DUMPSARENA

CyberArk Defender + Sentry

CyberArk CAU302

Version Demo

Total Demo Questions: 31

Total Premium Questions: 314

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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 OperationsStaff 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 OperationsManagers. The members of OperationsManagers never need to be able to use the show, copy or connect buttons themselves.

Which safe permissions do you need to grant to OperationsManagers? (Choose all that apply.)

A. Use Accounts

B. Retrieve Accounts

C. List Accounts

D. Authorize Password Requests

E. Access Safe without Authorization

ANSWER: C D

Explanation:

Members of OperationsManagers need **List Accounts** and **Authorize Password Requests**. Dual control separates the person requesting access to a privileged account from the person approving that access. The **Authorize Password Requests** safe permission allows an OperationsManagers member to approve or reject an OperationsStaff request that is awaiting authorization. This is the permission that makes the group an approver for the relevant safe.

List Accounts is also required so approvers can view the accounts and associated pending requests in the safe, identify the account for which approval is being requested, and make an informed authorization decision. These permissions support an approval-only role: the manager can participate in the request workflow without receiving the ability to retrieve a password or start a privileged session. CyberArk documents safe-member permissions and the authorization workflow in its Privilege Cloud and PAM Self-Hosted documentation. See CyberArk: Add Safe members and assign permissions and CyberArk: Dual control.

QUESTION NO: 2

CyberArk Logical Container

A. CPMlog

B. CPM_error.log

C. pm.log

D. pm.errors.log

ANSWER: C

Explanation:

pm.log is the correct selection because it is the Password Manager (CPM) operational log used to record the component's regular processing activity. In CyberArk Privileged Access Manager, the Central Policy Manager performs automated account-management tasks, including password verification, reconciliation, and changing passwords according to platform policies. Its operational log is therefore a key source when an administrator needs to trace the sequence of CPM activity for a managed account or understand the progress of a password-management operation.

The log should be reviewed alongside the account's status and the relevant CPM task details when investigating an operational issue. Entries provide context such as the account being processed, the platform and policy workflow involved, and the outcome or stage of the task. This makes **pm.log** the appropriate log name for the CyberArk Password Manager's primary activity logging in the context described. CyberArk's documentation for self-hosted PAM includes CPM

administration and troubleshooting information in the Central Policy Manager documentation. The broader product documentation and current version-specific administration guidance are available through the CyberArk Documentation Portal.

QUESTION NO: 3

PSM requires the Remote Desktop Gateway role service.

A. TRUE

B. FALSE

ANSWER: B

Explanation:

FALSE is correct. CyberArk Privileged Session Manager (PSM) is deployed on a Windows Server that provides controlled, isolated privileged sessions. Its Windows Remote Desktop Services dependency is the Remote Desktop Session Host capability used to host and broker the interactive sessions that PSM records and monitors. The Remote Desktop Gateway role service is not a mandatory PSM prerequisite. RD Gateway is a separate Microsoft role that can be used to provide secure external RDP connectivity over HTTPS, and an organization may deploy it as part of its wider network-access architecture, but PSM does not require that role to be installed in order to function.

CyberArk's PSM installation and system-requirement guidance identifies the required server components and installation process for the PSM machine, while Microsoft distinguishes Remote Desktop Gateway from the Remote Desktop Session Host role. This distinction matters during deployment: install and configure the components explicitly required for the PSM host, then add an RD Gateway only where the organization's remote-access design calls for it. See CyberArk's PSM installation documentation and Microsoft's Remote Desktop Services access planning documentation.

QUESTION NO: 4

What is the purpose of the Allowed Safes parameter in a CPM policy? Select all that apply.

A. To improve performance by reducing CPU workload.

B. To prevent accidental use of a policy in the wrong safe.

C. To allow users to access only the passwords they should be able to access.

D. To enforce Least Privilege in CyberArk.

ANSWER: B D

Explanation:

The Allowed Safes parameter limits the safes in which accounts governed by a particular CPM platform policy may be stored and managed. Therefore, *To prevent accidental use of a policy in the wrong safe.* is correct: defining the permitted safes creates a platform-to-safe boundary and helps ensure that accounts are onboarded only into the intended organizational, operational, or security context. This is particularly important where separate safes are used for different environments, business units, or account classes that require distinct password-management settings.

To enforce Least Privilege in CyberArk. is also correct because the parameter supports least-privilege administration by constraining where a platform's management capabilities can be used. It reduces the scope in which a given policy can affect accounts, helping administrators apply only the intended password-management rules to the intended account population. Safe membership and safe-level permissions remain the primary mechanism that determines whether individual users can view or use passwords; however, Allowed Safes complements those controls by restricting policy applicability. CyberArk's documentation portal provides product configuration guidance at CyberArk Docs, and CyberArk describes the underlying least-privilege principle at What Is the Principle of Least Privilege?.

QUESTION NO: 5

The Vault supports multiple instances of the following components. (Choose all that Apply.)

A. PVWA

B. CPM

C. PSM

D. AIM Provider

ANSWER: A B C D

Explanation:

A CyberArk PAM deployment is designed to scale by connecting multiple component instances to the same Vault environment. Multiple **PVWA** instances can be deployed behind a load balancer to provide resilient, scalable web access for users and administrators. Multiple **CPM** instances can distribute account-management workload, including password verification, reconciliation, and change operations, according to platform and account assignments. Multiple **PSM** instances can be deployed to increase concurrent-session capacity and provide high availability for monitored and isolated privileged sessions.

Multiple **AIM Provider** instances are also supported. Credential Providers are normally installed near the applications that need credentials, and each Provider securely retrieves authorized secrets from the Vault on behalf of its local application workloads. This distributed design supports application scaling and availability while preserving centralized credential policy and auditing in the Vault. Consequently, all four listed components can have multiple instances associated with the Vault. CyberArk's architecture documentation describes the Vault as the central secure repository used by distributed PAM components, while its high-availability guidance covers deploying redundant component infrastructure. See CyberArk PAM Self-Hosted architecture and CyberArk high-availability documentation.

QUESTION NO: 6

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

A. PAR Agent

B. PrivateArk Server Central Administration

C. Edit DBParm.ini in a text editor.

D. Setup exe

ANSWER: A B

Explanation:

PAR Agent and **PrivateArk Server Central Administration** can change the Vault Server's active debugging configuration while the Vault remains online. PAR Agent is a Vault administration utility that can issue operational commands to the server, including commands used for diagnostic tracing. This makes it suitable when an administrator needs to increase or reduce logging temporarily while investigating a live issue, without interrupting Vault availability.

PrivateArk Server Central Administration provides an administrative interface for managing server-level settings, including debugging controls. When debugging levels are changed through this supported administration mechanism, the Vault applies the relevant runtime setting without requiring the Vault Server service to be restarted. This is particularly valuable during troubleshooting because diagnostic collection can begin immediately while connected components and users continue to access the Vault.

CyberArk documents Vault configuration and administration procedures in its PAM Self-Hosted documentation. See the Vault configuration documentation and the Vault monitoring and troubleshooting documentation for supported operational administration guidance.

QUESTION NO: 7

What are the chief benefits of PSM? Choose all that apply

A. Privileged Session Isolation

B. Automatic Password Management

C. Privileged Session Recording

D. A & C

ANSWER: D

Explanation:

Privileged Session Isolation and Privileged Session Recording are the chief benefits provided by CyberArk Privileged Session Manager (PSM). PSM acts as a secure proxy between a privileged user and a target system, so users can connect to managed systems without receiving or directly handling the privileged account credential. This isolation reduces credential exposure and allows access to be governed through the CyberArk platform.

PSM also records privileged sessions, creating an auditable record of user activity performed through supported connection methods. Session recordings can be reviewed to support investigations, audit requirements, operational troubleshooting, and accountability for privileged access. CyberArk describes PSM as a component that isolates, monitors, and records privileged sessions, helping organizations control and oversee access to sensitive systems. These capabilities work together: the proxy-based connection protects the privileged credential and target environment while the recording provides visibility into actions taken during the session.

For additional product information, see CyberArk's Privileged Session Manager overview and the CyberArk PSM documentation.

QUESTION NO: 8

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

A. Dual Control

B. One Time Passwords

C. Exclusive Passwords

D. Password Reconciliation

E. Ticketing Integration

F. Required Properties

G. Custom Connection Components

H. Password Aging Rules

ANSWER: A B C E H

Explanation:

The Master Policy defines vault-wide controls for privileged-password access and lifecycle behavior. **Dual Control** is configured there to require an authorized approver before a requester can retrieve or use a password. **One Time Passwords** is also an access-control policy setting; it ensures a retrieved password is changed after use, preventing it from being reused by the same or another user. **Exclusive Passwords** can be enabled in the Master Policy to reserve an account for one user during the access period, preventing concurrent access to that account's password. **Ticketing Integration** is configured as part of Master Policy access controls so that users can be required to provide a valid ticket reference when requesting access. Finally, **Password Aging Rules** are Master Policy password-policy controls that govern password expiration and related aging behavior at the vault level. These settings establish the baseline policy that applies

broadly in the Vault; more account- or platform-specific operational behavior can then be configured separately as needed. CyberArk's product documentation describes the Master Policy as the location for configuring password policy and password-access control settings. See the CyberArk PAM Self-Hosted documentation and the CyberArk documentation portal.

QUESTION NO: 9

What values are acceptable in the address field on the Accounts Details.

A. It must be a fully qualified domain name (FQDN)

B. It must be an IP address

C. It must be NetBIOS name

D. Any name that is resolvable on the CPM server is acceptable

ANSWER: D

Explanation:

Any name that is resolvable on the CPM server is acceptable because the Address account property identifies the target system that the Central Policy Manager must contact when it performs password-management operations. CyberArk does not require one particular naming convention for every target: the value may be an IP address, a fully qualified DNS name, a short host name, or another host identifier, provided that the CPM can resolve it and establish the required network connection to the managed account's target system. In practice, administrators should use a stable, unambiguous address that resolves consistently from every CPM that may manage the account. This is especially important in distributed environments, where each relevant CPM must have equivalent DNS, hosts-file, or other name-resolution access. The Address property is also used along with platform configuration and account connection properties to direct CyberArk's password-management process to the intended endpoint. CyberArk's account-property documentation describes Address as the target machine address, while its password-management documentation explains the CPM's role in connecting to remote systems to change and verify credentials. See CyberArk Account Properties documentation and CyberArk Password Management documentation.

QUESTION NO: 10

When working with the CyberArk Disaster Recovery (DR) solution, which services should be running on the DR Vault?

A. CyberArk Vault Disaster Recovery (DR), PrivateArk Database

B. CyberArk Vault Disaster Recovery

C. CyberArk Vault Disaster Recovery, PrivateArk Database, PrivateArk Server

D. CyberArk Vault Disaster Recovery, PrivateArk Database, CyberArk Event Notification Engine

ANSWER: D

Explanation:

The required services on a standby DR Vault are **CyberArk Vault Disaster Recovery, PrivateArk Database, CyberArk Event Notification Engine**. The CyberArk Vault Disaster Recovery service is responsible for maintaining synchronization between the production Vault and the DR Vault, ensuring that protected data is available if the primary environment must be recovered. The PrivateArk Database service must be available because it provides the Vault's database functionality used by the DR process. The CyberArk Event Notification Engine must also run so that relevant Vault events and notifications can be handled as part of the DR environment's normal operation.

The DR Vault is deliberately maintained as a standby system while synchronization is in progress. CyberArk's documented DR design separates the services needed to replicate and maintain the standby Vault from the active Vault server operation that is used after a failover. This preserves the integrity of the DR configuration and supports a controlled activation process

when the primary Vault is unavailable. CyberArk describes the DR Vault synchronization and recovery architecture in its Disaster Recovery documentation. Additional Vault deployment and service information is available in the Vault installation documentation.

QUESTION NO: 11

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

A. Suspected credential theft

B. Over-Pass-The-Hash

C. Golden Ticket

D. Unmanaged privileged access

ANSWER: B C

Explanation:

Over-Pass-The-Hash and Golden Ticket require network-level visibility into Active Directory authentication traffic. CyberArk Privileged Threat Analytics obtains this visibility by using a deployed Network Sensor or, where network-sensor deployment is not suitable, by installing the PTA Agent on a domain controller. These collection methods allow PTA to inspect the Kerberos-related activity needed to identify suspicious ticket use and authentication patterns.

For Over-Pass-The-Hash, PTA analyzes Kerberos authentication behavior associated with the use of an NTLM hash to obtain a Kerberos ticket, rather than using a password in the normal interactive authentication flow. Detecting this technique depends on observing the relevant domain-controller authentication exchanges. Golden Ticket detection similarly relies on analyzing Kerberos ticket activity to identify indications that a forged ticket-granting ticket is being used. Because the domain controller processes and records the authentication events central to both techniques, the Network Sensor or PTA Agent on the domain controller provides the required telemetry.

CyberArk documents the detection types and their required data sources in its PTA detection documentation.

QUESTION NO: 12

Where does the Vault administrator configure in Password Vault Web Access (PVWA) the Fully Qualified Domain Name (FQDN) of the target email server during Simple Mail Transfer Protocol (SMTP) integration?

A. PVWA > Platform Management > Notification Settings

B. PVWA > Options > Notification Settings

C. PVWA > Administration > System Configuration > E-mail

D. PVWA > LDAP Integration > Notification Settings

ANSWER: C

Explanation:

The correct location is **PVWA > Administration > System Configuration > E-mail**. This administrative configuration area contains the settings that PVWA uses to send email notifications. The Vault administrator specifies the organization's SMTP server using its fully qualified DNS name in the SMTP server address setting. Using an FQDN rather than an unqualified host name allows PVWA to resolve and reach the mail server consistently through the configured DNS infrastructure, including in environments with multiple domains or network segments.

This configuration is performed by a user with the required administrative permissions in PVWA because the SMTP server setting applies to the system's notification delivery behavior. After the mail-server address and any required connection settings are configured, PVWA can use that server to deliver CyberArk notification messages, such as password-expiration,

access-request, and account-management notifications. CyberArk's documented email-notification configuration procedure identifies the PVWA Administration/System Configuration E-mail settings as the place to define the SMTP server details. See CyberArk: Configuring Email Notification.

QUESTION NO: 13

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:

Replicate is the CyberArk Vault component/utility used to create a backup copy of Vault data, including a backup written to tape. It performs a controlled replication of the Vault's protected data to the configured backup target, enabling organizations to retain an offline or long-term backup in accordance with their recovery and retention requirements. This backup process is distinct from ongoing Vault replication used for operational resiliency: its purpose is to produce a recoverable Vault backup that can be retained separately from the production Vault environment. A tape backup is particularly useful as an isolated recovery copy, helping protect against scenarios that affect online systems or storage. The backup operation must be planned with the appropriate media, permissions, and Vault backup procedures so that the resulting copy can be used during a supported recovery process. CyberArk's Vault backup documentation and its customer support guidance identify the Replicate utility as the mechanism for creating this type of Vault backup. See the CyberArk knowledge-base reference and the Vault backup documentation.

QUESTION NO: 14

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: A B C D

Explanation:

Ad-Hoc Access, previously called Secure Connect, extends Privileged Session Manager capabilities to target systems that do not have to be onboarded and managed as accounts in the CyberArk Vault. It enables authorized users to establish PSM-mediated connections to those target devices while retaining the security controls associated with PSM. Therefore, *PSM connections to target devices that are not managed by CyberArk* is a core Ad-Hoc Access use case.

Because these sessions traverse PSM, they can be captured as audit evidence. *Session Recording* is consequently available, and authorized personnel can use *Real-time live session monitoring* to observe an active connection as it occurs. Ad-Hoc Access is also designed to support direct workflows from a user's terminal or native client: *PSM connections from a terminal without the need to login to the PVWA* is supported through the Secure Connect/Ad-Hoc Access connection flow. This allows organizations to apply centralized session isolation, recording, and oversight without requiring every target or access workflow to begin in the PVWA interface. See CyberArk's Secure Connect documentation and its Privileged Session Manager documentation for the related session-control capabilities.

QUESTION NO: 15

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 Password Vault Web Access (PVWA)

ANSWER: A B C D

Explanation:

Ad-Hoc Access, previously called Secure Connect, extends Privileged Session Manager capabilities to connections for target devices whose accounts and credentials are not necessarily onboarded or managed in the CyberArk Vault. A user can supply the destination details when initiating the connection, while the session is still brokered through PSM. This preserves the security and governance controls associated with PSM for otherwise unmanaged target access.

Because the connection is handled by PSM, the session can be recorded and retained for audit and investigation according to the organization's PSM recording and retention policies. Authorized personnel can also use the live monitoring capabilities available through CyberArk's session-management workflow to observe an active session in real time. Ad-Hoc Access additionally supports initiating a PSM connection directly from a terminal or supported client workflow, rather than requiring the user to first sign in to the Password Vault Web Access interface. Together, these capabilities make it possible to broker, monitor, and audit temporary or unmanaged remote access while maintaining a consistent privileged-session control point. See CyberArk's Ad-Hoc Access documentation and its privileged session monitoring documentation.

QUESTION NO: 16

Which file is used to configure new firewall rules on the Vault?

A. firewall.ini

B. PARagent.ini

C. dbparm.ini

D. padr.ini

ANSWER: C

Explanation:

dbparm.ini is the Vault configuration file used to define and maintain Vault firewall rules. CyberArk uses the Vault's internal firewall controls to restrict which source IP addresses or network ranges can communicate with Vault services. Administrators configure these rules in the DBParm.ini file on the Vault server, using the relevant firewall-rule configuration entries and permitted ports. This makes the configuration part of the Vault's controlled runtime settings rather than relying solely on the operating system firewall.

After updating the file, the change must be applied according to the documented Vault administration procedure, which can include reloading the configuration or restarting the appropriate Vault service. Firewall changes should be planned carefully so that required CyberArk components, administrators, disaster-recovery communication, and approved application traffic retain connectivity. CyberArk's Vault implementation guidance identifies DBParm.ini as the location for Vault firewall configuration and describes the syntax and operational considerations for defining the rules. See the CyberArk documentation for configuring the Vault firewall and the Vault configuration files.

QUESTION NO: 17

Which keys are required to be present in order to start the PrivateArk Server Service?

A. Server Key

B. Recovery Public Key

C. Recovery Private Key

D. Safe Key

ANSWER: A

Explanation:

The **Server Key** must be present for the PrivateArk Server Service to start. This key is a fundamental component of the Digital Vault's cryptographic configuration. The PrivateArk Server uses it to access and process protected Vault data, including data encrypted within the Vault database and configuration required for normal Vault operation. During startup, the service must be able to locate and use the Server Key; without it, the Vault cannot establish the cryptographic capability needed to safely open its protected data stores and continue initialization.

CyberArk's security architecture is designed so that critical Vault contents remain unusable without the corresponding cryptographic material. Consequently, protecting the Server Key, maintaining a secure backup according to the organization's key-management procedures, and ensuring it is available on the Vault server after recovery or migration are essential operational requirements. The Server Key should be handled only through approved CyberArk administration and recovery procedures, because its confidentiality directly protects the Vault's stored privileged credentials and other sensitive records.

For CyberArk product and operational documentation, see the CyberArk Documentation Portal and CyberArk's Privileged Access Management resources.

QUESTION NO: 18

A Simple Mail Transfer Protocol (SMTP) integration allows you to forward audit records to a monitoring solution.

A. TRUE

B. FALSE

ANSWER: B

Explanation:

FALSE is correct. In CyberArk, SMTP integration is intended for email delivery, such as sending notifications and alert messages to designated recipients. It is not the integration mechanism used to export audit records to a monitoring platform. Audit-event forwarding for external monitoring, logging, and SIEM consumption is performed through CyberArk's Syslog/SIEM integration capabilities. Syslog provides a standardized event-forwarding channel that monitoring solutions can ingest, correlate, retain, and alert on. This distinction is important operationally: email is a human-readable notification method, whereas audit forwarding requires structured security-event transmission to a centralized monitoring service. When configuring CyberArk audit visibility in a SIEM or similar monitoring solution, use the documented Syslog integration and ensure the receiving system is configured to accept and parse the relevant CyberArk messages. CyberArk documentation describes forwarding audit records to SIEM systems through Syslog integration and separately documents email notification capabilities. See the CyberArk SIEM integration documentation and the CyberArk notifications documentation.

QUESTION NO: 19

What conditions must be met in order to log into the vault as the Master user? (Choose all that apply.)

A. Logon must be originated from the console of the Vault Server or an EmergencyStation defined in DBParm.ini

B. User must provide the correct master password.

C. Logon requires the Recovery Private Key to be accessible to the vault.

D. Logon must satisfy a challenge response request.

ANSWER: A B

Explanation:

The Master user is a built-in, highly privileged emergency administrative account for the CyberArk Vault. To reduce the risk of remote misuse, a Master-user logon is permitted only when the connection originates locally from the Vault Server console or from a workstation specifically configured as an EmergencyStation in the Vault's DBParm.ini configuration. This location restriction is a core protection for the account and is intended to ensure that use of Master access occurs through a controlled emergency-access path.

The person logging on must also enter the correct Master password. CyberArk uses this password to authenticate the Master user during the Vault logon process. These two conditions work together: the session must originate from an authorized emergency location and the Master credentials must be supplied correctly. Administrators should protect and manage this password under the organization's emergency-access procedures, because the Master user can be required for exceptional recovery and administration tasks.

CyberArk's documentation describes the Master user and the restricted locations from which it can access the Vault. See the CyberArk PAM Self-Hosted documentation on initial administrative accounts and the CyberArk emergency access documentation.

QUESTION NO: 20

Which of the following are secure options for storing the contents of the Operator CD. while still allowing the contents to be accessible upon a planned Vault restart? Choose alt that apply

A. Store the CD in a physical safe and mount the CD every time vault maintenance is performed.

B. Copy the contents of the CD to the System Safe on the vault

C. Copy the contents of the CD to a folder on the vault server and secure it with NTFS permissions.

D. Store the server key in a Hardware Security Module.

E. Store the server key in the Provider cache

ANSWER: A C D

Explanation:

The Operator CD contains sensitive Vault key material that is required when the Vault is started in a mode that needs operator-supplied key access. It must therefore be protected from unauthorized access while remaining available through an approved operational procedure for a planned restart. "Store the CD in a physical safe and mount the CD every time vault maintenance is performed." provides offline, physically controlled custody and makes use of the key material an explicit, auditable maintenance action. "Copy the contents of the CD to a folder on the vault server and secure it with NTFS permissions." can also support planned recovery when the folder is tightly restricted to the appropriate Vault service and authorized administrative identities, with the server itself protected under the organization's hardening and access-control standards. "Store the server key in a Hardware Security Module." is a secure alternative because an HSM protects key material in dedicated cryptographic hardware and can make the key available to the authorized Vault process without exposing the private key as ordinary file-based data. These approaches balance key protection with the operational requirement to restart the Vault. See CyberArk's Vault installation documentation and Privileged Access Security architecture resources.

QUESTION NO: 21

The Vault can only integrate with a single Security Information and Event Management (SIEM) or SYSLOG server.

A. True

B. False

ANSWER: B

Explanation:

False is correct because CyberArk Vault auditing can be sent to more than one external SIEM or Syslog destination. In the Vault's SIEM integration configuration, administrators can define multiple SIEM applications and associate each application with the relevant Syslog server details. This enables the same Vault audit information to be forwarded to separate monitoring platforms or collectors, such as an enterprise SIEM and an additional centralized logging or security-operations destination.

This capability is important where organizations operate multiple security-monitoring environments, need distinct destinations for regional or business-unit logging, or require parallel forwarding for operational monitoring and compliance retention. The Vault produces audit records for security-relevant activity, and the SIEM integration settings determine the external systems that receive those records; they are not restricted to a single server. Configuration should still be planned carefully so the selected destinations, network connectivity, Syslog protocol settings, and event handling meet the organization's monitoring and retention requirements.

CyberArk documents the ability to integrate the Vault with SIEM applications and configure the associated Syslog details in its Vault SIEM integration documentation. Additional product documentation is available through the CyberArk Documentation portal.

QUESTION NO: 22

Which of the following PTA detections are included in the Core PAS offering? (Choose all that apply.)

A. Suspected Credential Theft

B. Over-Pass-The-Hash

C. Golden Ticket

D. Unmanaged Privileged Access

ANSWER: A B

Explanation:

Suspected Credential Theft and **Over-Pass-The-Hash** are the Privileged Threat Analytics detections provided with the Core Privileged Access Security offering. Suspected Credential Theft identifies activity patterns that indicate a privileged credential may have been exposed or stolen, enabling security teams to investigate potentially compromised privileged identities quickly. This detection supports the core PAM objective of reducing the opportunity for attackers to reuse privileged credentials after compromise.

Over-Pass-The-Hash identifies attempts to use an NTLM credential hash to obtain Kerberos authentication material and then authenticate using that Kerberos context. This technique can allow an attacker to move through an environment without possessing the account's plaintext password. Detecting it is especially important for protecting privileged accounts because the technique is commonly associated with credential abuse and lateral movement. CyberArk's PAM platform combines privileged-access controls with threat detection to identify suspicious use of privileged credentials and sessions. See the CyberArk Privileged Access Manager overview and the CyberArk documentation portal for product and documentation resources.

QUESTION NO: 23

For an account attached to a platform that requires Dual Control based on a Master Policy exception, how would you configure access a password without approval

A. Create an exception to the Master Policy to exclude the group from the workflow process.

B. Edit 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:

Grant the group the **Access safe without confirmation** authorization on the Safe that contains the account. In CyberArk Privilege Cloud and PAM self-hosted environments, Dual Control requires an authorized requester to obtain confirmation from a designated confirmer before the password can be retrieved or used. The Safe-level *Access Safe without Confirmation* permission is specifically designed to exempt selected Safe members from that confirmation requirement. This lets the designated group retrieve passwords from accounts in that Safe without submitting an approval request, while the platform's Dual Control configuration remains in place for other users who do not hold the exemption. Because this is a Safe member authorization, it can be assigned precisely to the required group and applies in the context of that Safe, supporting controlled exception handling without broadly changing the Master Policy or the platform configuration. CyberArk documents Safe member permissions, including the authorization used to access a Safe without confirmation, in its Safe authorization guidance: CyberArk Safe Member Authorizations. For the broader policy context governing confirmation workflows, see CyberArk Master Policy.

QUESTION NO: 24

Which 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 CPM to a target system

D. To allow the use of additional passwords within a password management process

ANSWER: B

Explanation:

The purpose of linked accounts is to synchronize password-management activity for accounts that share a password. CyberArk designates one account as the original account and associates the related accounts with it. When the CPM changes the password for the original account, it updates the linked accounts as part of the same operation so that all associated accounts continue to use the synchronized credential. This is particularly useful where a single credential is used across multiple target systems or services and administrators need to avoid separate, inconsistent password-change operations.

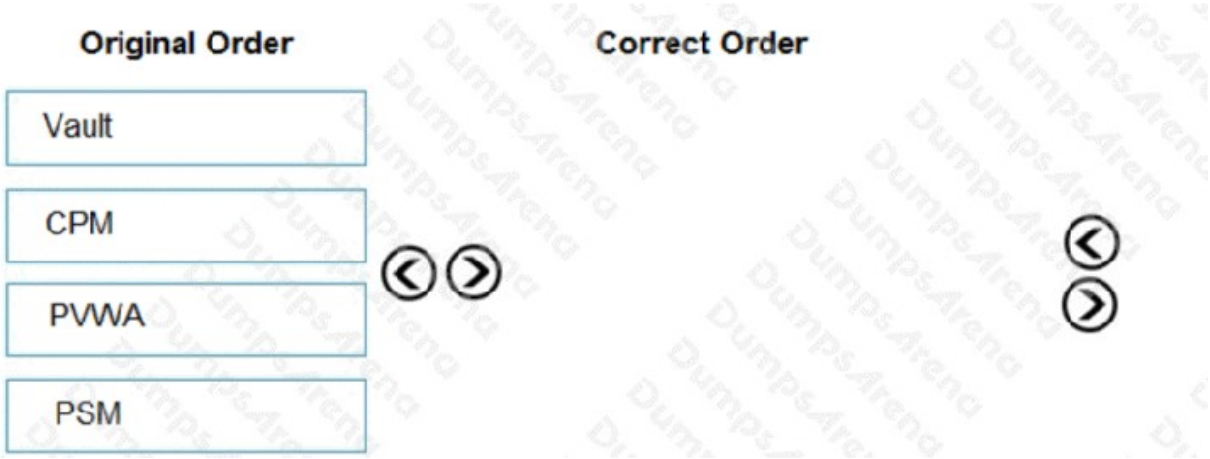
Therefore, *To ensure a particular set of accounts all change at the same time* correctly expresses the operational purpose of the linked-account capability. The linked-account relationship lets CyberArk manage the shared password consistently and reduces the administrative effort of maintaining the same credential independently in multiple account objects. CyberArk documents that linked accounts enable management of multiple accounts that use the same password, with password changes propagated from the original account to its linked accounts. See the CyberArk documentation on linked accounts and the account-management capabilities.

QUESTION NO: 25 - (DRAG DROP)

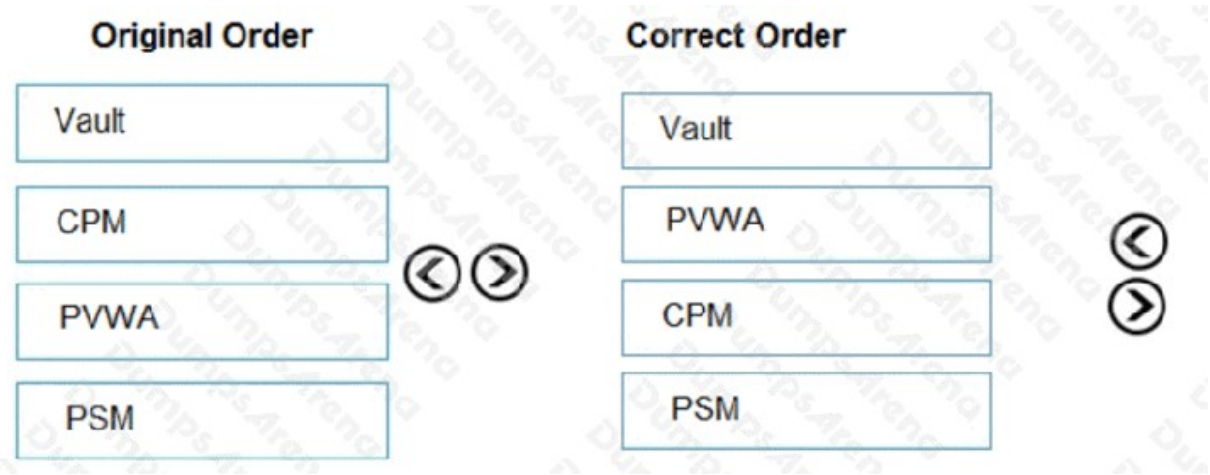
DRAG DROP

In version 10.7 the correct order of installation for components changed. Make the necessary corrections to the

list below to show the new installation order.
Select and Place:



ANSWER:



Explanation:

The required installation sequence is Vault, PVWA, CPM, and PSM. The Vault is installed first because it is the secure repository and core service on which the other Privileged Access Security components depend. It stores privileged-account data, safes, platform configuration, policies, and the credentials used by the remaining components to establish trusted communication.

PVWA is installed next. It provides the web-based management interface through which administrators and authorized users access the Vault, manage safes and accounts, submit requests, and perform administrative configuration. In the version 10.7 installation sequence, placing PVWA before CPM ensures that the web access layer is available before the password-management component is brought online and configured for operational use.

CPM follows PVWA. CPM is responsible for managing, verifying, and changing passwords according to the platform and policy settings stored in the Vault. Once the Vault and administrative interface are available, CPM can be installed, registered, and configured to process the privileged accounts it manages.

PSM is installed last. PSM uses the established Vault configuration and provides isolated, monitored session access to target systems. Installing it after the core repository, web interface, and credential-management services supports a clean configuration of connection components, session policies, and recordings. CyberArk documentation for Privileged Access Manager installation and component planning is available from the CyberArk PAM Self-Hosted installation documentation.

QUESTION NO: 26

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 UnixAdmms 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 OperationsStaff 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

OperationsManagers The members of OperationsManagers never need to be able to use the show, copy or connect buttons themselves.

Which safe permissions do you need to grant to UnixAdmins? Check all that apply

A. Use Accounts

B. Retrieve Accounts

C. List Accounts

D. Authorize Password Requests

E. Access Safe without Authorization

ANSWER: A B C E

Explanation:

The UnixAdmins group requires **Use Accounts**, **Retrieve Accounts**, **List Accounts**, and **Access Safe without Authorization**. CyberArk separates account visibility, credential retrieval, session use, and workflow bypass into distinct Safe-member permissions. **List Accounts** lets users see and locate the accounts in the UnixRoot Safe. **Retrieve Accounts** permits retrieval of the stored password value, which supports the Show and Copy actions. **Use Accounts** permits use of an account through a connection workflow, including Connect actions where the relevant platform and connection components are configured.

Because dual control is enabled for some accounts, UnixAdmins also need **Access Safe without Authorization**. This permission allows the group to retrieve or use accounts subject to dual control without waiting for an authorizer's confirmation, satisfying the requirement that they can act at any time. The authorization capability belongs with the personnel who approve emergency requests, not with the UnixAdmins group that must bypass approval. CyberArk documents Safe-member permissions and their role in controlling account listing, retrieval, use, and authorization workflows in its Managing Safe Members documentation and its accessing accounts documentation.

QUESTION NO: 27

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

A. True

B. False

ANSWER: A

Explanation:

True is correct. In a CyberArk Privileged Access Security self-hosted deployment, the Vault license is managed through the System Safe. A Vault administrator updates the license by obtaining the new CyberArk license file and uploading it into the System Safe using an authorized Vault administration connection, such as the PrivateArk Client. The Vault monitors the designated license file in that Safe and applies the updated licensing information, including the licensed components and capacity reflected in the replacement license.

This approach keeps the license update under Vault access controls and auditing rather than requiring a manual replacement of an operating-system file on the Vault server. The administrator performing the action must have the appropriate authorization to access and manage the System Safe. After the file is uploaded, it is important to confirm that the new license is recognized and that the licensed environment remains compliant with the organization's CyberArk entitlement. CyberArk's Vault installation and administration documentation describes license management as an administrative task involving the System Safe and the supplied license file. See the CyberArk documentation for managing the Vault license and the CyberArk knowledge-base reference.

QUESTION NO: 28

What are the functions of the Remote Control Agent service? (Choose all that apply.)

A. Allows remote monitoring of the Vault

B. Sends SNMP traps from the Vault

C. Maintains audit data

D. Allows CyberArk Services to be managed (start/stop/status) remotely

ANSWER: A B D

Explanation:

The Remote Control Agent is a Vault-side service that supports centralized operational monitoring and administration without requiring an administrator to interact directly with the Vault console. “Allows remote monitoring of the Vault” is correct because the agent exposes Vault health and status information to authorized remote-management tooling, helping administrators identify operational conditions and monitor the Vault from a separate management workstation. “Allows CyberArk Services to be managed (start/stop/status) remotely” is also a core function: authorized operators can use the remote-control capability to query service state and perform supported service-control actions, which is useful for controlled maintenance and recovery operations. “Sends SNMP traps from the Vault” is correct because the Remote Control Agent integrates Vault events with enterprise monitoring systems through SNMP notifications. This lets an organization route significant Vault operational alerts into its established network-management and incident-response workflows. These functions are designed for secure, authorized administration and monitoring of the Vault environment. CyberArk describes the Remote Control Agent and its remote monitoring and service-management role in its Remote Control Agent documentation. Additional Vault administration guidance is available in the CyberArk Privileged Access Security installation documentation.

QUESTION NO: 29

Name two ways of viewing the ITAlog:

A. Log into the vault locally and navigate to the Server folder under the PrivateArk install location.

B. Log into the PVWA and go to the Reports tab.

C. Access the System Safe from the PrivateArk client.

D. Go to the Thirdpary log directory on the CPM

ANSWER: A C

Explanation:

The ITAlog can be viewed directly on the Vault server and through the PrivateArk Client. When access to the Vault server is available, the log is stored in the Server folder beneath the PrivateArk installation directory, allowing an authorized administrator to open and review it locally. This method is useful for direct Vault-side troubleshooting, including situations where access through other management interfaces may not be available.

The same log is also available as an object in the System Safe. An authorized user can open the System Safe in the PrivateArk Client and access the ITAlog there. The System Safe is the Vault location used to store system-level data and logs, providing a controlled, audited means of viewing this information through the client. Both methods therefore provide valid paths to the same Vault log: one through the server file location and one through the System Safe interface. CyberArk’s documentation for Vault administration and log collection provides the relevant operational context for reviewing Vault-side logs: CyberArk Vault Server Logs documentation and CyberArk System Safe documentation.

QUESTION NO: 30

What is the primary purpose of Exclusive Accounts?

A. Reduced risk of credential theft

B. More frequent password changes

C. Non-repudiation (individual accountability)

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

ANSWER: C

Explanation:

Non-repudiation (individual accountability) is the primary purpose of CyberArk Exclusive Accounts. A shared privileged account can otherwise be used by more than one authorized person, making it difficult to establish with certainty which individual performed actions during a particular session. When an account is configured as exclusive, CyberArk reserves it for one user at a time and associates the use of that privileged credential with the requesting user. This creates a clear, attributable chain between the individual's authenticated identity, the account checkout or connection, and the recorded session activity.

That accountability is particularly important for highly sensitive administrative, emergency, and shared service credentials. CyberArk can enforce exclusive use for the duration of the access request and rotate the password after the account is released, helping ensure that another user cannot subsequently use the same known credential during that access period. The resulting audit trail supports investigations, compliance evidence, and the ability to hold an individual accountable for privileged actions. CyberArk documents Exclusive Accounts as a mechanism for ensuring that only one user can access an account at a time and for supporting individual accountability. See CyberArk documentation on Exclusive Accounts and CyberArk Privileged Access Management resources.

QUESTION NO: 31 - (SIMULATION)

In version 10.7 the correct order of installation for components changed. Make the necessary corrections to the list below to show the new installation order.

Select and Place:

ANSWER: Check the explanation for the answer

Explanation:

Place the components in this order:

1. **Digital Vault**
2. **Central Policy Manager (CPM)**
3. **Password Vault Web Access (PVWA)**
4. **Privileged Session Manager (PSM)**

Version 10.7 changed the recommended sequence so that the **CPM is installed before the PVWA**. The Vault must always be installed first because it provides the underlying secure storage and component users/configuration required by the other components.

If a DR Vault is included among the selectable items, deploy it immediately after the primary Digital Vault, before the CPM.