PassQueen
a.k.a dumpsqueen.com

CyberArk CDE Recertification

CyberArk PAM-CDE-RECERT

Version Demo

Total Demo Questions: 27

Total Premium Questions: 271

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

You need to recover an account localadmin02 for target server 10.0.123.73 stored in Safe Team1.

What do you need to recover and decrypt the object? (Choose three.)

A. Recovery Private Key

B. Recover.exe

C. Vault data

D. Recovery Public Key

E. Server Key

F. Master Password

ANSWER: A C E

Explanation:

Recovering and decrypting a Vault object requires the encrypted **Vault data** that contains the requested account object, the applicable **Server Key**, and the **Recovery Private Key**. The Vault data is the encrypted source material from which the account object is recovered. The Server Key is part of the Vault encryption hierarchy and is required to access data encrypted for the relevant Vault environment. The Recovery Private Key is used during the recovery process to decrypt the protected key material needed to make the Server Key usable. Together, these components provide both the encrypted object and the cryptographic materials necessary to restore it in a controlled recovery operation. CyberArk documents the role of Server Keys and recovery keys in its Vault key hierarchy, including the recovery process that uses the recovery private key to access protected server-key material. See the CyberArk Server Keys documentation and the Vault structure and key-management reference.

QUESTION NO: 2

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 included in the Core PAS offering. This detection is intended to identify privileged-account activity that occurs outside CyberArk's managed access path, such as use of a privileged credential that is not being brokered and controlled through the expected Privileged Access Manager workflow. Identifying this activity is important because it gives security teams visibility into potential bypasses of privileged-access controls and helps them investigate whether privileged credentials, access methods, or administrative practices require remediation.

CyberArk Privileged Threat Analytics correlates activity and risk indicators to surface suspicious privileged behavior. Within the Core PAS entitlement, the unmanaged privileged-access capability supports the foundational goal of monitoring whether privileged access is occurring through approved, governed channels. This allows organizations to prioritize investigation of privileged sessions or account usage that may not be subject to the normal vaulting, rotation, session monitoring, and audit processes expected for managed privileged access. CyberArk describes Privileged Threat Analytics as part of its privileged-

access security capabilities and documents its threat-detection functions in its product documentation. See CyberArk Privileged Access Manager and CyberArk Privileged Threat Analytics documentation.

QUESTION NO: 3

You are installing PSM for SSH with AD-Bridge in CyberArkSSHD mode for your customer. ACME Corp What do you need to install to meet your customer's needs? (Choose 2)

A. libssh

B. CARKpsmp-infra

C. CARKpsmp

D. CARKpsmp-AD Bridge

ANSWER: B C

Explanation:

For a PSM for SSH deployment operating in CyberArkSSHD mode, the required CyberArk installation components are **CARKpsmp-infra** and **CARKpsmp**. The infrastructure package must be installed first because it provides the underlying PSM for SSH infrastructure, including the CyberArk SSH daemon-related components and dependencies required by the primary PSM for SSH package. The **CARKpsmp** package then installs the PSM for SSH application itself, enabling CyberArk to proxy, isolate, and record SSH sessions through the configured PSM for SSH environment. AD Bridge is a supported identity-integration configuration for this deployment model; it does not replace the required infrastructure and core PSM for SSH packages. After package installation, the administrator completes the applicable AD Bridge integration and PSM for SSH configuration tasks so directory users can be authenticated and authorized according to the organization's CyberArk policies. CyberArk's PSM for SSH deployment documentation describes installing the infrastructure RPM before the main PSM for SSH RPM and then configuring the selected SSH deployment mode. See the CyberArk PSM for SSH deployment documentation and the PSM for SSH documentation overview.

QUESTION NO: 4

Which service should NOT be running on the DR Vault when the primary Production Vault is up?

A. PrivateArk Database

B. PrivateArk Server

C. CyberArk Vault Disaster Recovery (DR) service

D. CyberArk Logical Container

ANSWER: B

Explanation:

PrivateArk Server should not be running on the DR Vault while the primary Production Vault is available. In CyberArk's Vault disaster-recovery architecture, the DR Vault remains a standby instance while the CyberArk Vault Disaster Recovery service maintains the replicated Vault data. Keeping the PrivateArk Server service stopped prevents the standby Vault from operating as an accessible production Vault before an authorized failover has occurred. This preserves the intended active/passive design and ensures that production clients, components, and administrative activity continue to use the primary Vault as the authoritative service endpoint.

During a real disaster-recovery activation, an administrator promotes the DR Vault and starts the required Vault services as part of the controlled failover process. At that point, the formerly standby Vault can accept the operational role of the production Vault. This separation between ongoing DR replication and the active PrivateArk Server role is fundamental to maintaining a consistent, recoverable Vault environment. CyberArk's self-hosted PAM documentation includes the Vault

deployment and disaster-recovery guidance at CyberArk PAM Self-Hosted documentation and the related product documentation portal at docs.cyberark.com.

QUESTION NO: 5

Which capabilities are available when an authorized user accesses a target system through Privileged Session Manager (PSM)? Choose all that apply.

A. Isolate and proxy connections to target systems

B. Record privileged sessions

C. Monitor active sessions in real time

D. Change account passwords on managed targets

E. Assign Safe permissions to Vault users

ANSWER: A B C

Explanation:

PSM can **isolate and proxy the connection** between the user and the target system, **record the privileged session**, and enable authorized personnel to **monitor an active session in real time**. These capabilities provide oversight and auditability while reducing the need for a direct administrative connection from the user workstation to the target device.

PSM does not itself change a managed account password or grant Safe-member permissions. Password changes are performed by CPM according to the account platform, and Safe permissions are managed through Safe membership administration. See the CyberArk Privileged Session Manager documentation and Monitor Privileged Sessions documentation.

QUESTION NO: 6

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

A. Privileged Accounts Inventory

B. Privileged Accounts Compliance Status

C. Activity Log

D. Privileged Accounts CPM Status

ANSWER: B

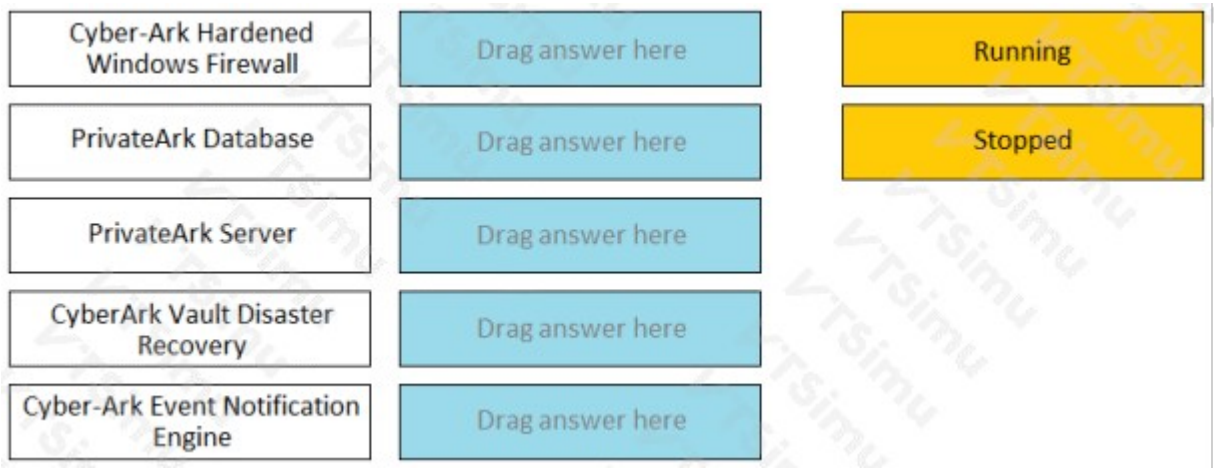
Explanation:

Privileged Accounts Compliance Status is the built-in PVWA report that provides password-compliance information for privileged accounts, including the number of days remaining before a password is due to expire. This report is intended to give administrators a consolidated view of account compliance and password-management status, making it useful for identifying credentials that need attention before their configured expiration date.

The days-to-expiration value supports operational password lifecycle management: teams can review approaching expirations, prioritize remediation, and verify that managed accounts remain aligned with organizational password policies. Because the information is presented as part of the compliance view, it helps administrators assess password status across the relevant account population rather than inspecting accounts individually. CyberArk documents the available PVWA reports and identifies the password-expiration information supplied by the Privileged Accounts Compliance Status report. See the CyberArk documentation for reports in PVWA and the CyberArk PVWA reports documentation.

QUESTION NO: 7 - (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:

When a Disaster Recovery Vault is operating normally in Replication mode, it is a passive standby Vault that continuously receives replicated Vault data from the active Primary Vault. Its service state reflects that role: the Cyber-Ark Hardened Windows Firewall is running so that the secured communications required by the Vault environment remain protected and available. The PrivateArk Server is also running, because the DR Vault must be online and able to participate in the replication arrangement.

The CyberArk Vault Disaster Recovery service is running in this mode. This is the service responsible for the DR replication activity, so it must remain active while the DR Vault is receiving and maintaining the replicated data set. CyberArk describes the Disaster Recovery solution as maintaining a synchronized standby Vault that can be activated if the primary environment is unavailable. See the CyberArk Disaster Recovery documentation for the DR Vault replication model.

Because the DR Vault has not been activated, the PrivateArk Database is stopped. The replicated Vault data is retained for standby and recovery purposes rather than being opened as the active database service. The Cyber-Ark Event Notification Engine is likewise stopped during normal passive replication operation. Event processing should occur in the active Vault environment and should not be independently generated by the standby Vault. This avoids duplicate processing while preserving the DR Vault as a synchronized recovery target. CyberArk's DR implementation guidance explains the distinction between the normal replicated standby state and activation of the DR Vault.

QUESTION NO: 8

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

A. Operating System Username

B. Host IP Address

C. Client Hostname

D. Operating System Type (Linux/Windows/HP-UX)

E. Vault IP Address

F. Time Frame

ANSWER: A B C

Explanation:

The CreateCredFile utility can bind, or harden, a credential file to characteristics of the client environment in which it is intended to run. **Operating System Username**, **Host IP Address**, and **Client Hostname** are the supported hardening parameters. They allow the Credential Provider to validate the requesting context before using the information stored in the CredFile. In practical terms, the file can be associated with the specific operating-system account that runs the application, the network address of the host, and the host's machine name. This adds protection beyond file-system permissions: copying a CredFile to a different computer, running it under an unintended OS account, or attempting to use it from a different network identity can prevent the file from being accepted. Organizations should select values that remain stable for the application's deployment model, particularly where IP addresses or host names may change because of clustering, autoscaling, or DHCP. CyberArk documents these hardening inputs as part of the CreateCredFile utility parameters and recommends protecting credential files according to the application host and execution identity. See the CyberArk CreateCredFile Utility documentation and the CyberArk Credential Provider documentation.

QUESTION NO: 9

Within the Vault each password is encrypted by:

A. the server key

B. the recovery public key

C. the recovery private key

D. its own unique key

ANSWER: D

Explanation:

Within the CyberArk Digital Vault, each stored password is protected using its own unique encryption key. This per-password key model is a core element of the Vault's layered encryption architecture: the password data is encrypted with a unique key, and the key material is itself protected through additional Vault encryption mechanisms. Consequently, obtaining or compromising data associated with one stored credential does not provide the key needed to decrypt another credential. This design supports strong separation of protected secrets and helps limit the scope of a potential cryptographic exposure.

The unique key is generated and managed internally by the Digital Vault; users and applications retrieve authorized credentials through CyberArk controls rather than handling the encryption key directly. CyberArk describes the Digital Vault as using multiple layers of encryption and protecting credentials with strong cryptographic controls. This architecture is intended to safeguard privileged-account credentials both while stored in the Vault and when accessed through authorized workflows. See CyberArk's Privileged Account Security Solution Technical White Paper and the CyberArk encryption implementation documentation for further details.

QUESTION NO: 10

Secure Connect provides the following. Choose all that apply.

A. PSM connections to target devices that are not managed by CyberArk.

B. Session Recording

C. Real-time live session monitoring.

D. PSM connections from a terminal without the need to login to the PVWA

ANSWER: A B C D

Explanation:

Secure Connect is a Privileged Session Manager capability designed to extend controlled PSM access to target systems even when those systems and their accounts are not onboarded and managed in the CyberArk Vault. A user can initiate a connection from a supported native client or terminal workflow, while PSM brokers the session, so the user does not need to first sign in to the Privileged Vault Web Access portal to launch it. This preserves the familiar connection experience while applying CyberArk session controls.

Because the connection is brokered through PSM, Secure Connect sessions can be recorded for auditability and later review. Authorized personnel can also use PSM's monitoring capabilities to view an active session in real time, supporting oversight and rapid response during privileged activity. Together, unmanaged-target connectivity, portal-free session initiation, recording, and live monitoring provide the controlled-access and accountability model intended by Secure Connect. See CyberArk's Secure Connect documentation and its session monitoring documentation.

QUESTION NO: 11

Which of the following can be configured at the platform level? Choose all that apply.

A. Password complexity requirements.

B. CPM plug-in configuration.

C. Required account properties.

D. Connection components.

E. Safe membership.

F. Dual Control approval levels.

ANSWER: A B C D

Explanation:

Platforms define target-system-specific behavior for accounts. They can specify password complexity requirements, the CPM plug-in used to manage the target account type, required account properties, and the connection components available for accounts assigned to the platform. This enables different account types to use the appropriate password-management and connection settings.

Safe membership is configured on the Safe, not in a platform. Dual Control approval workflows are configured through the Master Policy and applicable policy exceptions, rather than through a platform password policy. See the CyberArk Platform Management documentation.

QUESTION NO: 12

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

Explanation:

Ad-Hoc Access, previously called Secure Connect, extends Privileged Session Manager protection to connections where the target device and its account are not onboarded and managed in CyberArk. This lets authorized users establish a controlled PSM-mediated connection to an otherwise unmanaged target while retaining the security controls associated with a brokered privileged session. The connection is routed through PSM rather than exposing a direct administrative path from the user's workstation to the target.

Because the activity is handled as a PSM session, CyberArk can record the session for audit, investigation, and compliance purposes. The resulting recording provides an evidentiary trail of actions performed during the remote connection. Ad-Hoc Access sessions can also be monitored live by authorized personnel, allowing security teams to observe an active privileged session and respond when necessary. Together, PSM brokering, recording, and live monitoring provide controlled temporary access without requiring the destination system to be fully managed as a standard CyberArk account and target. See CyberArk's PAM Self-Hosted documentation and its overview of Privileged Session Manager.

QUESTION NO: 13

Which password-management operations can the CPM perform for an account when they are enabled and configured for the account platform? Choose all that apply.

A. Password verification

B. Password change

C. Password reconciliation

D. Password retrieval

E. Live session monitoring

ANSWER: A B C

Explanation:

The Central Policy Manager can perform **password verification**, **password change**, and **password reconciliation** for managed accounts. Verification checks whether the password stored in the Vault matches the password on the target system. Password change replaces the target password with a new value and updates the Vault. Reconciliation restores management when the password on the target no longer matches the password stored in the Vault.

Retrieving a password and monitoring a session are user-access and session-management activities, not CPM password-management operations. See the CyberArk password management documentation.

QUESTION NO: 14

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 CyberArk PAM Self-Hosted, Vault licensing is managed through the system Safe, which is a protected internal Safe used for Vault-level configuration and operational files. A Vault administrator updates the license by obtaining the new CyberArk license file and uploading it to the system Safe through the appropriate administrative workflow, such as the PrivateArk Client. The Vault reads the license information from this controlled location and applies the updated entitlement information, including the licensed component capacity and validity details.

This approach keeps license administration inside the Vault's security model: access to the system Safe is restricted, actions are authenticated and auditable, and the license file is not handled as an unprotected operating-system file. The administrator should use a valid license issued for the relevant Vault environment and confirm that the upload has completed successfully so the Vault recognizes the new license state. CyberArk's PAM Self-Hosted documentation describes license-management procedures and the use of the system Safe for maintaining the Vault license. See CyberArk PAM Self-Hosted: License management and CyberArk PAM Self-Hosted: The system Safe.

QUESTION NO: 15

If a user is a member of more than one group that has authorizations on a safe, by default that user is granted_____.

A. the vault will not allow this situation to occur.

B. only those permissions that exist on the group added to the safe first.

C. only those permissions that exist in all groups to which the user belongs.

D. the cumulative permissions of all groups to which that user belongs.

ANSWER: D

Explanation:

The correct result is **the cumulative permissions of all groups to which that user belongs.** CyberArk Vault Safe authorization is additive for group membership. When a user belongs to multiple groups and each of those groups is a member of the same Safe, the Vault evaluates the permissions granted through each applicable group and gives the user the combined effective set. For example, if one group permits viewing Safe accounts and another permits retrieving passwords, a user who belongs to both groups receives both capabilities for that Safe. This behavior enables administrators to assign access through reusable, role-oriented groups rather than needing to create a separate Safe-member definition for every combination of duties. Effective access should therefore be reviewed with all of a user's direct and inherited group memberships in mind, especially for sensitive Safes. CyberArk's Safe-member administration documentation describes assigning Safe permissions to users and groups, while its authorization guidance explains that permissions are evaluated for the identities authorized to access the Safe. See CyberArk PAM Self-Hosted: Safe members and CyberArk PAM Self-Hosted: Safe permissions.

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 and Ticketing Integration

E. Required Properties

F. Custom Connection Components

G. Password Aging Rules

ANSWER: A B C D G

Explanation:

CyberArk's Master Policy is the central policy layer that establishes common password-management and privileged-access controls across the Vault. It can enforce Dual Control, requiring an authorized request and approval workflow before a credential can be retrieved. It also supports One Time Passwords, which invalidate a password after its permitted use, and Exclusive Passwords, which reserve a credential for a single user during an approved access period. These controls help reduce simultaneous or uncontrolled credential use. Password Reconciliation and Ticketing Integration are also Master Policy capabilities: reconciliation defines the response when the CPM cannot change a password normally, while ticketing controls can require and validate a service-management ticket before access is granted. Password Aging Rules are governed through Master Policy password-management settings, enabling organizations to establish password-change timing and related lifecycle controls centrally. CyberArk documents the Master Policy as the location for configuring access-control and password-management policy behavior; platform-specific configuration is then applied separately where appropriate. See the CyberArk Master Policy configuration documentation and the password-management policy documentation for details.

QUESTION NO: 17

Which platform parameters can be used to control when CPM performs password-management activity? Choose all that apply.

A. Interval

B. ImmediateInterval

C. VFExecutionDays

D. RCExecutionDays

E. Safe retention period

F. PVWA session timeout

ANSWER: A B C D

Explanation:

Interval controls how frequently CPM checks for system-initiated work, while **ImmediateInterval** controls how frequently it checks for user-initiated immediate requests. **VFExecutionDays** can limit verification activity to specified days, and **RCExecutionDays** can limit reconciliation activity to specified days.

These platform-level settings help align password-management activity with maintenance windows and target-system availability. Safe retention and PVWA session timeout settings are configured elsewhere and do not control the CPM work schedule. See the CyberArk CPM platform parameters documentation.

QUESTION NO: 18 - (DRAG DROP)

Match each permission to where it can be found.

ANSWER:

Explanation:

CyberArk separates authorization responsibilities between the Vault and individual Safes. A Safe is the protected logical container that holds privileged accounts and controls the actions members can perform against the accounts stored in that specific Safe. Consequently, **Add Accounts** belongs in a Safe because this permission allows an authorized Safe member to create and store account objects in that container. **Initiate CPM account management operations** also belongs in a Safe because CPM actions, such as requesting or initiating management activity for an account, apply to accounts governed by Safe-level membership and permissions.

The Vault is the platform-wide security boundary and provides administrative authorizations for managing foundational Vault objects and identities. **Add/Update Users** is a Vault authorization because creating and maintaining users affects identities that may be granted access across the environment. **Add Safes** is likewise a Vault authorization because it permits creation of the Safe containers themselves rather than work within an existing Safe. This division supports CyberArk's least-privilege model: administrators can manage the Vault structure and user population, while Safe owners and members receive only the permissions needed to manage accounts and operations within assigned Safes.

CyberArk documents Safe member permissions, including account-related and CPM-operation permissions, in its Safe members and permissions documentation. The completed mappings correctly reflect the distinction between Safe-scoped account controls and Vault-scoped administrative authorizations.

QUESTION NO: 19

dbparm.ini is the main configuration file for the Vault.

A. True

B. False

ANSWER: A

Explanation:

`dbparm.ini` is the primary configuration file for the CyberArk Digital Vault. It stores the Vault's central operational parameters, including settings that govern database behavior, communication, logging, security-related operation, and other core Vault services. Because these parameters affect how the Vault starts, communicates, stores and manages data, and performs its foundational functions, CyberArk identifies `dbparm.ini` as the main Vault configuration file.

Administrators should treat this file as a sensitive, tightly controlled component of the Vault environment. Changes should be made only through approved administrative procedures, with an appropriate backup and change record, because an invalid or unsuitable setting can affect Vault availability or behavior. In a distributed CyberArk deployment, configuration changes also need to be evaluated in the context of the relevant Vault architecture and maintenance guidance. CyberArk documentation describes Vault configuration and administration as part of the Digital Vault server administration workflow. See the CyberArk Privileged Access Manager Self-Hosted documentation and the Vault server preparation guidance.

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 three.)

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

B. Copy the entire contents of the CD to the system Safe on the Vault

C. Copy the entire contents of the CD to a folder on the Vault Server and secure it with NTFS permissions

D. Store the server key in a Hardware Security Module (HSM) and copy the rest the keys from the CD to a folder on the Vault Server and secure it with NTFS permissions

ANSWER: A C D

Explanation:

The Operator CD contains material required to start and operate the Vault following planned maintenance or a restart, so its contents must remain available to authorized Vault administrators without being exposed through ordinary application storage. Storing the CD in a physical safe and mounting it only when Vault maintenance is performed preserves the original removable-media protection model while making the files available when they are needed. A protected folder on the Vault Server is also an acceptable operational approach when the entire CD content is copied there and access is restricted with appropriately controlled NTFS permissions. Those permissions should be limited to the authorized operating accounts and administrators, with inheritance and unnecessary access removed. Using an HSM for the server key provides stronger protection for the most sensitive key material because the key remains protected by dedicated cryptographic hardware. The remaining Operator CD files can then be retained in a locally secured NTFS-protected folder so that a planned restart can access the required material. These approaches balance recoverability with access control and support the Vault's key-protection architecture. CyberArk's documentation portal provides the Vault installation, security, and recovery procedures relevant to protecting Vault key material: CyberArk PAM Self-Hosted documentation. For HSM integration and supported key protection workflows, consult CyberArk Vault HSM integration documentation.

QUESTION NO: 21

Which one the following reports is NOT generated by using the PVWA?

A. Accounts Inventory

B. Application Inventory

C. Sales List

D. Compliance Status

ANSWER: C

Explanation:

Sales List is correct because it is not a Privileged Session/Password Management reporting category or report generated through the Password Vault Web Access (PVWA). PVWA reporting is intended to provide operational and security visibility into privileged-account management, such as information about managed accounts, applications associated with credential use, and the environment's compliance posture. These reports support activities including account governance, auditing, identifying unmanaged or noncompliant items, and monitoring the use of privileged credentials.

A sales list is a business or commercial-reporting artifact rather than a privileged-access-management artifact. It does not contain the type of vault, account, application, policy, or compliance data collected and presented by CyberArk PAM. Therefore, it would not be available as a report generated from PVWA. CyberArk's documentation describes PVWA as the web interface used to manage privileged accounts and access the reporting capabilities supplied by the PAM solution; its report content is focused on privileged-access operations and security oversight. See CyberArk's Reports documentation and PVWA documentation.

QUESTION NO: 22

Which statement is correct concerning accounts that are discovered, but cannot be added to the Vault by an automated onboarding rule?

A. They are added to the Pending Accounts list and can be reviewed and manually uploaded.

B. They cannot be onboarded to the Password Vault.

C. They must be uploaded using third party tools.

D. They are not part of the Discovery Process.

ANSWER: A

Explanation:

They are added to the Pending Accounts list and can be reviewed and manually uploaded. Account Discovery identifies privileged and non-privileged accounts on defined target systems and evaluates them against the automated onboarding rules configured for the platform. When a discovered account does not meet the criteria needed for automated onboarding, CyberArk retains the discovery result in the Pending Accounts list rather than discarding it. This gives authorized administrators visibility into accounts that require a decision or additional handling.

From Pending Accounts, an administrator can review the discovered account's properties and decide whether it should be brought under CyberArk management. The administrator can then manually onboard the account to the appropriate Safe and platform, supplying or validating required account details as part of that process. This workflow ensures that discovery continues to provide actionable inventory information even where no automated rule can place an account directly into the Vault. It also supports controlled onboarding by allowing review before the account becomes managed. CyberArk documents the pending-account workflow in its Account Discovery documentation and describes account onboarding in the onboarding accounts documentation.

QUESTION NO: 23

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 the correct group. In CyberArk Privileged Access Manager, the built-in Auditors group is intended for users who need oversight of privileged activity without performing privileged-account management tasks. Its members can access the session-monitoring capabilities in the Password Vault Web Access interface, including viewing recorded privileged sessions and monitoring active sessions in real time when the relevant session-monitoring controls are enabled.

This separation supports an audit-focused, least-privilege model: personnel responsible for security review, compliance, investigation, or operational oversight can examine what occurred during a privileged session while maintaining an appropriate separation from users who administer the Vault or operate privileged accounts. In practice, access to a particular recording or live session can also depend on the user having the required Safe-level authorizations and on the platform/session configuration permitting recording and monitoring. However, the CyberArk role that provides the standard group-level capability for these oversight activities is Auditors.

CyberArk documents session monitoring and recording review in its Monitor Privileged Sessions documentation. Additional role and authorization context is available in the Manage Users documentation.

QUESTION NO: 24

Which tools are used during a CPM renaming process?

A. APIKeyManager Utility

B. CreateCredFile Utility

C. CPMinDomain_Hardening.ps1

D. PMTerminal.exe

E. Data Execution Prevention

ANSWER: A B

Explanation:

The correct tools are **APIKeyManager Utility** and **CreateCredFile Utility**. Renaming a Central Policy Manager changes the CPM's identity and requires its internal authentication material to be re-created or updated so that the renamed component can authenticate securely with the Vault and continue performing password-management tasks. CreateCredFile Utility is used to create the credential file required by the CPM after the rename procedure. This credential file securely stores the information that enables the CPM service to log on to the Vault using its designated Vault user. APIKeyManager Utility is also part of the rename workflow because it manages the API key material used by the CPM for authenticated communication in applicable CyberArk configurations. Using these utilities as directed ensures that the CPM's service identity, credential-file configuration, and authentication artifacts align with the new CPM name before the service resumes normal operation. This avoids a mismatch between the CPM configuration and the authentication information that CyberArk components rely on. Consult the CyberArk PAM self-hosted documentation and the installation or maintenance instructions corresponding to the deployed version before performing the procedure: CyberArk Documentation and CyberArk Privileged Access Manager.

QUESTION NO: 25 - (SIMULATION)

Arrange the steps to install the Password Vault Web Access (PVWA) in the correct sequence

ANSWER: Check the explanation for the answer

Explanation:

Correct installation sequence:

1. Prepare the PVWA server: install and configure the required IIS/.NET prerequisites and ensure the server can communicate with the Vault.
2. Log on to the PVWA server using the designated installation account with local Administrator permissions.
3. Copy/extract the PVWA installation media locally and run `Setup.exe` (Run as Administrator).

4. In the installation wizard, accept the license agreement and specify the required installation options, including the PVWA installation directory/virtual directory when prompted.
5. Allow the installer to install the PVWA components and create/configure the IIS PVWA application.
6. Configure the PVWA connection to the Vault (Vault address, port, and applicable Vault/application credentials) using the PVWA configuration step/wizard.
7. Complete the installation, apply the required IIS/TLS certificate and post-installation hardening, then browse to the PVWA URL to verify that the PVWA logon page is available.

In short: **Prerequisites → run Setup → select installation options → install PVWA/IIS components → configure Vault connectivity → secure and validate access.**

QUESTION NO: 26

CyberArk user Neil is trying to connect to the Target Linux server 192.168.1.64 using a domain account ACME/linuxuser01 on Domain Acme.corp using PSM for SSH server 192.168.65.145. What is the correct syntax?

A. Ssh neil@linuxuser01:acme.corp@192.168.1.64@192.168.1.45

B. ssh neil@linuxuser01#acme.corp@192.168.1.64@192.168.65.145

C. Ssh neil@linuxuser01@192.168.1.64@192.168.65.145

D. Ssh neil@linuxuser01@acme.corp@192.168.1.64@192.168.1.45

ANSWER: B

Explanation:

`ssh neil@linuxuser01#acme.corp@192.168.1.64@192.168.65.145` is the required PSM for SSH connection format for this scenario. The first value, `neil`, identifies the CyberArk Vault user authenticating to PSM for SSH. The next component identifies the managed account to be used on the target: `linuxuser01` is the account name and `acme.corp` is its domain. PSM for SSH uses the hash character (`#`) between the managed-account user name and domain so the domain is interpreted as part of the account identity rather than as another SSH host separator. The following address, `192.168.1.64`, is the Linux target system where the privileged session will be established. Finally, `192.168.65.145` is the PSM for SSH server address; the SSH client connects to this server, which authenticates the user, retrieves and injects the managed credential according to policy, and proxies the session to the target. This format lets CyberArk control, monitor, and record the privileged SSH session without exposing the managed account password to Neil. CyberArk documents the PSM for SSH connection-string structure and domain-account delimiter in its PSM for SSH documentation and PSM for SSH connection guidance.

QUESTION NO: 27

When creating an onboarding rule, it will be executed upon .

A. All accounts in the pending accounts list

B. Any future accounts discovered by a discovery process

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

ANSWER: C

Explanation:

Both “All accounts in the pending accounts list” and “Any future accounts discovered by a discovery process” is correct because an onboarding rule has both an immediate and an ongoing effect. When the rule is created, CyberArk evaluates the accounts already awaiting action in the Pending Accounts list and applies the rule to those that meet its defined criteria. This enables administrators to automate onboarding for discovered accounts that accumulated before the rule was available, rather than requiring manual processing or waiting for another discovery cycle.

The rule also remains active for subsequent discovery results. Each time a discovery process identifies an account, CyberArk evaluates that account against the configured onboarding rules. If the account matches the rule's conditions, the rule applies the specified onboarding settings, such as the target Safe, platform, and account properties. This continuing evaluation makes onboarding rules suitable for consistent, scalable handling of both the current discovery backlog and newly discovered accounts. CyberArk's documentation describes automatic onboarding through discovery and onboarding rules in the Onboard accounts automatically guidance and the CyberArk documentation portal.