PassQueen
a.k.a dumpsqueen.com

CyberArk Defender - PAM

CyberArk PAM-DEF

Version Demo

Total Demo Questions: 29

Total Premium Questions: 293

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

Which dependent accounts does the CPM support out-of-the-box? (Choose three.)

A. Solaris Configuration file

B. Windows Services

C. Windows Scheduled Tasks

D. Windows DCOM Applications

E. Windows Registry

F. Key Tab file

ANSWER: B C E

Explanation:

CPM supports the built-in dependent-account types **Windows Services**, **Windows Scheduled Tasks**, and **Windows Registry**. A dependent account represents an application, configuration location, or system component that uses the password of a related target account. When CPM changes the password of that target account, it also updates the associated dependent-account instances so the resource continues to authenticate with the new credential. This synchronization is essential for preserving availability after automated password management: a service can continue to start, a scheduled task can continue to run under its configured identity, and a registry value that stores the credential can remain aligned with the managed account password. These types are provided as standard CPM support rather than requiring a separately developed custom dependent-account plug-in. The wording “Windows Scheduled Tasks” is the official resource type; “Windows Scheduled” is incomplete but clearly refers to that supported dependent-account type. CyberArk’s dependent-account documentation describes how related accounts are updated as part of CPM password-management activity and identifies the supported dependent-account implementations. See CyberArk Docs: Dependent accounts and CyberArk Docs: Manage dependent accounts.

QUESTION NO: 2 - (SIMULATION)

Arrange the steps to restore a Vault using PARestore for a Backup in the correct sequence.

ANSWER: Check the explanation for the answer

Explanation:

Arrange the full Vault restore steps in this order:

The backup-file deletion setting is first disabled so the files required for recovery are retained. Run PARestore for the full Vault restore, recover the backup files, restore the database, and then return `BackupFilesDeletion` to its normal configured value.

Reference: CyberArk documentation — Restoring Safes or the Vault

QUESTION NO: 3

A user needs to view recorded sessions through the PVWA.

Without giving auditor access, which safes does a user need access to view PSM recordings? (Choose two.)

A. Recordings safe

B. Safe the account is in

C. System safe

D. PVWAConfiguration safe

E. VaultInternal safe

ANSWER: A B

Explanation:

To view a PSM recording in the PVWA without using the Auditor role, the user requires authorization related both to the recorded account and to the recording object itself. Access to the safe that contains the privileged account establishes the user's entitlement to the account whose session was recorded. This allows PVWA to present the applicable account and its session information in the user's authorized scope. Access to the Recordings safe provides the required permission to retrieve and play the session recording that PSM stored for that session. Together, these permissions let an appropriately authorized user locate the session through the account context and open its video or text recording, without granting broad auditor-level visibility across recordings. Permissions should be assigned according to least privilege: grant only the required safe memberships and recording-related permissions for the accounts and recordings the user is expected to review. CyberArk documents that PSM records privileged sessions and makes recordings available for review through the PVWA, while access is controlled through Vault safe authorization and role permissions. See the CyberArk PSM documentation and the CyberArk Safes documentation.

QUESTION NO: 4

Which controls can be configured for an individual Vault user? Choose all that apply.

A. Allowed interfaces

B. Logon hours

C. User expiration date

D. Password complexity for managed accounts

E. PSM connection component source code

ANSWER: A B C

Explanation:

Vault user properties can be configured to restrict the user's **allowed interfaces**, define permitted **logon hours**, and specify a user **expiration date**. These controls provide additional restrictions beyond Safe membership and permissions. For example, a user can be limited to PVWA access, prevented from authenticating outside approved working hours, or disabled automatically after a defined date.

Password complexity is not configured as an individual Vault user property. Password composition requirements for managed accounts are defined through the applicable platform password policy. See the CyberArk user management documentation.

QUESTION NO: 5

Members of which built-in Vault group are used by the Central Policy Manager to manage passwords?

A. Password Managers

B. Auditors

C. Security Operators

D. Backup Users

ANSWER: A

Explanation:

Password Managers is correct. The CPM uses a Vault user that is a member of the Password Managers built-in group to perform password-management operations on accounts in Safes where it has been granted the required permissions.

Membership in this group identifies the user as a password-management component user. The CPM user must also be added to the relevant account Safes with the permissions needed to retrieve and update account information during verification, change, and reconciliation operations. See the CyberArk built-in Vault groups documentation.

QUESTION NO: 6

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

A. PSM (i.e., launching connections by clicking on the connect button in the Password Vault Web Access (PVWA)

B. PSM for Windows (previously known as RDP Proxy)

C. PSM for SSH (previously known as PSM-SSH Proxy)

D. All of the above

ANSWER: D

Explanation:

All of the above is correct because CyberArk provides live session monitoring capabilities across its PSM connection methods. Authorized users can use the PVWA active-sessions interface to locate an in-progress privileged session and monitor it in real time, subject to the organization's permissions and applicable session configuration. This capability enables security personnel to oversee sensitive activity while it occurs, respond quickly to suspicious behavior, and maintain accountability for privileged access.

Sessions launched through the standard PSM workflow from the PVWA Connect button can be monitored live. CyberArk also supports live monitoring for RDP-based sessions handled through PSM for Windows and for SSH-based sessions handled through PSM for SSH. The live-monitoring function is part of CyberArk's broader session-management controls, which also include recording and audit evidence for privileged sessions. Access to session monitoring should be tightly governed through Safe and role permissions so that only appropriately authorized personnel can view active privileged activity. CyberArk's documentation describes monitoring active PSM sessions through PVWA and the session-management capabilities of its PSM components. See the CyberArk documentation for monitoring privileged sessions and the Privileged Session Manager overview.

QUESTION NO: 7 - (DRAG DROP)

Match each key to its recommended storage location.

ANSWER:

Explanation:

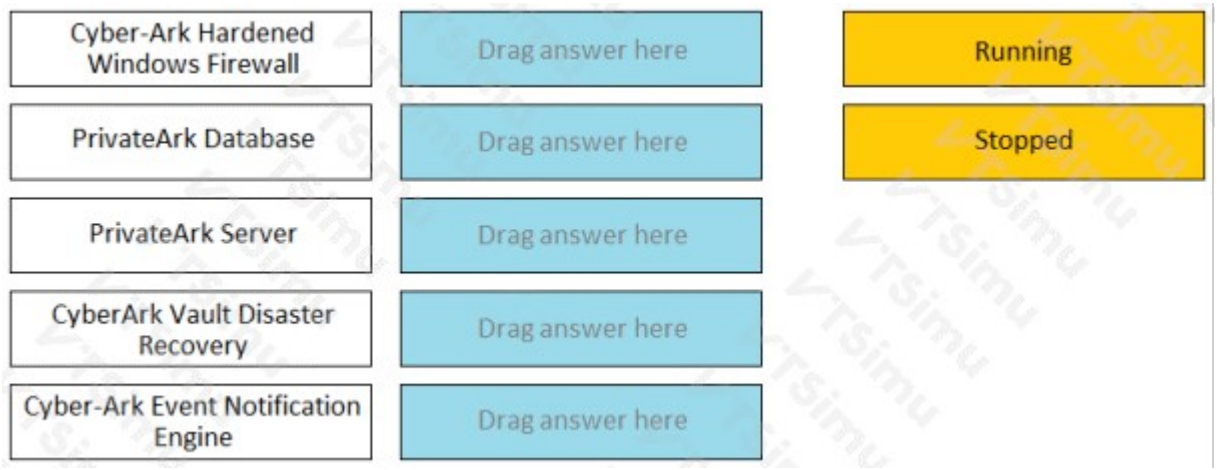
CyberArk separates these keys according to both their cryptographic purpose and the level of protection required for the information they hold. The Recovery Private Key is the highly sensitive offline component needed for recovery operations, so it belongs in a physical safe. Keeping it physically secured and separate from the Vault infrastructure preserves the recovery process as an out-of-band control.

The Recovery Public Key is used by the Vault-side recovery-key mechanism and is kept on the Vault Server disk drive. A public key is intended to be available to the system component that needs to use it, while the corresponding private key remains protected offline. The Server Key is stored in the Vault because it is a core Vault cryptographic asset and must be protected through the Vault's own security controls and access model.

SSH Keys are private authentication credentials and should be protected by a hardware security module. An HSM provides hardware-backed protection for cryptographic key material and can prevent private key material from being exposed in normal software storage. This allocation supports CyberArk's layered approach: offline recovery protection for the recovery private key, local availability for the recovery public key, Vault protection for the server key, and hardware-backed custody for SSH keys. CyberArk's Server Keys documentation describes the recovery-key and server-key storage model in more detail: CyberArk Server Keys documentation.

QUESTION NO: 8 - (DRAG DROP)

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



ANSWER:

Explanation:

A DR Vault in normal Replication mode is maintained as a passive, synchronized recovery environment while the production Vault continues to provide the active Vault service. Its service state therefore reflects two goals: keep the DR infrastructure able to receive replicated data, and avoid running components that would actively process Vault activity as though the DR environment were the production system.

The Cyber-Ark Hardened Windows Firewall is Running because the DR Vault must maintain the protected communications required for the Vault environment and replication traffic. PrivateArk Server is also Running, providing the core Vault server capability needed by the DR configuration. PrivateArk Database is Stopped in this normal DR replication state, consistent with the replicated database being managed as the passive copy rather than an independently active production database.

Most importantly, CyberArk Vault Disaster Recovery is Running. This is the service responsible for the DR replication role, so it must remain active while the DR Vault is continuously synchronized and ready for a controlled failover. Cyber-Ark Event Notification Engine is Stopped on the DR Vault during replication mode. Keeping notification processing inactive supports the passive role of the recovery Vault until it is promoted for recovery operations.

This combination—firewall running, PrivateArk Server running, PrivateArk Database stopped, Disaster Recovery running, and Event Notification Engine stopped—represents the expected normal service posture for a DR Vault that is replicating successfully. CyberArk documentation and product resources are available through the CyberArk Documentation portal.

QUESTION NO: 9

Which of the Following can be configured in the Master Poky? Choose all that apply.

A. Dual Control

B. One Time Passwords

C. Exclusive Passwords

D. Password Reconciliation
Ticketing Integration

E. Required Properties

F. Custom Connection Components

G. Password Aging Rules

ANSWER: A B C G

Explanation:

CyberArk's Master Policy defines organization-wide controls governing how privileged-account passwords are accessed and managed. **Dual Control** can be enabled to require an authorized request and approval workflow before a user retrieves or uses a password. **One Time Passwords** can be configured so that a password is changed after it is retrieved, limiting the usefulness of a previously disclosed credential. **Exclusive Passwords** can be configured to reserve an account for a single user during a defined access period, preventing concurrent use by other authorized users. **Password Aging Rules** are also controlled through the Master Policy to govern password expiration and the required frequency of password replacement. These settings establish baseline security behavior across the Vault; more specific account or platform configuration can supplement them where applicable. CyberArk documents the Master Policy as the central location for configuring password access controls and password-management behavior, including dual control, exclusive access, one-time passwords, and password aging. See the CyberArk Master Policy documentation and the password access-control configuration guidance.

QUESTION NO: 10

Which of the following PTA detections are included in the Core PAS offering?

A. Suspected Credential Theft

B. Over-Pass-The Hash

C. Golden Ticket

D. Unmanaged Privileged Access

ANSWER: D

Explanation:

Unmanaged Privileged Access is the PTA detection included with the Core PAS offering. It provides visibility when privileged credentials are used in ways that bypass the organization's expected CyberArk-managed access path. This gives security teams an important baseline control: they can identify privileged access that is occurring outside managed vaulting, credential rotation, and monitored session workflows, then investigate and bring that access under governance as appropriate. The detection supports the core PAM objective of reducing unmanaged privileged-access risk by making such activity visible rather than leaving it outside the privileged-access management program. CyberArk's Privileged Access Manager offering is designed to secure, control, monitor, and audit privileged access across the enterprise; identifying unmanaged privileged access directly supports those capabilities. See CyberArk's Privileged Access Manager overview for the Core PAM capabilities and the CyberArk documentation portal for product documentation and detection-related configuration details.

QUESTION NO: 11

You have been asked to identify the up or down status of Vault services.

Which CyberArk utility can you use to accomplish this task?

A. Vault Replicator

B. PAS Reporter

C. Remote Control Agent

D. Syslog

ANSWER: C

Explanation:

The **Remote Control Agent** is the CyberArk utility used to remotely monitor and administer Vault and Disaster Recovery Vault services. It enables an authorized administrator to connect to the Vault server and view the operational status of its CyberArk services, allowing the administrator to determine whether a service is running or stopped. This is particularly useful when direct interactive access to the Vault server is restricted, as is typical for a hardened Digital Vault deployment. The utility supports remote administrative operations through the secured Vault-management channel and is intended for operational tasks such as checking service status, starting or stopping applicable services, and collecting relevant service information. To use it, the administrator must have the appropriate Vault authorization and the Remote Control Agent must be configured and available on the target Vault environment. CyberArk documents Remote Control Agent usage as part of remote administration for the Vault and DR Vault, including monitoring and managing Vault services. See CyberArk's Remote Administration for the Vault and DR Vault documentation and the Vault monitoring documentation.

QUESTION NO: 12

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

A. Auditors

B. Vault Admin

C. DR Users

D. Operators

ANSWER: A

Explanation:

Auditors is correct. In CyberArk Privileged Access Manager, the Auditors built-in Vault group is intended for personnel who must review privileged activity for audit, compliance, investigation, or security-monitoring purposes. Its role includes access to session-monitoring capabilities, allowing authorized members to locate and review recordings of privileged sessions and, where live monitoring is enabled and permitted, monitor active sessions through the PVWA interface. This separation supports least privilege: reviewers can inspect evidence of privileged activity without being granted administrative control over the Vault or the managed accounts themselves.

In practice, the user must also be able to access the relevant Safe and have the applicable Safe authorizations for viewing or monitoring session activity. CyberArk's session-monitoring workflow lets authorized users search session data, open recorded sessions, and monitor active connections according to the organization's configured retention, access-control, and PSM policies. The Auditors group is therefore the standard group association for users whose primary responsibility is reviewing privileged-session recordings and live activity. See CyberArk's Monitor Privileged Sessions documentation and the default Vault groups documentation.

QUESTION NO: 13

Users who have the 'Access Safe without confirmation' safe permission on a safe where accounts are configured for Dual control, still need to request approval to use the account.

A. TRUE

B. FALSE

ANSWER: B

Explanation:

FALSE is correct because the *Access Safe without confirmation* Safe-member authorization allows its holder to access accounts in that Safe without obtaining a confirmation, including when Dual Control is configured for an account. In CyberArk terminology, Dual Control is implemented through account-access requests and an authorized confirmation or approval workflow. The Safe permission is an explicit exception to that confirmation requirement for the member to whom it is granted.

This permission should therefore be assigned carefully and only to users or groups that are intended to have emergency, operational, or otherwise pre-authorized access. It does not remove the account's Dual Control configuration; rather, it permits the specifically authorized Safe member to retrieve or use the account without waiting for another user to confirm the request. CyberArk administrators can still use the Safe's membership permissions, account properties, auditing, and event monitoring to control and review this access appropriately.

CyberArk documents Safe-member permissions, including *Access Safe without confirmation*, in its Safe member management documentation. The account request and confirmation workflow is described in CyberArk's Dual Control documentation.

QUESTION NO: 14

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

A. The PSM software must be instated on the target server

B. PSM must be enabled in the Master Policy (either directly, or through exception)

C. PSMConnect must be added as a local user on the target server

D. RDP must be enabled on the target server

ANSWER: A C

Explanation:

The PSM software must be instated on the target server and PSMConnect must be added as a local user on the target server are the statements that are not true. CyberArk Privileged Session Manager is deployed on a dedicated PSM server, which acts as the secure connection proxy between the user and the target system. It launches the requested protocol connection, records the session activity, and stores the recording through the CyberArk platform; it is not installed separately on every Windows server that will be accessed and recorded. This centralized architecture enables consistent session isolation, monitoring, and auditing across many target systems. The PSMConnect account is a component of the PSM host configuration and is used by PSM to establish and manage session processes on the PSM machine. It is therefore not an account that must be created locally on each target Windows server. Target-system access is instead performed using the privileged account stored in the relevant CyberArk Safe and governed by the platform, account, and connection-component configuration. CyberArk's PSM deployment guidance describes installing and configuring PSM on its designated server: CyberArk PSM installation documentation. CyberArk also documents PSM as the component that securely proxies and records privileged sessions: CyberArk Privileged Session Manager.

QUESTION NO: 15

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

A. in PVWA at the account level

B. in PVWA in the platform configuration

C. in the Master policy of the PVWA

D. at the Safe level

E. in the CPM settings

ANSWER: A B

Explanation:

in PVWA at the account level is correct because CyberArk allows a reconcile account to be associated directly with an individual managed account. This account-specific association is used when the account's password must be reconciled, such as after the CPM detects that the password in the Vault differs from the password on the target system. A reconcile account configured for the individual account takes precedence over a reconcile account defined by its platform, enabling exceptions for particular accounts that need different reconciliation credentials.

in PVWA in the platform configuration is also correct because a platform can define the default reconcile account for every account assigned to that platform. In the platform's Automatic Password Management settings, the reconcile-account safe and reconcile-account name settings identify the privileged account that CPM uses for reconciliation. This provides a centralized, consistent configuration for managed accounts using the same platform while still permitting an account-level assignment where an override is required. CyberArk documents reconciliation as part of password-management configuration and describes platform properties used to supply the reconcile account details. See the CyberArk Privileged Access Manager Self-Hosted documentation and the CyberArk guidance for reconciling passwords.

QUESTION NO: 16

Which of the Following can be configured in the Master Poky? 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

ANSWER: A B C

Explanation:

CyberArk's Master Policy provides global password-access control rules that are inherited by Safes unless a more specific configuration is applied where supported. **Dual Control** is a Master Policy access-control setting that requires an authorized owner or approver to approve a user's request before the requester can access the privileged credential. This supports separation of duties for sensitive accounts. **One Time Passwords** can also be enforced through the Master Policy, requiring CyberArk to change a password after it has been viewed or used, so that the disclosed password cannot be reused. **Exclusive Passwords** is likewise a Master Policy capability, providing exclusive access to a password for a defined period and preventing concurrent access by other users while that exclusive access is active. Together, these settings centrally enforce approval, post-use credential rotation, and controlled single-user access for privileged credentials. CyberArk documents Master Policy as the central location for defining these password access-control rules; see the CyberArk PAM Self-Hosted documentation and CyberArk's Privileged Access Management overview.

QUESTION NO: 17

A Logon Account can be specified in the Master Policy.

A. TRUE

B. FALSE

ANSWER: B

Explanation:

FALSE is correct. In CyberArk PAM, the Master Policy provides centralized, high-level controls for password-management behavior, such as whether password changes, reconciliations, verifications, and related processes are enabled. It is not the location where a specific logon account relationship is assigned. A logon account is an account-level association used when CyberArk must authenticate to a target with credentials other than those being managed. This relationship is configured for the applicable privileged account, with the relevant account and platform configuration governing how the connection and password-management process use that logon credential. Keeping the logon-account assignment at the account level allows separate target accounts to use different authentication identities while still inheriting the common controls defined centrally by the Master Policy. CyberArk's documentation describes the Master Policy as the source for global password-management settings and describes account properties as the place where account-specific information and associations are maintained. See the CyberArk Master Policy documentation and the CyberArk account properties documentation.

QUESTION NO: 18

What is the purpose of a linked account?

A. To ensure that a particular collection of accounts all have the same password.

B. To ensure a particular set of accounts all change at the same time.

C. To connect the CPNI to a target system.

D. To allow more than one account to work together as part of a password management process.

ANSWER: D

Explanation:

To allow more than one account to work together as part of a password management process is correct. In CyberArk PAM, linked accounts establish an account dependency: one account requires another account's credentials to perform a defined password-management action. For example, the CyberArk Central Policy Manager can use a linked account with the necessary administrative permissions to log on to a target system and change, verify, or reconcile the password of a dependent managed account. The linked account is therefore part of the operational workflow for managing the dependent account, rather than merely being a grouping mechanism. CyberArk supports several dependency types, such as logon accounts and reconcile accounts, so the CPM can select the appropriate credentials during the relevant process. This design enables secure, automated management where a managed account cannot independently perform its own password operation. The relationship also allows CyberArk to maintain the dependency data required for the password-management process while keeping credentials protected in the Vault. See CyberArk's official product documentation portal and the Password Management Dependencies documentation for details on configuring and using account dependencies.

QUESTION NO: 19

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

A. an account stored in the Vault

B. an account specified by the user

C. the Vault Administrator

D. any user with Auditor membership

E. the PasswordManager user

ANSWER: A B

Explanation:

The correct selections are *an account stored in the Vault* and *an account specified by the user*. Windows account discovery needs credentials that can authenticate to the target Windows machines and enumerate local or domain accounts, services, scheduled tasks, and related dependencies. A credential already stored in the Vault can be selected so that the discovery configuration uses a centrally protected, managed privileged account without exposing its password to the operator. This supports the PAM principle that credentials used for discovery should themselves be secured and auditable.

CyberArk also permits an operator to specify an account for the discovery operation. This accommodates environments in which a suitable credential has not yet been onboarded, or where a particular Windows credential is required for a defined discovery scope. The supplied account must have the Windows permissions necessary to connect to and inspect the targeted systems. In both cases, the selected account provides the authentication context for the discovery scan; the scan then identifies candidate privileged accounts and dependencies that may need to be onboarded and managed. CyberArk's account-discovery documentation and product documentation are available at CyberArk Documentation and CyberArk Privileged Access Management.

QUESTION NO: 20

You have been given the requirement that certain accounts cannot have their passwords updated during business hours.

How can you set up a configuration to meet this requirement?

A. Change settings on the CPM configuration safe so that access is permitted after business hours only.

B. Update the password change parameters of the platform to match the permitted time frame.

C. Disable automatic CPM management for all accounts that are assigned to this platform.

D. Add an exception to the Master Policy to allow the action for this platform during the permitted time.

ANSWER: B

Explanation:

Update the password change parameters of the platform to match the permitted time frame. In CyberArk PAM, a platform defines the CPM management behavior for accounts associated with that platform, including the policy and timing controls used when CPM performs password-management operations. Configuring the password-change time window at the platform level lets the organization define the hours during which automatic password changes are allowed. For accounts that use this platform, CPM then schedules password changes only within that approved window, such as evenings or other non-business hours. This is the appropriate scope because the requirement applies to a defined set of accounts, and platform assignment is the standard way to apply common management behavior consistently to those accounts. The configuration can therefore protect business-hour availability while retaining automated CPM password management, periodic rotation, and compliance controls. Administrators should ensure that the allowed window is sufficiently long for CPM processing and aligns with the organization's maintenance schedule and target-system availability. CyberArk documents CPM as the component responsible for automatically managing and changing privileged-account passwords, while platform settings provide the policy framework CPM uses for those managed accounts. See the CyberArk CPM documentation and the CyberArk platform documentation.

QUESTION NO: 21

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

A. PACli.ini

B. Vault.ini

C. conf.ini

D. A comma delimited upload file

ANSWER: B C D

Explanation:

The Password Upload Utility requires a configured **Vault.ini** file, a configured **conf.ini** file, and a comma-delimited upload file. Vault.ini provides the connection information that enables the utility to locate and communicate with the CyberArk Digital Vault. The utility must have this connectivity information before it can authenticate and create accounts or upload credentials. The conf.ini file defines how the utility processes the upload data, including the relevant safe, platform, account-property, and column-mapping settings. It therefore connects the fields in the input data to the properties required for the accounts being created. Finally, the comma-delimited upload file supplies the actual account records and credential information that the utility imports. The input file must conform to the structure and mappings defined in conf.ini. Together, these files provide the Vault connection settings, upload-processing configuration, and account data needed for a successful bulk upload. CyberArk documents the Password Upload Utility as a legacy account-onboarding method and recommends reviewing its account onboarding guidance when planning bulk account creation: CyberArk Password Upload Utility documentation and CyberArk account onboarding documentation.

QUESTION NO: 22

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

A. Safe Name

B. Platform ID

C. All required properties specified in the Platform

D. Username

E. Address

F. Hostname

ANSWER: A B C

Explanation:

When accounts are imported from a file into CyberArk Privilege Cloud or PVWA, **Safe Name** is mandatory because it identifies the target Safe in which CyberArk will create and store each account. **Platform ID** is also mandatory because it associates the account with the platform that defines how the account is managed, including the applicable password-management and verification settings. In addition, the import file must include **all required properties specified in the Platform**. Platform configuration determines the account-property requirements for that account type, so the file must supply every property that the selected platform requires before the account can be created successfully. This allows a single import mechanism to support different managed system types while maintaining the required account metadata and management behavior. The CSV file headings must match the corresponding CyberArk account-property names, and the values must satisfy the requirements configured for the selected platform. For the documented file-import procedure and required account details, see CyberArk documentation: Add multiple accounts. Additional information about account properties and platform-driven account management is available in the CyberArk Accounts documentation.

QUESTION NO: 23

Which statements about a CyberArk Vault Disaster Recovery environment are true? Choose all that apply.

A. The DR Vault maintains a replicated copy of primary Vault data.

B. The PrivateArk Disaster Recovery service performs replication.

C. The DR Vault can be activated when the primary Vault is unavailable.

D. A DR Vault removes the need for regular Vault backups.

E. The DR Vault is used to record all PSM sessions.

ANSWER: A B C

Explanation:

A Disaster Recovery environment maintains a **replicated copy of the primary Vault data** and is intended to support recovery when the primary Vault becomes unavailable. The DR Vault is maintained by the **PrivateArk Disaster Recovery service**, which replicates data from the primary Vault. During a disaster-recovery event, the DR Vault can be activated to provide Vault availability.

The DR Vault is not a replacement for regular backups. Backups remain necessary to protect against corruption, accidental deletion, and recovery scenarios that replication alone cannot address. CyberArk documents DR architecture and activation procedures in the CyberArk Disaster Recovery documentation.

QUESTION NO: 24

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

A. REST API

B. PrivateArk Client

C. PACLI

D. PVWA

E. Active Directory

F. Sailpoint

ANSWER: A B C

Explanation:

REST API, **PrivateArk Client**, and **PACLI** can be used to manage direct Vault group membership, including assigning a user to the Vault Admin Group. The REST API supports automated administration workflows, enabling an authorized application or script to manage Vault users and group members programmatically. This is appropriate when onboarding or privileged-access administration is integrated with an approved automation process. The PrivateArk Client provides a native administrative interface for managing Vault objects, including users, groups, and group membership. An administrator can use it to locate the relevant user or group and make the direct membership assignment. PACLI provides command-line administration of Vault objects and supports scripted or operational management where a graphical client is not required. In each case, the administrator or service identity performing the change must have the required Vault-level authorization, because membership in the Vault Admin Group confers highly privileged administrative capabilities. CyberArk documents its REST interface for programmatic Vault administration in the REST APIs documentation; PACLI is documented in the PACLI documentation.

QUESTION NO: 25

A recently-hired colleague onboarded five new Local Accounts that are used for five standalone Windows Servers. After attempting to connect to the servers from PVWA, the colleague noticed that the " Connect " button was greyed out for all five new accounts.

What can you do to help your colleague resolve this issue? (Choose two.)

A. Verify that the address field is populated with an IP or FQDN of each server.

B. Verify that the correct PSM connection component appears within account platform settings.

C. Verify that the address field is blank and that the correct PSM connection component appears within account platform settings.

D. Notify the Windows Team that created the new accounts that the CyberArk PAM solution is not designed to manage local accounts on Windows Servers.

E. Verify that the " Disable automatic management for this account " setting for each account is not enabled.

ANSWER: A B

Explanation:

Verify that the address field is populated with an IP or FQDN of each server. is correct because PVWA needs a target-machine address to create a PSM connection. The Address property identifies the endpoint that the connection component must reach; if it is absent, PVWA cannot construct a valid session target and the Connect action is unavailable. For each local account, populate Address with the applicable standalone Windows server's resolvable FQDN or IP address.

Verify that the correct PSM connection component appears within account platform settings. is also correct because the PVWA Connect button is driven by PSM connection components enabled for the account's platform and available to the user. A Windows local-account platform must expose an appropriate PSM connection method, such as a supported RDP component, so that PVWA has a defined way to launch the session. Confirm the platform assignment and that the required connection component is enabled and configured for PSM use. CyberArk documentation describes configuring platform connection components and their availability for account connections in the Connection Components documentation and provides account-property guidance in the Account Properties documentation.

QUESTION NO: 26

What is the chief benefit of PSM?

A. Privileged session isolation

B. Automatic password management

C. Privileged session recording

D. 'Privileged session isolation' and 'Privileged session recording'

ANSWER: D

Explanation:

The chief benefit is *'Privileged session isolation' and 'Privileged session recording'*. CyberArk Privileged Session Manager (PSM) acts as a secure proxy between a privileged user and the target system. Rather than allowing a direct connection from the user's workstation to the managed target, PSM brokers the connection. This isolates the target environment from the endpoint used by the administrator and helps prevent exposure of privileged credentials, while allowing access to be governed by CyberArk policy.

PSM also monitors and records the activity performed during the privileged connection. The resulting recordings provide an auditable account of actions in the session, supporting security investigations, operational review, and compliance requirements. The isolation and recording capabilities work together: PSM provides controlled access to the target while creating session evidence for later review. Password management is performed by other components and capabilities in the CyberArk PAM solution, whereas PSM's core role is securing privileged access sessions through proxy-based isolation and monitoring/recording. CyberArk describes PSM as a component that enables organizations to secure, control, and monitor privileged sessions. See the CyberArk Privileged Session Manager documentation and CyberArk's Privileged Access Manager overview.

QUESTION NO: 27

You are configuring a Vault HA cluster.

Which file should you check to confirm the correct drives have been assigned for the location of the Quorum and Safes data disks?

A. ClusterVault.ini

B. my.ini

C. vault.ini

D. DBParm.ini

ANSWER: A

Explanation:

ClusterVault.ini is the Vault HA cluster configuration file that records the disk-drive assignments used by the clustered Vault. During HA implementation, each cluster node must use consistent storage definitions so that the Quorum disk and the Vault Safes data disk are identified correctly when the active Vault role changes between nodes. Checking this file lets an administrator validate that the configured drive letters or paths correspond to the intended shared disks before completing or troubleshooting cluster failover configuration.

This check is particularly important because the Quorum provides the cluster's shared arbitration and coordination storage, while the Safes data disk holds the protected Vault data. An incorrect drive assignment can prevent the Vault cluster from starting correctly or from accessing the expected shared storage after a failover. CyberArk's High Availability implementation guidance describes the clustered Vault configuration and the shared storage prerequisites that must be consistently configured across the nodes. See the CyberArk PAM Self-Hosted High Availability documentation and the CyberArk HA preparation guidance.

QUESTION NO: 28

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

A. TRUE

B. FALSE

ANSWER: B

Explanation:

FALSE is correct. In CyberArk PAM, the ability to assign Safe permissions is governed by the administrative authorization held by the user, such as the authority to manage Safe members, rather than by a requirement that the administrator personally possess every permission being assigned. A Safe owner or another user authorized to manage Safe members can add members and configure the access permissions those members receive. This delegated administration model enables organizations to separate operational administration from privileged access: for example, an administrator responsible for managing a Safe can assign an application account the permissions required for password retrieval or account management without needing to use those permissions personally.

CyberArk documents Safe member authorizations as permissions that are configured for each member of a Safe. Administrative users with the appropriate Safe-management authority can manage the membership and authorization configuration needed to support business access requirements. The relevant control is therefore the administrator's authority to manage the Safe and its members, combined with organizational governance over who receives such authority. For details, see CyberArk's Safe Member Authorizations documentation and the Safes documentation.

QUESTION NO: 29

An account has the Disable automatic management account property enabled. What is the result?

A. The CPM does not perform automatic password-management operations for the account.

B. The account is deleted from its Safe.

C. The account password is immediately reconciled.

D. The account can no longer be viewed in PVWA.

ANSWER: A

Explanation:

The CPM does not perform automatic password-management operations for the account is correct. The Disable automatic management property can be used to exclude a specific account from automatic CPM processing while retaining the account in the Vault and preserving its assigned platform and other account properties.

This setting is useful when a managed account must be temporarily excluded from scheduled password changes, verification, or reconciliation because of maintenance, an application dependency, or an approved operational exception. Administrators should review such exceptions regularly so that accounts are returned to normal password management when appropriate. See the CyberArk account properties documentation.