM (Hardware Security Module) provides tamper-resistant hardware-based protection and enables features like auto-unsealing.

• SSH Keys are a type of dynamic or static secret that Vault is designed to manage and broker access to. Their intended location is securely within the Vault's encrypted storage, managed by a secrets engine.

• The Recovery Public Key (e.g., a PGP key for rekeying operations) is less sensitive. Storing it

on the Vault server's disk drive makes it available for administrative operations without requiring the extreme security of an HSM or physical safe.

References:

HashiCorp Vault Documentation, "Concepts - Seal/Unseal": This document explains that the unseal keys (Recovery Private Keys) are distributed to trusted operators who are responsible for their secure storage. Offline methods like a physical safe are the standard recommendation.
HashiCorp Vault Documentation, "Auto-unseal with HSM": This guide details using a Hardware Security Module (HSM) to protect the master key (a critical Server Key). It states, "Auto-unseal is a convenient feature that decrypts the Vault's master key with a key from a trusted source... such as a hardware security module (HSM)." This directly supports matching the Server Key to an HSM.
HashiCorp Vault Documentation, "Secrets Engines - SSH": The official documentation for the SSH secrets engine explicitly describes its function as managing SSH credentials. It states, "The SSH secrets engine for Vault provides multiple ways to secure and manage access to your fleet of machines," confirming that SSH keys are a type of secret to be stored in the Vault.
HashiCorp Vault Documentation, "Rekeying and Rotating": The rekey operation documentation shows a -pgp-keys flag, which takes a file path to one or more PGP public keys. This supports the concept of a "Recovery Public Key" being stored as a file on the server disk to be used during an administrative CLI operation.

Question: 19

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

A. Recovery Private Key

B. Recover.exe

C. Vault data

D. Recovery Public Key

E. Server Key

F. Master Password

Answer:

A, B, C

Explanation:

To recover and decrypt a specific object from the Vault data files outside of a running Vault, three core components are required. First, the Vault data (C) containing the encrypted Safe files is necessary as it holds the target object. Second, the Recover.exe (B) utility is the specific command-line tool designed for this disaster recovery task. Third, the Recovery Private Key (A) is the cryptographic key required by Recover.exe to decrypt the Vault's Server Key, which in turn is used to decrypt the Safe's contents and retrieve the object's information.

Why Incorrect Options are Wrong:

D. Recovery Public Key: This key is used during Vault installation to encrypt the Server Key. It is not used for decryption during the recovery process.
E. Server Key: The Server Key is required for decryption, but it is itself encrypted. The Recovery Private Key is the component you must provide to the utility to unlock the Server Key.
F. Master Password: The Master Password is a credential used to protect access to the Recovery Private Key on the Master CD, not a direct input for the decryption algorithm within the Recover.exe utility.

References:

1. CyberArk Privileged Access Manager - Self-Hosted Documentation v12.6, "Disaster Recovery for the Digital Vault Recover the Vault Data". This section details the recovery procedure, stating: "The Vault recovery process is performed with the CAVaultManager utility... This utility uses the Server private recovery key to access the Server key and decrypt the Vault files." It also lists the required files for recovery, which include the Vault data and metadata files, and the Recovery Private Key (recprv.key). The Recover.exe is the underlying legacy tool for this function.

2. CyberArk Privileged Access Manager - Self-Hosted Documentation v12.6, "CAVaultManager Recover". The documentation for the CAVaultManager Recover command, which performs this function, specifies the required parameters: /RecoveryPrvKey (the path to the Recovery Private Key) and the path to the Vault data files. This confirms the necessity of both the utility, the key, and the data.
3. CyberArk Privileged Access Manager - Self-Hosted Documentation v12.2, "Privileged Access Security System Basics The Master CD". This section explains the contents of the Master CD, explicitly stating it contains "The recovery private key that is required to restore the CyberArk Vault data." This highlights the key's role as a fundamental component for data restoration.

Question: 20

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 most straightforward and officially recommended method to create a new platform based on an existing one is through the Password Vault Web Access (PVWA) interface. The PVWA provides a dedicated "Duplicate" button in the Platform Management section. This function creates an exact copy of the selected platform's configuration, which can then be renamed and modified. This GUI-based approach is the simplest, safest, and least error-prone method, as it leverages the built-in administrative tools designed for this purpose.

Why Incorrect Options are Wrong:

A. Manually copying and renaming Policy.ini files in PrivateArk is a complex backend procedure, not the "easiest" way, and it bypasses built-in validation.
C. The PVConfiguration.xml file contains general PVWA settings, not the specific definitions for individual account platforms.
D. The platform management interface in the PVWA does not have a "Save as" function; the correct and available option is "Duplicate".

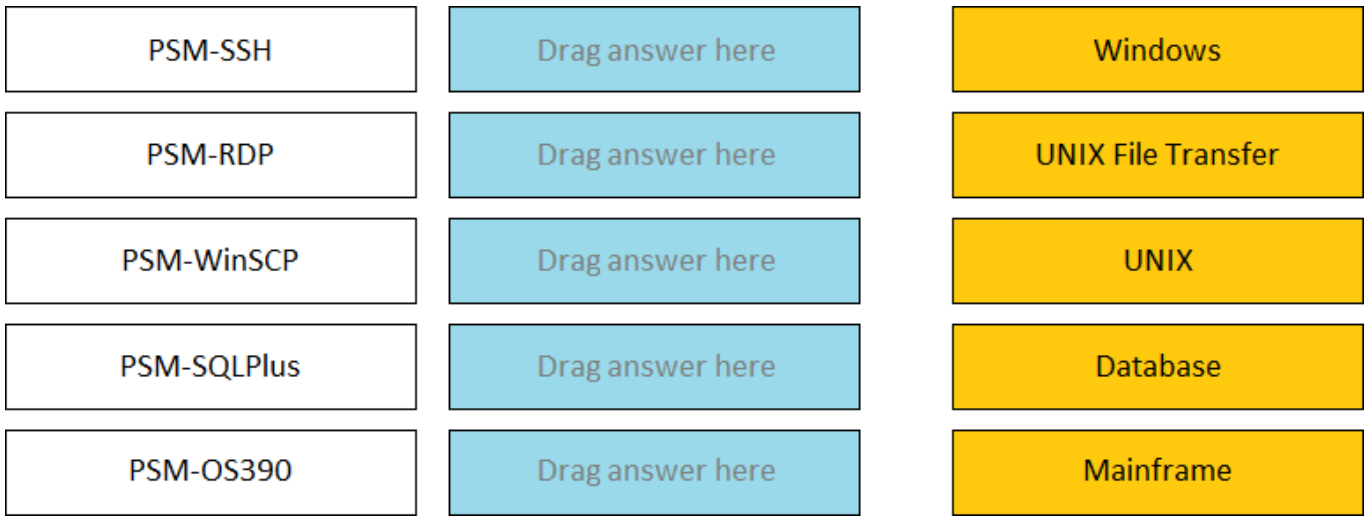
References:

1. CyberArk Privileged Access Manager - Self-Hosted Documentation v12.6: In the "Administration" section, under "Platform Management," the procedure is explicitly detailed. It states: "Select an existing platform that is similar to the new target account platform you want to create, and then click Duplicate. In the Duplicate Platform window, specify the Name of the new

platform, and then click Save & Close." This directly confirms the process described in option B. (Source: CyberArk Docs, "Manage platforms").
2. CyberArk Privileged Access Management (PAM) - Self-Hosted - Administration Courseware: This official training material instructs administrators on best practices for platform management. The course demonstrates that duplicating an existing, similar platform via the PVWA is the standard first step when onboarding a new type of account that requires a custom platform. This reinforces that "Duplicate" is the intended and easiest method. (Source: CyberArk Education, PAM Administration Course Module on Platform Management).

Question: 21

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



Answer:

PSM-SSH: UNIX

PSM-RDP: Windows

PSM-WinSCP: UNIX File Transfer

PSM-SQLPlus: Database

PSM-OS390: Mainframe

Explanation:

The question requires matching each Privileged Session Manager (PSM) connection component to its target operating system or function.

• PSM-RDP uses the Remote Desktop Protocol, which is native to Windows for providing a graphical user interface to a remote computer.

• PSM-SSH utilizes the Secure Shell protocol, the standard for secure command-line access to UNIX and Linux systems.

• PSM-WinSCP integrates with the WinSCP client, which is used for secure file transfers over protocols like SFTP and SCP, primarily with UNIX-based systems.

• PSM-SQLPlus is a specific connector for launching the SQL*Plus command-line tool to connect to an Oracle Database.

• PSM-OS390 uses a 3270 terminal emulator to connect to IBM Mainframe systems running z/OS, the successor to OS/390.

References:

CyberArk Privileged Session Manager Documentation - PSM for SSH: The documentation states, "CyberArk's PSM for SSH, also known as the SSH Proxy, enables you to connect to, monitor and record SSH sessions on UNIX, Linux and network devices." See Privileged Session Manager Implementation PSM Connectors PSM for SSH.
CyberArk Privileged Session Manager Documentation - Out-of-the-Box PSM Connectors: The list of default connectors specifies that the PSM-RDP connection component is used for "Connections to Windows machines, using any RDP client." See Privileged Session Manager Reference Out-of-the-Box PSM Connectors PSM-RDP.
CyberArk Privileged Session Manager Documentation - PSM for Databases: This section details the configuration for database connections, explicitly mentioning clients like SQLPlus for Oracle. See Privileged Session Manager Implementation PSM Connectors PSM for Databases.
CyberArk Privileged Session Manager Documentation - PSM for Z/OS: This documentation describes the solution for securing and managing privileged sessions on IBM Mainframes, which run the z/OS operating system (the successor to OS/390). See PSM for z/OS PSM for z/OS Overview.
CyberArk Marketplace - WinSCP PSM Connection Component: The official marketplace entry for the WinSCP connector describes it as a component to "initiate a secure file transfer session using WinSCP." This is used for secure file transfers, typically to UNIX servers. See the WinSCP PSM Connection Component page on the CyberArk Marketplace.

Question: 22

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

A. CyberArk stores Private keys in the Vault and updates Public keys on target systems.

B. CyberArk stores Public keys in the Vault and updates Private keys on target systems.

C. CyberArk does not store Public or Private keys and instead uses a reconcile account to create keys
on demand.

D. CyberArk stores both Private and Public keys and can update target systems with either key.

Answer:

A

Explanation:

The "UNIX Via SSH Keys" platform in CyberArk operates on the fundamental principles of public-key cryptography for secure authentication. The private key, which is the confidential component used to prove identity, is securely stored and managed within the CyberArk Vault. The corresponding public key is then distributed and configured on the target UNIX/Linux systems, typically within the authorizedkeys file of the target user. When CyberArk rotates the SSH key, it generates a new key pair, stores the new private key in the Vault, and replaces the old public key with the new one on the target system.

Why Incorrect Options are Wrong:

B. Storing the public key in the Vault and distributing the private key to target systems would be a severe security vulnerability, as the private key would be exposed.
C. CyberArk must store the private key in the Vault to manage the credential and facilitate secure, brokered connections to the target system.
D. While both keys are stored in the Vault for management, only the public key is ever pushed to the target system for authentication purposes.

References:

1. CyberArk Privileged Access Security Documentation, Version 12.6: "SSH Key Management". The documentation states, "The SSH Key Manager secures and rotates SSH private keys and provides control over the corresponding public keys on remote hosts." This confirms the private key is secured (in the Vault) and the public key is managed on the target.
2. CyberArk Privileged Access Security Documentation, Version 12.6: "Onboard SSH Keys". This section details the process: "When you onboard a private key, you provide the private key content... The SSH Key Manager deploys the corresponding public key to the target machines."

This explicitly supports the workflow described in option A.

3. CyberArk Privileged Access Security Documentation, Version 12.6: "Central Policy Manager Target Platforms UNIX". The configuration details for the "UNIX via SSH Keys" platform show parameters for managing the private key within the Vault and processes for updating the public key on the target (/etc/ssh/sshdconfig and /.ssh/authorizedkeys).

Question: 23

You want to generate a license capacity report. Which tool accomplishes this?

A. Password Vault Web Access

B. PrivateArk Client

C. DiagnoseDB Report

D. RestAPI

Answer:

B

Explanation:

The License Capacity Report is a system-level administrative report that provides a summary of the number of users and components defined in the Vault compared to the licensed capacity. This report is generated using the PrivateArk Client, which is the primary thick-client administrative interface for the CyberArk Vault. It is specifically designed for core administrative tasks, including managing licenses and generating related reports. The report can be accessed directly from the Tools Reports menu within the PrivateArk Client interface.

Why Incorrect Options are Wrong:

A. Password Vault Web Access: The PVWA is the web interface for end-users and auditors. Its reporting capabilities focus on user activities, entitlements, and compliance, not core system license management.
C. DiagnoseDB Report: This is a low-level diagnostic utility used by CyberArk support and advanced administrators for troubleshooting database integrity and performance issues, not for generating standard administrative reports.
D. RestAPI: While the REST API can retrieve various system health and configuration details, the specific, pre-formatted "License Capacity Report" is a built-in function of the PrivateArk Client GUI.

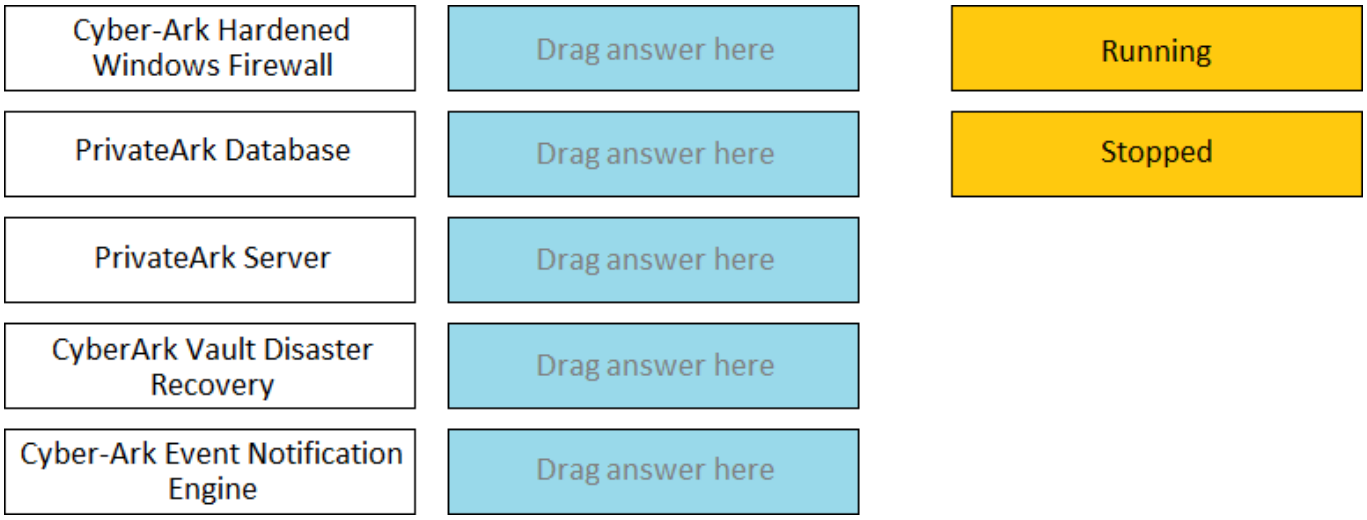
References:

1. CyberArk Privileged Access Manager Documentation (Self-Hosted) v13.2, "Reports in the PrivateArk Client", Section: "Generate a License Capacity report". The documentation explicitly states, "This report provides a summary of the number of users and components that are defined in the Vault, according to the license." It then provides the step-by-step procedure: "In the PrivateArk Client, from the Tools menu, select Reports, and then select License Capacity."
2. CyberArk Privileged Access Manager Documentation (Self-Hosted) v13.2, "PrivateArk Client", Section: "The PrivateArk Interface". This section describes the PrivateArk Client as the interface for performing all administrative tasks in the Vault, which includes system-level reporting like

license capacity. The "Tools" menu is identified as the location for administrative utilities and reports.

Question: 24

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



Answer:

Running:

• Cyber-Ark Hardened Windows Firewall

• PrivateArk Database

• CyberArk Vault Disaster Recovery

Stopped:

• PrivateArk Server

• Cyber-Ark Event Notification Engine

Explanation:

In a standard CyberArk Disaster Recovery (DR) configuration, the DR Vault operates in a passive, standby mode, continuously replicating data from the production Vault.

For this replication to function, the CyberArk Vault Disaster Recovery service must be Running to manage the data synchronization. The underlying PrivateArk Database service also needs to be Running to write the incoming replicated data to the DR Vault's storage. The Cyber-Ark Hardened Windows Firewall is a critical security component and should always be Running.

Conversely, services that handle active client connections and business logic, such as the PrivateArk Server and the Cyber-Ark Event Notification Engine, must be Stopped. This prevents the DR Vault from serving traffic or performing active operations, which could lead to a "split-brain" scenario and data inconsistency.

References:

CyberArk Privileged Access Security Documentation, Version 12.6, "Configure the CyberArk Digital Vault for Disaster Recovery." This section details the setup and expected state of services on a DR Vault. It specifies that the CyberArk Vault Disaster Recovery service should be running to enable replication, while the PrivateArk Server service must be stopped.
CyberArk Privileged Access Security Implementation Guide, "The CyberArk Digital Vault Server," Section: "CyberArk Vault Disaster Recovery." This guide explains the architecture of the DR solution, noting that the DR Vault is a passive node. The documentation explicitly states, "On the DR Vault, the CyberArk Vault Disaster Recovery service is started automatically, but the CyberArk Server service remains shut down."
CyberArk Privileged Access Security Installation Guide, "Post Installation Tasks," Section: "DR Vault Services." This guide provides a checklist for verifying a DR installation. It indicates that the PrivateArk Database service must be running for the replication to write data, but the Event Notification Engine service remains stopped as it is not an active Vault.

Question: 25

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:

B

Explanation:

The Master Policy is the central location for defining and enforcing global security controls across the CyberArk PAM environment. Within the Master Policy, the Session Management section contains the specific rules to globally enable and require privileged session monitoring and isolation via PSM. Activating rules such as "Require privileged session monitoring and isolation" and "Record and save session activity" here applies the policy to all relevant platforms, ensuring a consistent security posture. This is the primary and most effective method for enabling PSM for all platforms from a policy perspective.

Why Incorrect Options are Wrong:

A. Platform Management (Platform) UI & Workflows: This configures PSM settings for a single, specific platform. It does not enable PSM globally for all platforms as the question requires.
C. Master Policy Privileged Access Workflows: This section manages access request policies, such as requiring dual control or confirming access, not the fundamental enablement of session recording or isolation.
D. Administration Options Connection Components: This area is for defining and configuring the parameters of the connection components themselves (e.g., PSM-RDP), not for enforcing their use on platforms.

References:

1. CyberArk Docs - Master Policy Settings: "The Master Policy provides a high level of control over your privileged accounts security policy. For example, you can require users to connect to target machines through PSM, ensuring that all their activities are recorded." This is configured under the Session Management settings. (Source: CyberArk Privileged Access Security Documentation, v12.6, "Master Policy", Section: "Session Management settings").
2. CyberArk Docs - Platform vs. Master Policy: "The Master Policy settings for session management determine whether or not privileged sessions are recorded... These settings are the default for all privileged accounts, but can be overridden for specific accounts by creating

exceptions." This highlights that the global enablement is in the Master Policy. (Source: CyberArk Privileged Access Security Documentation, v12.6, "Privileged Session Manager", Section: "Configure Session Recording and Auditing").
3. CyberArk Docs - Platform Configuration: The documentation for configuring individual platforms states that under UI & Workflows Connection Components, you associate an already defined PSM connection component with the platform. This is a secondary, implementation step that follows the global policy decision made in the Master Policy. (Source: CyberArk Privileged Access Security Documentation, v12.6, "Platforms", Section: "UI & Workflows").

Question: 26

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

A. 500 GB

B. 1 TB

C. same as disk size on Satellite Vault

D. same as disk size on Primary Vault

Answer:

D

Explanation:

PAReplicate is the utility that facilitates the creation of a Disaster Recovery (DR) Vault. The DR Vault is designed to be a complete, byte-for-byte replica of the Primary (or Production) Vault. To ensure a full and successful replication of all safes, data, metadata, and recordings, the server designated for the DR Vault must have a disk capacity that is at least equal to that of the Primary Vault. This requirement guarantees that there is sufficient space to store the entire replicated dataset, both for the initial full synchronization and for ongoing incremental changes.

Why Incorrect Options are Wrong:

A. 500 GB: This is an arbitrary fixed value. The Primary Vault's data can easily be smaller or significantly larger than this, making it an unreliable requirement.
B. 1 TB: This is also a fixed value and is incorrect for the same reason as the 500 GB option; it does not scale with the actual size of the Primary Vault.
C. same as disk size on Satellite Vault: PAReplicate is used to replicate the Primary Vault for disaster recovery, not a Satellite Vault, which is a component of the Distributed Vaults architecture.

References:

1. CyberArk Privileged Access Manager - Self-Hosted Installation Guide v14.0, Section: "Install the Disaster Recovery Vault", Subsection: "Before you install the DR Vault". The guide states, "The DR Vault machine must have the same hardware and software configuration as the production Vault machine." This requirement for identical hardware configuration explicitly includes disk size.
2. CyberArk Privileged Access Security System Requirements Guide v12.6, Page 11, Section: "CyberArk Digital Vault Server", Subsection: "Disaster Recovery Site". The document specifies, "The Disaster Recovery site must have the same hardware and software configuration as the production Vault." This reinforces that all hardware aspects, including disk space, must match the primary production server.

Question: 27

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

A. Select Update on the CyberArk group, and then click Add LDAP Group

B. Select Update on the LDAP Group, and then click Add LDAP Group

C. Select Member Of on the CyberArk group, and then click Add LDAP Group

D. Select Member Of on the LDAP group, and then click Add LDAP Group

Answer:

A

Explanation:

To add an LDAP group as a member of a native CyberArk group using the PrivateArk Client, the administrator must modify the membership list of the target CyberArk group. One correct method is to select the CyberArk group, click "Update" to open its properties, navigate to the "Members" tab, and then click "Add". From the list of available users and groups, the administrator can then select the desired LDAP group to add as a member. This action effectively nests the LDAP group within the CyberArk group.

Why Incorrect Options are Wrong:

B. Select Update on the LDAP Group, and then click Add LDAP Group
This is incorrect. The "Update" function on an LDAP-mapped group is used to manage its properties, not its membership within other CyberArk groups.
C. Select Member Of on the CyberArk group, and then click Add LDAP Group
This is incorrect. The "Member Of" function on the CyberArk group is used to make the CyberArk group a member of another group, not to add members to it.
D. Select Member Of on the LDAP group, and then click Add LDAP Group
This describes an incorrect procedure. While you can select the LDAP group and use "Member Of" to add it to a CyberArk group, the final step as written ("Add LDAP Group") is illogical.

References:

1. CyberArk Privileged Access Manager Documentation (v12.6), "Privileged Access Manager - Self-Hosted," Section: Administration PrivateArk Client Manage CyberArk Users and Groups Update group properties.
This section details the process of updating a group's properties, explicitly stating: "In the Members tab, you can add existing users and groups to the selected group." This directly supports the procedure described in option A.
2. CyberArk Privileged Access Manager Documentation (v12.6), "Privileged Access Manager - Self-Hosted," Section: Administration PrivateArk Client Manage CyberArk Users and Groups Add

a user or group as a member of another group.
This document outlines the primary methods for managing group membership. It confirms that actions to add a member are performed on the container group's "Members" list, which is accessible via the main window pane or the "Update" properties dialog (supporting option A). It also implicitly clarifies that the "Member Of" function (used in option C) serves the opposite purpose.

Question: 28

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

A. The heartbeat s no longer detected on the private network.

B. The shared storage array is offline.

C. An alert is generated in the Windows Event log.

D. The Digital Vault Cluster does not detect a node failure.

Answer:

A

Explanation:

The CyberArk Digital Vault Cluster relies on a dedicated private network connection between the two nodes for high availability monitoring. Each node sends a periodic "heartbeat" signal to the other over this private link. If the active node fails to receive this heartbeat from the passive node within a predefined timeout period, it concludes that the peer node is down or unreachable. This missed heartbeat is the primary trigger for the cluster management service to initiate failover procedures, ensuring service continuity. This mechanism is fundamental to the cluster's ability to automatically detect and respond to node failures.

Why Incorrect Options are Wrong:

B. The shared storage array is offline.
This represents a storage failure affecting the entire cluster, not the specific mechanism for one node to detect the failure of another node.
C. An alert is generated in the Windows Event log.
An event log entry is a result or a record of a detected failure; it is not the detection mechanism itself. The failure is detected first, then logged.
D. The Digital Vault Cluster does not detect a node failure.
This is fundamentally incorrect. The primary purpose of a high availability cluster is to detect node failures and manage failover to maintain service availability.

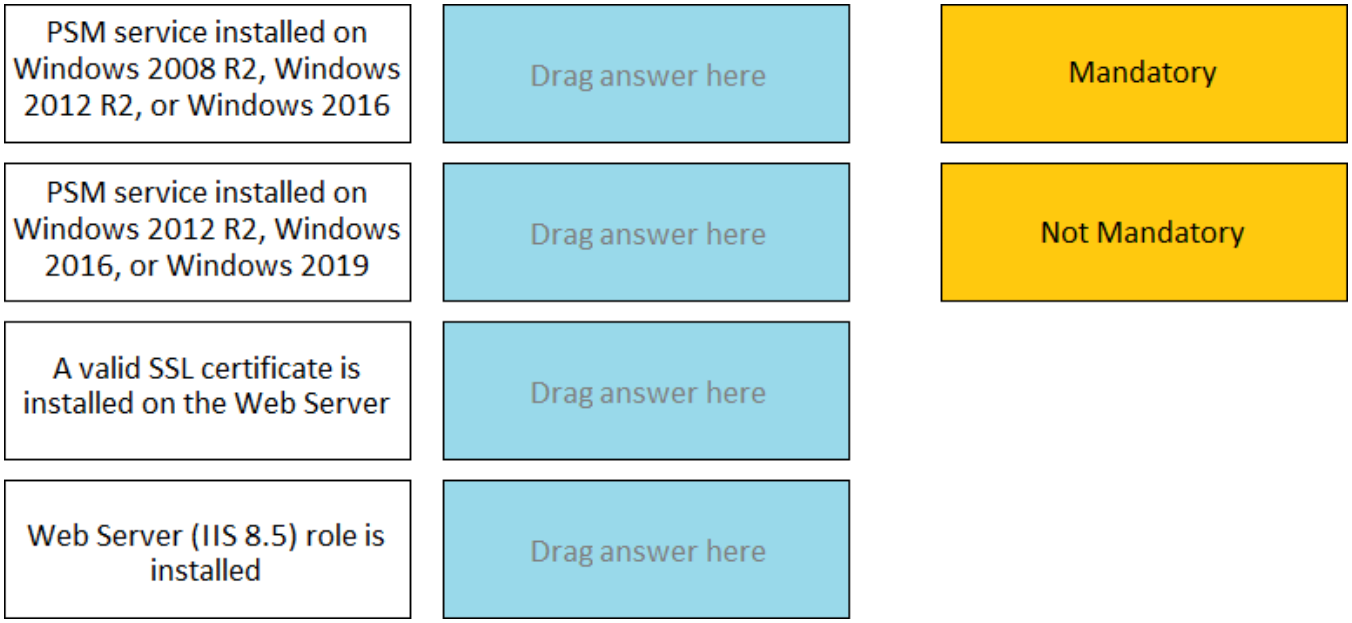
References:

1. CyberArk Privileged Access Security Installation Guide (Version 12.6), "Cluster Vault Environment", Page 215. The document states: "Private network - A dedicated network that connects the two Cluster Vault nodes. This network is used for synchronization and for the heartbeat that is sent between the nodes to check that they are both active."
2. CyberArk Privileged Access Security System Requirements Document (Version 12.6), "High Availability Vault Cluster Requirements", Page 11. This document specifies the requirement for a

dedicated NIC for "the private network between the two cluster nodes (heartbeat and synchronization)." This underscores the heartbeat's role in the dedicated network architecture for failure detection.

Question: 29

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



Answer:

Mandatory

• PSM service installed on Windows 2012 R2, Windows 2016, or Windows 2019

• A valid SSL certificate is installed on the Web Server

Not Mandatory

• PSM service installed on Windows 2008 R2, Windows 2012 R2, or Windows 2016

• Web Server (IIS 8.5) role is installed

Explanation:

The PSM Health Check utility requires the PSM service to be installed on a currently supported operating system, which includes Windows Server 2012 R2, 2016, and 2019. The list including the end-of-life Windows Server 2008 R2 is therefore not a mandatory prerequisite.

A valid SSL certificate is a mandatory prerequisite for the proper functioning and security of the HTML5 gateway, a key component that the Health Check utility is designed to validate. Running a health check on a system without a valid certificate would result in a failed check for that

component.

The Web Server (IIS) role is only a prerequisite if the PSM environment includes the HTML5 Gateway. The Health Check tool can still run and validate a core PSM installation that does not use the HTML5 Gateway feature. Therefore, IIS is not a mandatory prerequisite for the tool itself to run.

References:

CyberArk Privileged Access Security System Requirements Documentation: The official documentation specifies the supported operating systems for Privileged Session Manager (PSM). For versions 11.x and newer, support for Windows Server 2008 R2 has been deprecated. The mandatory requirement is a modern, supported OS like Windows Server 2012 R2, 2016, or 2019.
CyberArk Privileged Session Manager Implementation Guide: In the section "Install the PSM HTML5 Gateway," the documentation explicitly lists a "valid SSL certificate for the web server" as a prerequisite for the installation and operation of the gateway. The Health Check tool validates this configuration.
CyberArk Post-Installation and Upgrade Tasks Documentation: The page describing the "PSM Health Check" outlines the checks performed. It shows that checks for the HTML5 Gateway (which requires IIS) are part of the process, but the tool can be executed on a PSM server without the gateway installed to check other core PSM functionalities. This confirms that IIS is not a universal prerequisite to simply run the utility.

Question: 30

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

A. Suspend, Terminate, None

B. Suspend, Terminate, Lock Account

C. Pause, Terminate, None

D. Suspend, Terminate

Answer:

A

Explanation:

Within the CyberArk Privileged Threat Analytics (PTA) security rule configuration for "Privileged Session Analysis and Response," administrators can define automated actions to be taken on a live privileged session when a rule is triggered. The available direct session response options are to Suspend the session, which pauses it for review by an authorized user; Terminate the session, which immediately ends it; or take None action, which logs the event and creates an alert without interfering with the session. These options allow for a tiered response based on the detected risk.

Why Incorrect Options are Wrong:

B. Suspend, Terminate, Lock Account: "Lock Account" is an action performed on a user's account within the Vault, not a direct response option for a live session in the PTA rule configuration.
C. Pause, Terminate, None: "Pause" is not the official terminology used in the CyberArk interface for this function; the correct and available option is "Suspend".
D. Suspend, Terminate: This option is incomplete because it omits the "None" action, which is a valid and the default choice for a response.

References:

1. CyberArk Privileged Threat Analytics Implementation Guide (Version 13.0), Section: "Configure PTA Rules". In the rule creation wizard, under the "Response" tab for a "Privileged Session Analysis and Response" rule, the guide details the available actions. The documentation explicitly lists the radio button options as "None", "Suspend session", and "Terminate session". This directly confirms that A is the correct set of available choices.
2. CyberArk Privileged Threat Analytics Documentation, Section: "Security Rules". This section describes the components of a PTA rule, including the response. It states, "For privileged sessions, you can configure an automatic response to either suspend or terminate the session." It also implicitly includes "None" as the default behavior of only alerting.