PassQueen
a.k.a dumpsqueen.com

CyberArk Sentry PAM

CyberArk PAM-SEN

Version Demo

Total Demo Questions: 15

Total Premium Questions: 159

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

You are installing PSM for SSH with AD-Bridge and CyberArkSSHD mode set to integrated for your customer.

Which additional packages do you need to install to meet the customer's needs? (Choose two.)

A. CARKpsmp-infra

B. libssh

C. OpenSSH 7.8 or higher

D. CARKpsmp-ADBridge

E. CARKpsmp-SSHD

ANSWER: D E

Explanation:

`CARKpsmp-ADBridge` is required when the PSM for SSH deployment is configured to use AD Bridge. This component supplies the PSM for SSH integration needed to use Active Directory identities and authentication through the AD Bridge configuration. Installing it ensures that the configured AD Bridge capability is actually available to the PSM for SSH environment.

`CARKpsmp-SSHD` is required when CyberArkSSHD is configured in integrated mode. This package provides the CyberArk SSH daemon component that operates as the integrated SSH service for PSM for SSH. The package selection must match the selected SSHD mode; therefore, an integrated CyberArkSSHD deployment requires the CyberArkSSHD package in addition to the base PSM for SSH installation components.

These two packages correspond directly to the two explicitly selected optional integrations: AD Bridge and integrated CyberArkSSHD. CyberArk's PSM for SSH installation documentation describes selecting and installing the relevant component packages for the capabilities enabled in the deployment. See the CyberArk PSM for SSH installation documentation and the PSM for SSH documentation overview.

QUESTION NO: 2

In which configuration file do you add LoadBalancerClientAddressHeader when you enable x-forwarding on the PVWA loadbalancer?

A. PVconfiguration.xml

B. web.config

C. apigw.ini

D. CyberArkScheduledTasks.exe.config

ANSWER: B

Explanation:

web.config is correct because it is the Internet Information Services and ASP.NET application configuration file for the Password Vault Web Access (PVWA) site. When PVWA is deployed behind a load balancer or reverse proxy that forwards the original client IP address, the PVWA application must be told which HTTP header contains that address. The `LoadBalancerClientAddressHeader` application setting is added or updated in PVWA's `web.config`, typically with the value that matches the header inserted by the load balancer, such as `X-Forwarded-For` or a deployment-specific header. This enables PVWA to use the originating client address rather than the address of the intermediary load balancer for relevant client-address handling and auditing behavior. The change is made in the configuration file of the PVWA web

application and should be performed consistently on every PVWA node participating in the load-balanced deployment. After modifying the file, follow the organization's change-control process and validate that the proxy is supplying the configured header only from trusted infrastructure. CyberArk's PVWA load-balancing guidance is available in the CyberArk load balancing documentation; the setting is also covered in CyberArk's PVWA configuration documentation.

QUESTION NO: 3

You are installing a CPM.

In addition to Add Safes, Add/Update Users, Reset Users' Passwords and Manage Server File Categories, which Vault authorization(s) does a CyberArk user need to install the CPM?

A. Manage Directory Mapping

B. Activate Users

C. Backup All Safes, Restore All Safes

D. Audit Users, Add Network Areas

ANSWER: B

Explanation:

Activate Users is required in addition to the listed Vault authorizations when installing the Central Policy Manager. CPM installation uses the designated Vault administrative account to create and configure the CPM-related Vault objects, including the CPM application user and the components that allow the service to authenticate and operate. The user activation capability is necessary because a newly created Vault user must be activated before it can be used by the CPM service. This is part of the required authorization set for the installation account; it is not merely an optional post-installation administrative task.

CyberArk's CPM installation guidance specifies that the Vault user performing installation must have the listed administrative permissions together with the ability to activate users. Assign these permissions before launching the installation so the installer can complete its required Vault-side configuration without manual intervention or authorization failures. After installation, organizations should continue to follow least-privilege practices and use dedicated service and administrative accounts where appropriate. See CyberArk's CPM installation documentation and the CPM preinstallation requirements for the required Vault permissions and installation prerequisites.

QUESTION NO: 4

Which statements describe appropriate use of a CyberArk Reconcile Account? Check all that apply.

A. It can reset a managed account password that is out of synchronization.

B. It requires sufficient permissions to reset the managed account on the target.

C. Its credentials should be secured in the Vault.

D. It replaces the need for scheduled password changes.

E. It must be a domain administrator for every managed Windows account.

ANSWER: A B C

Explanation:

A Reconcile Account is configured for use when CPM must reset a managed account password after the password stored in the Vault is no longer valid on the target. The account must have sufficient target-system permissions to reset the managed account, and its credentials should be stored and protected in the Vault like other privileged credentials.

Reconciliation is not a replacement for scheduled password changes and does not require giving every CPM service account unrestricted domain-administrator rights. Reconcile permissions should follow least-privilege principles while still allowing the required reset operation. See the CyberArk documentation on reconciling accounts.

QUESTION NO: 5 - (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 and install the required prerequisites, especially the supported Windows/IIS roles and features, .NET requirements, and required IIS components.
2. Ensure the Vault is reachable from the PVWA server and prepare the Vault/PVWA application identity (the PVWA Vault user/credential information) that PVWA will use to connect to the Vault.
3. Run the PVWA installation package (`Setup.exe`) as a local Administrator and complete the installation wizard, including the PVWA installation path and IIS virtual application settings.
4. Configure the installed PVWA to connect to the Vault: provide the Vault address/port, configure the PVWA application user credentials, and verify the Vault connection.
5. Apply post-install IIS security configuration, including the HTTPS certificate/binding and required PVWA hardening settings.
6. Open the PVWA URL over HTTPS and validate that users can log on and that the PVWA can retrieve information from the Vault.

In short: **install IIS/prerequisites → prepare Vault connectivity/PVWA identity → install PVWA → configure Vault connection → secure IIS with HTTPS/hardening → test.**

QUESTION NO: 6

The account used to install a PVWA must have ownership of which safes? (Choose two.)

A. VaultInternal

B. PVWAConfig

C. System

D. Notification Engine

E. PVWAReports

ANSWER: A B

Explanation:

The account used to install the Password Vault Web Access must be an owner of the **VaultInternal** and **PVWAConfig** safes. VaultInternal is a core internal safe that the PVWA installation and resulting application require for protected internal Vault data and operational configuration. Ownership provides the administrative Safe permissions needed for the installer to establish and maintain the required access configuration rather than merely consume accounts stored in the Safe.

PVWAConfig is the dedicated Safe used to protect PVWA configuration data. The installation process must be able to create, update, and manage the configuration content required for the PVWA to operate. Assigning Safe ownership to the installation account ensures the deployment can complete its required configuration steps and that the PVWA environment has the necessary protected configuration repository available from the outset. CyberArk's PVWA installation prerequisites specifically identify ownership of these two Safes for the installing user. See the CyberArk PVWA installation documentation and the CyberArk Safe administration documentation.

QUESTION NO: 7

What are the basic network requirements to deploy a CPM server?

A. Port 1858 to Vault and Port 443 to PVWA

B. Port 1858 only

C. all ports to the Vault

D. Port UDP/1858 to Vault and all required ports to targets and Port 389 to the PSM

E. TCP port 1858 to the Vault and the required management ports to target devices

ANSWER: E

Explanation:

TCP port 1858 to the Vault and the required management ports to target devices is correct because the Central Policy Manager must establish its secure Vault connection over TCP 1858. This connection lets CPM retrieve platform and account information, obtain credentials, process password-management tasks, and securely store the resulting passwords and task status in the Vault. CPM also needs network access to each managed target using the protocol required by that target's applicable platform or connection component. For example, a Unix account-management workflow commonly requires SSH access, while Windows password-management workflows may require the Windows remote-management ports and services configured for the selected platform. These target-device ports are not one universal fixed set; they depend on the operating system, account type, and password-management method in use. The required firewall design should therefore permit TCP 1858 between CPM and the Vault, plus only the specific, least-privilege management connectivity needed from CPM to the target systems. CyberArk's deployment guidance describes the CPM-to-Vault connection and its network requirements, while platform documentation identifies the connectivity needed for individual managed account types. See CyberArk's CPM requirements documentation and Privileged Account Security implementation guidance.

QUESTION NO: 8

If a customer has one data center and requires fault tolerance, how many PVWAs should be deployed?

A. two or more

B. one PVWA cluster

C. one

D. two PVWA clusters

ANSWER: A

Explanation:

two or more is correct because PVWA fault tolerance within a single data center requires multiple independently deployed PVWA servers. A PVWA is the web-facing component through which users access CyberArk PAM services, so deploying at least two instances prevents a single PVWA server failure, maintenance event, or web-service outage from making the portal unavailable. The PVWA servers are deployed separately and are typically placed behind a load balancer, which directs user sessions to an available instance and supports continuity when one server is unavailable. The PVWAs connect to the same CyberArk environment and are configured consistently, allowing either server to provide the web access function. This design addresses availability of the PVWA tier within the data center; broader resiliency planning can additionally include redundant Vault, CPM, PSM, network, and load-balancing components as required by the customer's recovery objectives. CyberArk's PAM Self-Hosted documentation describes high-availability architecture and component deployment considerations at CyberArk PAM high availability. General CyberArk documentation is available through the CyberArk Documentation portal.

QUESTION NO: 9

Which CyberArk component changes passwords on Target Devices?

A. Vault

B. CPM

C. PVWA

D. PSM

E. PrivateArk

F. OPM

G. AIM

ANSWER: B C

Explanation:

CPM is CyberArk's Central Policy Manager and is the component that performs the password-management operation on target devices. It retrieves the relevant account and platform policy, connects to the target through the configured management method, changes or reconciles the credential as required, and stores the resulting password securely in the Vault. CPM also performs password verification according to the platform's policy settings.

PVWA is the web interface through which authorized users and administrators manage accounts and initiate or request password-management activities. In normal operation, a password-change request submitted through PVWA is processed by CPM; therefore, PVWA participates in the password-change workflow as the user-facing management component, while CPM carries out the target-device action. This relationship is fundamental to CyberArk's separation of the web management interface from the automated password-management engine. For additional detail, see CyberArk's Central Policy Manager documentation and Password Vault Web Access documentation.

QUESTION NO: 10

Which settings can be configured in a CyberArk platform? Check all that apply.

A. Password policy rules

B. Password-management plug-in settings

C. PSM connection components

D. Password verification and reconciliation settings

E. Safe member permissions

ANSWER: A B C D

Explanation:

A platform defines how CyberArk manages and connects to accounts of a particular type. Platform configuration can include the password policy applied by CPM, the password-management plug-in used to communicate with the target, and the connection components made available for PSM sessions. It can also define whether password verification, change, and reconciliation operations are enabled.

Safe membership is not configured in a platform. Safe owners manage Safe membership and permissions separately, while each account is associated with a platform that determines its applicable management and connection behavior. See the CyberArk platform management documentation.

QUESTION NO: 11

Which of the following protocols need to be installed on a standalone vault server? Check all that apply.

A. Client for Microsoft Networks

B. QoS Packet Scheduler

C. File and Printer Sharing for Microsoft Networks

D. Internet Protocol version 4 (TCP/IPv4)

E. NIC Teaming Driver, if applicable

ANSWER: A B C D

Explanation:

A standalone CyberArk Digital Vault requires the standard Windows networking components that support its network connectivity and the SMB-based services used by the Vault environment. Client for Microsoft Networks provides the workstation-side Microsoft networking component, while File and Printer Sharing for Microsoft Networks provides the server-side SMB component required by the supported Vault configuration. QoS Packet Scheduler must also be present in the adapter bindings as part of the prescribed Vault server network configuration. Internet Protocol version 4 (TCP/IPv4) is required because the Vault's network communication is configured using IPv4 addressing and TCP/IP connectivity. These components should be verified in the properties of every network adapter used by the Vault before installation or commissioning. CyberArk's Vault-server preparation guidance specifies the required adapter components as part of establishing a supported, hardened Vault host configuration. The installation and hardening process should be performed according to the relevant version of the CyberArk PAM Self-Hosted documentation, including its network and operating-system prerequisites. See the CyberArk guidance for preparing the Vault server and the CyberArk PAM Self-Hosted system requirements.

QUESTION NO: 12

Which file would you modify to configure the vault to send SNMP traps to your monitoring solution?

A. dbparm ini

B. paragent.ini

C. ENEConf.ini I

D. padr ini

ANSWER: C

Explanation:

ENEConf.ini I is the correct file because SNMP trap notification is handled by the Vault's Event Notification Engine (ENE). The ENE monitors configured Vault events and can forward qualifying event notifications to external monitoring infrastructure through SNMP traps. Its configuration file, ENEConf.ini, contains the settings that enable SNMP notification and identify the destination monitoring system, such as the SNMP manager or trap receiver. After updating the applicable SNMP-related settings, the Event Notification Engine uses that configuration when processing Vault events and generating traps. This makes the ENE configuration the appropriate place to integrate CyberArk Vault event monitoring with an enterprise monitoring or SIEM platform that accepts SNMP notifications. CyberArk's Vault monitoring documentation describes the Event Notification Engine as the mechanism for forwarding Vault notifications, while its configuration guidance identifies ENE configuration as part of managing those notifications. See the CyberArk PAM Self-Hosted monitoring documentation and the CyberArk documentation portal for the documentation version that matches the deployed Vault release.

QUESTION NO: 13

There is a requirement for a password to change between 01:00 and 03:00 on Saturdays and Sundays; however, this does not work consistently.

Which platform setting may be the cause?

A. The Interval setting for the platform is incorrect and must be less than 120.

B. The ImmediateInterval setting for the platform is incorrect and must be greater than or equal to 1.

C. The DaysToRun setting for the platform is incorrect and must be set to Sat,Sun.

D. The HeadStartInterval setting for the platform is incorrect and must be set to 0.

ANSWER: A D

Explanation:

The Interval setting for the platform is incorrect and must be less than 120. The CPM evaluates and processes scheduled password-management activity according to its configured interval. Because the permitted change window is only 120 minutes long, an interval of 120 minutes or more can cause the CPM to miss all or part of that window depending on when its processing cycle begins. Configuring an interval shorter than the available window gives the CPM an opportunity to identify and process eligible accounts while the Saturday/Sunday 01:00–03:00 schedule is active.

The HeadStartInterval setting for the platform is incorrect and must be set to 0. HeadStartInterval controls how far before the configured schedule window the CPM may begin processing. For a requirement that changes occur strictly within the specified window, a nonzero head-start can cause work to begin before 01:00, creating apparent inconsistency with the intended schedule. Setting it to zero aligns the earliest possible processing time with the window start. These settings must be considered together: the processing cadence must fit inside the window, and the permitted start time must not precede it. CyberArk documents CPM scheduling and platform password-management configuration in its Central Policy Manager documentation and platform management documentation.

QUESTION NO: 14

After installing the Vault, you need to allow Firewall Access for Windows Time service to sync with NTP servers 10.1.1.1 and 10.2.2.2.

What should you do?

A. Edit DBParm.ini to add: AllowNonStandardFWAddresses=[10.1.1.1,10.2.2.2],Yes,123:outbound/udp. Most Voted

B. Edit DBParm.ini to add: NTPServer=[10.1.1.1:123/UDP,10.2.2.2:123/UDP].

C. Edit DBParm.ini to add: AllowNonStandardFWAddresses=[10.1.1.1,10.2.2.2],Yes,123:outbound/udp,123:inbound/udp.

D. Edit the Windows Firewall configuration to add a rule for Port 123/udp outbound to 10.1.1.1 and 10.2.2.2.

ANSWER: A

Explanation:

Edit DBParm.ini to add: AllowNonStandardFWAddresses=[10.1.1.1,10.2.2.2],Yes,123:outbound/udp. Most Voted is correct because the Vault's firewall configuration is managed through the `AllowNonStandardFWAddresses` DBParm parameter when a Vault component requires communication that is not part of the standard CyberArk firewall rules. The two NTP server addresses are explicitly listed as permitted destinations, while `123:outbound/udp` allows the Vault host's Windows Time service to send NTP requests on the standard NTP UDP port. The `Yes` setting enables access to the specified nonstandard addresses under the Vault firewall configuration. Windows Time initiates synchronization requests to the configured NTP servers, so the required communication is outbound UDP from the Vault to port 123. The response traffic is associated with that outbound session and is handled by the stateful firewall behavior; a separate inbound NTP listener rule is not required for time synchronization. After changing DBParm.ini, apply the configuration according to the Vault administration procedure so that the firewall policy is updated. CyberArk documents Vault firewall configuration and custom permitted addresses in its Vault firewall implementation guidance. Microsoft also documents that the Windows Time service uses UDP port 123 for NTP communication in its Windows Time Service documentation.

QUESTION NO: 15

What is the purpose of the PSM health check hardening?

A. Remove IIS settings which can be considered security vulnerabilities.

B. Validate that the PSM is ready to be placed behind a load balancer.

C. Confirm that the Windows Services for PSM are running on the server.

D. Ensure that the AppLocker script does not have any syntax errors.

ANSWER: A

Explanation:

The purpose is to **remove IIS settings which can be considered security vulnerabilities.** CyberArk Privileged Session Manager relies on Microsoft IIS components to provide its secure connection and session-management capabilities. The PSM hardening process evaluates and adjusts the IIS configuration so that unnecessary or insecure web-server functionality and settings are removed or disabled. This reduces the attack surface of the PSM host and helps ensure the IIS layer is configured in accordance with CyberArk's secure deployment requirements.

Hardening is therefore a security-configuration activity, rather than simply an operational availability test. It is intended to protect the server that brokers privileged sessions by applying restrictive IIS settings appropriate for a dedicated PSM installation. Maintaining this hardened state is important because PSM handles highly sensitive privileged access workflows and session traffic. Administrators should run the documented hardening procedure as part of PSM deployment and review its results when making IIS-related changes, applying updates, or troubleshooting configuration drift.

CyberArk describes PSM as a component for isolating, monitoring, and recording privileged sessions; its implementation guidance includes securing the PSM environment. See CyberArk Privileged Session Manager and Microsoft's IIS security configuration guidance.