CYBERARK PAM-SENTRY

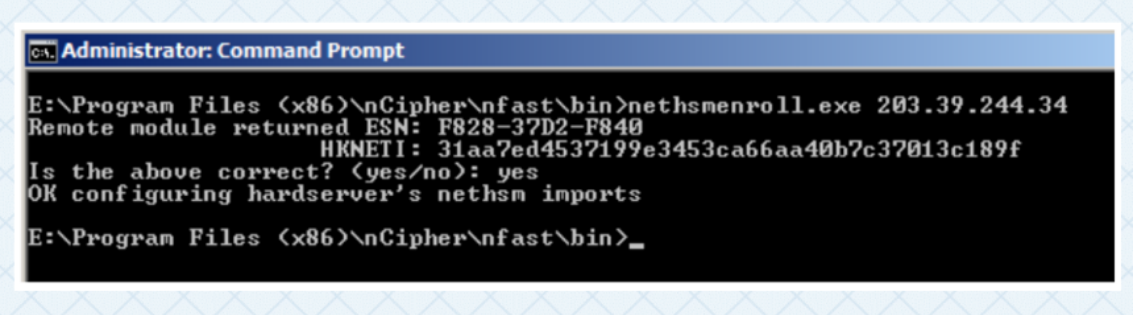
Deploy the Vault

Identify and describe the steps to migrate the server key to an HSM

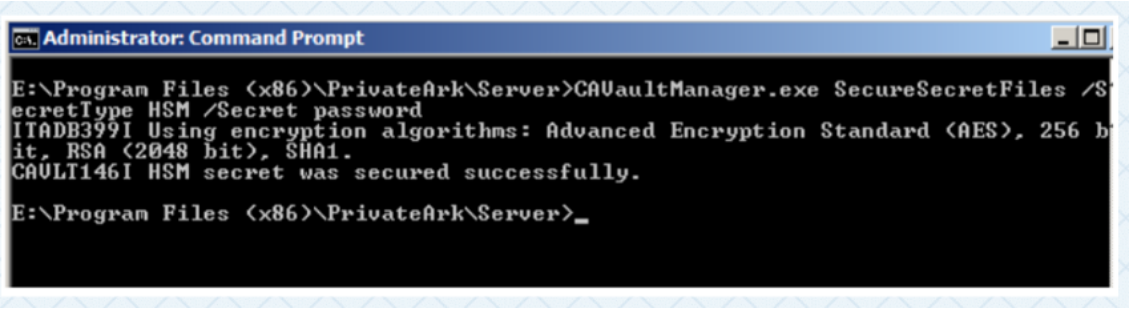
- Best practice is to install HSM Software BEFORE installing CyberArk and test connectivity
- But HSM Software could be Installed even after CyberArk installation
    - Install Vault as usual
    - In DBparm.ini open FW port to HSM using “AllowNonStandardFWAddresses” statement.
    - In DBparm.ini configure HSM using “PKCS11ProviderPath”

```
[CRYPTO]
SymCipherAlg=AES-256
ASymCipherAlg=RSA-2048
AllowNonStandardFWAddresses=[203.39.244.34],Yes,9004:inbound/tcp,9004:outbound/tcp
[HSM]
PKCS11ProviderPath="E:\Program Files (x86)\nCipher\nfast\toolkits\pkcs11\cknfast.dll"
ReconnectHSMOnErrorCodes=48,50,179
```

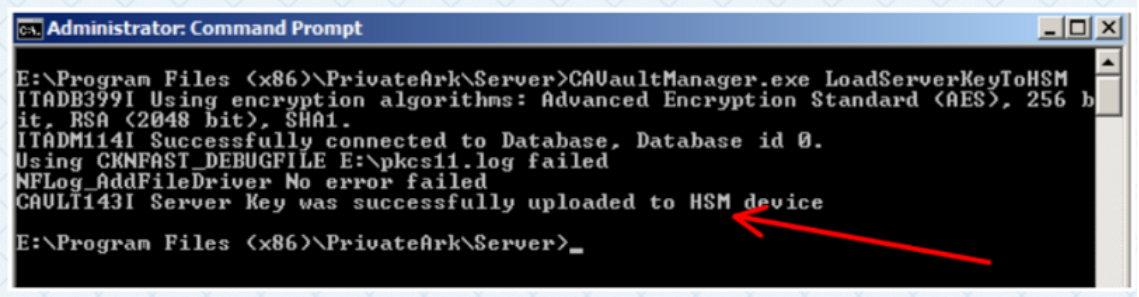
    - Enroll the Vault in the HSM Server



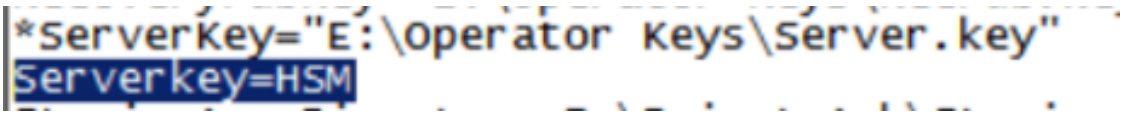
    - Encrypt HSM PIN Code using CAVaultManager.exe



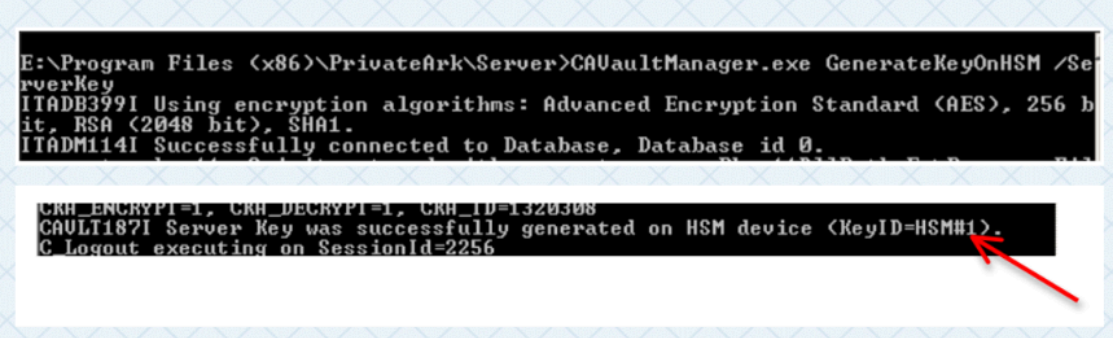
    - Load Existing Key to HSM using “CAVaultManager.exe LoadServerKeyToHSM”



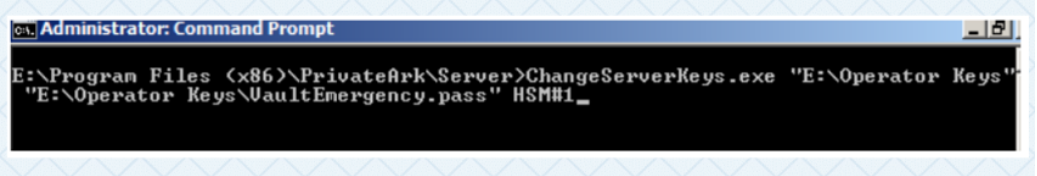
- Point DBParm.ini to Server key on HSM



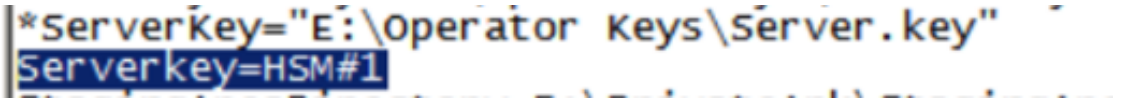
- Restart the Vault.
- Generate a NEW Server Key on HSM



- Rekey the Vault
  - Insert Master CD
  - Run ChangeServerKeys



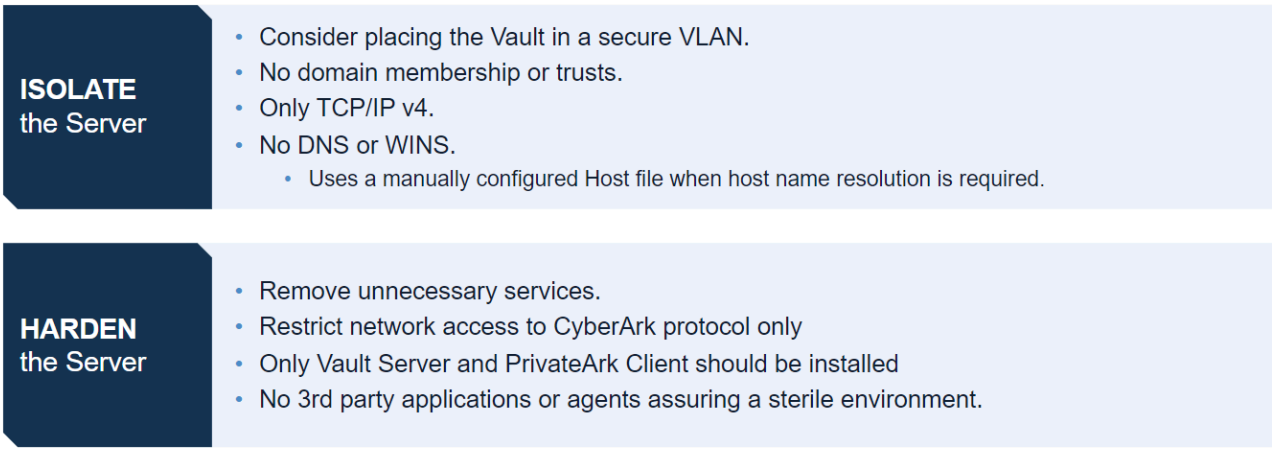
- Point (again) the DBParm.ini to the new server Key



- Restart the Vault once more.

Identify and describe the steps to complete a post-install hardening

In summary, we isolate the vault server and restrict network access to only authorized addresses. Hardening is a process that ensures that only necessary applications, services, protocols, roles and features are installed in support of the vault.



There are four main steps listed in the file: "Hardening.ini" that can be found here by default: *"<vault installation path>\server\hardening\hardening.ini"* and are explained in more detail in the sections below. These can be set to 'No' if required/needed. (art: 000007835)

Hardening.ini

HardenNetworkDevice=Yes
HardenWindowsSecurity=Yes
HardenWindowsLocalSecurity=Yes
HardenWindowsFireWall=Yes

Network Cards/Adapters Hardening
IPv4
- Disable 'NetBIOS' setting
- Disable 'LMHOSTS lookup'
- Disable 'Register this connection's addresses in DNS'

IPv6
- Disable 'Register this connection's addresses in DNS'

Windows Security Hardening
There are three files that can be used for this part: server 2008, server 2012 and server 2016 (in later versions). These can be found on the installation CD/media and also in the 'Hardening' folder within the vault local install path (*C:\Program Files (x86)\PrivateArk\Server\Hardening\StandaloneVault*). The files 'Windows2008Security.inf', 'Windows2012Security.inf' or 'Windows2016Security.inf' will be used depending on the operating system. A more detailed list can be found by opening the .inf file with a text editor.

Windows Audit Policy Hardening
As with the 'Windows Security' hardening there are three files, 'Windows2008Audit.csv', 'Windows2012Audit.csv', and 'Windows2016Audit.csv' depending on the operating system. These can be found in the same location as the files used for the hardening of the Windows security.

Windows Local Security Hardening
The following changes are made:
- local users disabled apart from the user that is logged in during the install
- Users removed from the local groups apart from the local admin users and the user that is logged in (should be the same user).
- Registry value deleted: LMachine/Software/Microsoft/Windows/CurrentVersion/Run/VMware User Process
- Daylight saving enabled

Windows Firewall Hardening
During the install all the firewall rules are deleted, then from this point firewall rules will be dynamically added and removed when required. A log can be seen within the windows event logs here:
- *Event Viewer (Local) > Applications and Services Logs > Microsoft > Windows > Windows Firewall With Advanced Security > Firewall*
Static rules will also be added however these are still managed by the vault and depend on rules that have been added the DBParm.ini file.

Identify and describe the components and steps to complete a Vault installation

Installation package

- CyberArk Server and client installation software
- Operator CD, copied locally in preparation for HSM (recommended) or slotted into CD Drive
- CyberArk License File
- Digital certificates installed in support for LDAP integration (root CA certificate)

Installation Steps

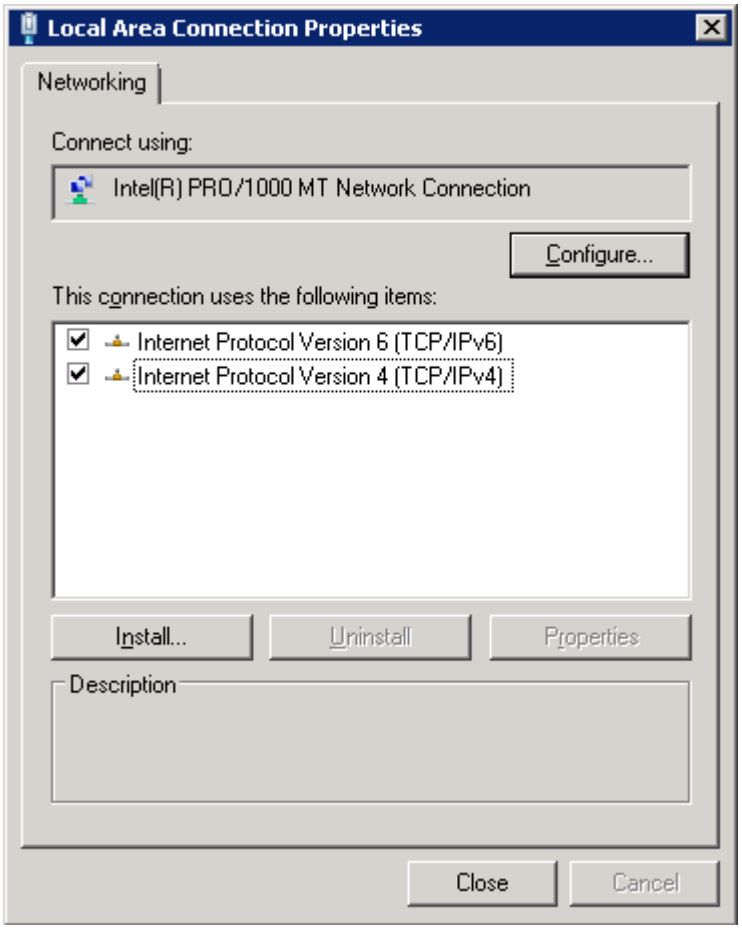
- Check Server Prerequisites
- Prepare Windows Server for Vault Installation
- Install the Vault
- Server Hardening
- Post installation tasks

Describe how to prepare a Windows server for Vault installation

- Verify server requirements
- Make sure server is not and has never been part of a domain
- Sync the Vault with NTP
- Install Microsoft Visual C++ Redistributable for Visual Studio 2015-2022 32-bit and 64-bit versions
- Install Microsoft Framework .NET 4.8 Runtime, and restart the machine
- Ensure that the Administrator password is appropriately strong. As a best practice, we recommend setting a minimum of 14 alphanumeric characters.
- Check that the server IP address is correctly configured, and that it is static.
- In the Network Connection properties, clear the Preferred DNS Servers check box

- Review the number of network cards, so that later you can verify that the Vault has recognized them all
- Ping a known IP address to check the network connection is working correctly

If non clustered installation: uninstall/disable all protocols except the following TCP/IP protocols.

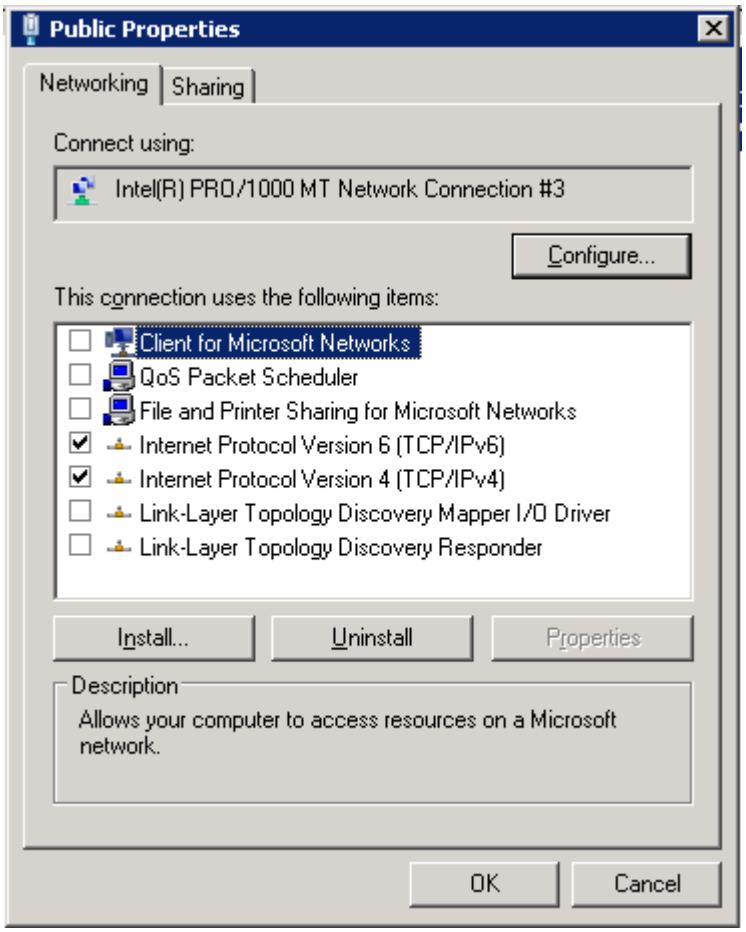


Reboot the server

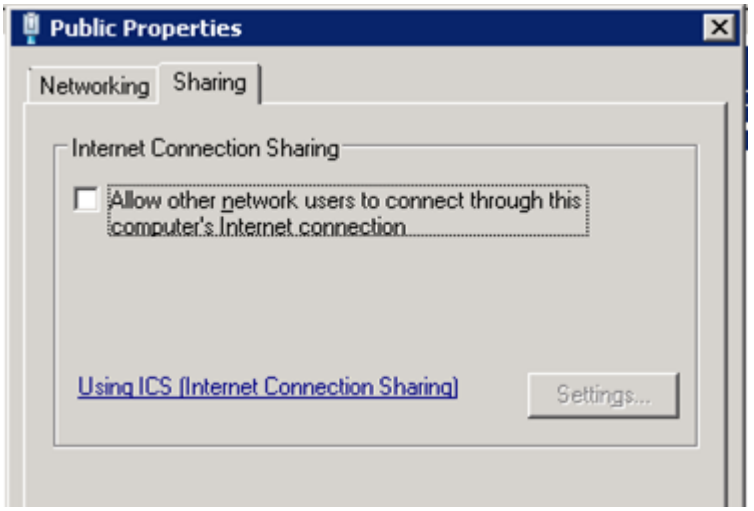
If a cluster is required complete these tasks on the host machines for both node A and node B before continuing to the Vault installation:

- Run chkdsk to confirm that the drive where you will install the Digital Vault is healthy.
- Configure the network
    - Allocate three IP addresses on your enterprise network for the Vault Cluster node's public addresses and the Virtual IP. The public IPs and the Virtual IP must be from the same subnet.
    - If using a Private Cluster Network, create the network and connect one NIC from each Cluster Vault node to it. Otherwise, connect one NIC from each Cluster Vault node directly using a cross-over cable.
- Configure the network cards
    - Configure the public network card and private network card on each node (do not configure VIP now)
    - Save the network card name of the public network of each node for later use
    - On the public network card for each node:

- Uncheck Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks on the Public Networking properties.



- Disable **Internet Connection Sharing** on the Public Sharing Properties



- Reboot each server
- Prepare shared storage with two drives. One drive is for the Vault data and metadata, and the other drive is for the Quorum Disk.
    - Before installing the Cluster Vault, format the drives to make sure they are healthy.

    - Ensure that the drive letters for the Quorum are identical in both nodes. For example, if the Quorum drive in node A is assigned to Q:, make sure that the Quorum drive on node B is also assigned to Q:.
    - Ensure that the drive letters for storage are identical in both nodes.
- Verify network access between the Vaults
    - Run the following Powershell command from each Vault to all of your other Vaults:
      Test-NetConnection <IP Address> -port 1858 | findstr "TcpTestSucceeded"

      The result should be: **TcpTestSucceeded : True**

Describe how to register a primary vault in AWS using AMIs

- Follow the prerequisites shown in Vault registration prerequisites in AWS.
- Connect to the DR Vault using RDP.
- Copy the following files to the Primary Vault instance.
    - recpub.key
    - license.xml
- Navigate to C:\Program Files (x86)\PrivateArk\Server.
- Open CMD as Administrator.
- Run the following CAVaultManager PostInstall command to configure the Vault.

```
CAVaultManager.exe PostInstall /AcceptEULA /RecPub "<path to the recpub key>" /LicensePath "<path to the license file>" /AdminPass "<New Administrator password>" /MasterPass "<New Master password" /DRPassword "<New DR password" /CloudVendor <AWS>/CloudRegion <AWS region>
```

1. If the installation completes successfully, the Vault server is up and running and you receive the message:

   `"ITATP146I Postinstall command has been finished successfully."`

-

Describe how to register a primary vault in Azure using the CyberArk image

Register the Primary Vault

- Follow the prerequisites in Vault registration prerequisites in Azure.
- Connect to the Primary Vault using RDP.
- Copy the following files to the Primary Vault instance.
    - recpub.key
    - license.xml
- Navigate to C:\Program Files (x86)\PrivateArk\Server.

- Open CMD as Administrator.
- Run the following CAVaultManager PostInstall command to configure the Vault.

```
CAVaultManager.exe PostInstall /AcceptEULA /RecPub "<path to the recpub key>" /LicensePath "<path to the license file>" /AdminPass "<New Administrator password>" /MasterPass "<New Master password>" /DRPassword "<New DR password" /CloudVendor Azure /VKMName "<VKM URL>" /RDPGateway <RDP Gateway IP>
```

- If the installation completes successfully, you receive the message

```
ITATP146I Postinstall command has been finished successfully.
```

  - Navigate to C:\Cyberark.
  - Run HardenAzureFW.ps1 in PowerShell as Administrator.
  - Reboot the machine to apply hardening.

Deploy the Password Vault Web Access (PVWA)

Identify and describe the steps to install the first and additional PVWAs

Note: You can have a maximum combined total of 60 PVWA and CPM instances in one environment.

The installation procedure consists of the following tasks:

- **Pre-installation**
  - Review Requirements
  - Close all other Applications and log on
  - Run Prerequisites Scripts

- **Installation**
  - Run the PVWA Installation Script
  - Registration (connect to the Vault)

- **Post Installation tasks**
  - Check Installation log files
    - PVWAInstall.log
    - PVWAInstallEnv.log
    - PVWAInstallError.log
    - PVWAInstallErrorEnv.log

  - Check Connection log files
    - CheckConnection.log (information about the PVWA connection to the Vault)
    - ConfigureInstance.log
    - ConfigureVault.log
    - RegisterInstance.log

  - Check user permissions on the web server according to table below

Folder	User/Group	Permission
CredFiles	Administrators	Full control
	Application pool's dedicated user: • IIS AppPool\PasswordVaultWebAccessPool	Full control
VaultInfo	Administrators	Full control
	Application pool's dedicated user: • IIS AppPool\PasswordVaultWebAccessPool	Full control
WebCharts	Administrators	Full control
	Application pool's dedicated user: • IIS AppPool\PasswordVaultWebAccessPool	Full control
	Internet Guest user[1] (IIS_IUSR)	Read & Execute
<Windows folder>\Temp	Administrators	Full control
	Application pool's dedicated user: • IIS AppPool\PasswordVaultWebAccessPool	Full control

- Add Restrictions to credentials file.
- Additional optional steps:
  - Change Authentication
  - Replace self-signed certificate
  - Specify multiple Vault IP addresses
  - Enable FIPS cryptography

- **Hardening**
  - Run the hardening script
  - Perform manual hardening steps
  - Apply post hardening congifurations
  - Harden server in a domain environment (if required)

Evaluate and scope a customer environment to determine the appropriate number of PVWAs and their placement within the network

Small implementation (<1,000 managed passwords)	Mid-range implementation (1,000-20,000 managed passwords)	Large implementation (20,000 – 100,000 managed passwords)	Very large implementation (more than 100,000 managed passwords)
Hardware specifications			
• Quad core processor (Intel compatible) • 8GB RAM • 2X 80GB SATA/SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM	• 2X Quad core processor (Intel compatible) • 16GB RAM • 2X 80GB SATA/SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM	• 2X Eight core processors (Intel compatible) • 32GB RAM • 2X 80GB SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM	• 4X Eight core processors (Intel compatible) • 64GB RAM • 2X 80GB SAS hot-swappable drives • RAID Controller • Network adapter (1Gb) • DVD ROM

Describe the process to correctly harden a PVWA server

You can harden the PVWA server automatically using a script file. The hardening script file performs the following tasks:

- Imports the INF configuration
- Validates server roles
- Enables IIS Anonymous authentication
- Disables IIS Registry shares
- Disables IIS Directory browsing
- Disables IIS WebDAV
- Removes unnecessary IIS Mime types
- IIS SSL/TLS settings
    - Updates IIS SSL\TLS settings
    - Configures ciphers suites
- Policy configuration
    - Enables screen saver policies
    - Configures advanced audit policies
    - Configures Remote Desktop Services policies
- Sets EventLog size and retention
- General auditing, registry, and file system configuration
    - Registry audits

    - Registry permissions
    - FileSystem permissions
    - FileSystem audit
- Disables services

Run the hardening script

If you have installed PSM on the same machine as PVWA before you run the hardening script, in the *PVWA\InstallationAutomation* folder, locate and open the PVWA_Hardening_Config.xml file, and set the IsPSMInstalled parameter to True

In a PowerShell window, run the ***PVWA_Hardening.ps1*** script as Administrator.

Manual hardening steps

Perform the following hardening steps after you have run the hardening script:

- Remove or disable other protocols, services, or clients
    - Only the following protocols services or clients are required for the PVWA server:
        - Client for Microsoft Network
        - File and Printer Sharing for Microsoft Network
        - Internet Protocol Version 4 (TCP/IPv4)

      Remove or disable any other protocols, services, or clients from your network connection properties.

      Also disable IPv6 unless it is specifically required for your PVWA server.
- Remove Adobe Flash

Describe various PVWA load balancing options

Two main scenarios: High Availability or Load Balancing

Load balancer requirements

The load balancer must not alter page content, or it should include a mechanism to prevent pages from being altered.

The load balancer must not alter the application path hierarchy (leave the default application path as it is).

The load balancer must support 'sticky sessions'.

Configure the PVWA to work with the load balancer

In the web.config file, for the LoadBalancerClientAddressHeader parameter, enter the HTTP Header field name from which the PVWA reads the client IP.

This allows the Vault to log incoming requests as if their source is the the real client IP and not the load balancer.

Prepare a Windows server for PVWA installation

Close applications and log on

- Close all other applications currently running on your computer
- Log on to Windows as the Administrator user

Run the PVWA server prerequisites script

The **PVWA_Prerequisites** script automates and performs the following tasks:

- Verifies .NET version
- Installs Web server roles, for details, see Web server roles
- Disables IPv6
- Configures the self-signed certificate
- Sets IIS SSL TLS configuration

Deploy the Central Policy Manager (CPM)

Identify and describe the steps to correctly harden a CPM server

If the PVWA and CPM are installed on the same machine, make sure to run the CPM hardening script after you have run the PVWA hardening script.

You can harden the CPM server automatically using a script file. The hardening script file performs the following tasks:

- Imports the INF configuration
- Validates server roles
- Sets policy configuration
    - Enables screen saver policies
    - Configures advanced audit policies
    - Configures Remote Desktop Services policies
- Sets EventLog size and retention
- General auditing, registry, and file system configuration
    - Registry audits
    - Registry permissions
    - FileSystem permissions
    - FileSystem audit

- Creates three local Windows users that run the CPM services
- Disables services
- Disables DEP on files used by the CPM

If you have installed PSM on the same machine as CPM

Before you run the hardening script, in the CPM\InstallationAutomation folder, locate and open the CPM_Hardening_Config.xml file, and set the IsPSMInstalled parameter to True.

If you want to automatically enable FIPS cryptography during hardening, before you run the hardening script, in the CPM\InstallationAutomation folder, locate and open the CPM_Hardening_Config.xml file. Set the EnableFIPSCryptography parameter to Yes.

Hardening CPM servers in a domain

When CPM servers are part of a domain, you must back up the existing Group Policy Object (GPO), and create a new one importing the one provided in the installation folder.

Identify and describe the steps required to prepare a Windows server for CPM installation

PVWA must be installed before you can install CPM.

Enable a secure channel between the CPM and PVWA

If PVWA is configured to communicate through a secure channel (HTTPS), the CPM machine needs to trust the PVWA SSL certificate.

Import the CA certificate from the CA that issued the PVWA's SSL certificate to the CPM server.

Make sure that the CPM server can access the CRL Distribution Points referenced in the PVWA's certificate.

Run the CPM prerequisites script

The CPM_PreInstallation.ps1 script automates and performs the following tasks:

- Verifies .NET version
- Sets IIS SSL TLS configuration

Identify and describe the steps to install the first and additional CPMs

The installation procedure consists of the following tasks:

- **Pre-installation**
    - Review Requirements
    - Run Prerequisites Scripts

- **Installation**
    - Run the CPM Installation Script
    - Registration (connect to the Vault)
- **Post Installation tasks**
    - Create a trusted network area
    - Check installation log files
        - CPMInstall.log
    - Check the CPM services (These services are started automatically after installation)
        - CyberArk Password Manager
        - CyberArk Central Policy Manager Scanner
    - Add restrictions to credentials file
- **Hardening**
    - Run the hardening script (apply GPO policy if needed)
    - Apply post hardening configurations

Identify and describe the steps to rename a CPM

Article # 000026086

1) Stop CPM services.

The following steps need to be completed using PAClient;

2) Rename the <ExistingCPMUser>_* safes to the new names except the three shared safes: PasswordManger_Pending, PasswordMangerShared, PasswordMangerTemp

3) Rename the CPM user and reset its password

The following steps then need to be completed on the CPM Server;

4) Re-cred user.ini using CreateCredFile Utility

CreateCredFile.exe user.ini Password /Username {NewCPMUser} /Password {password} /AppType CPM /EntropyFile

5) Update the APIKey file:

- Revoke the old key

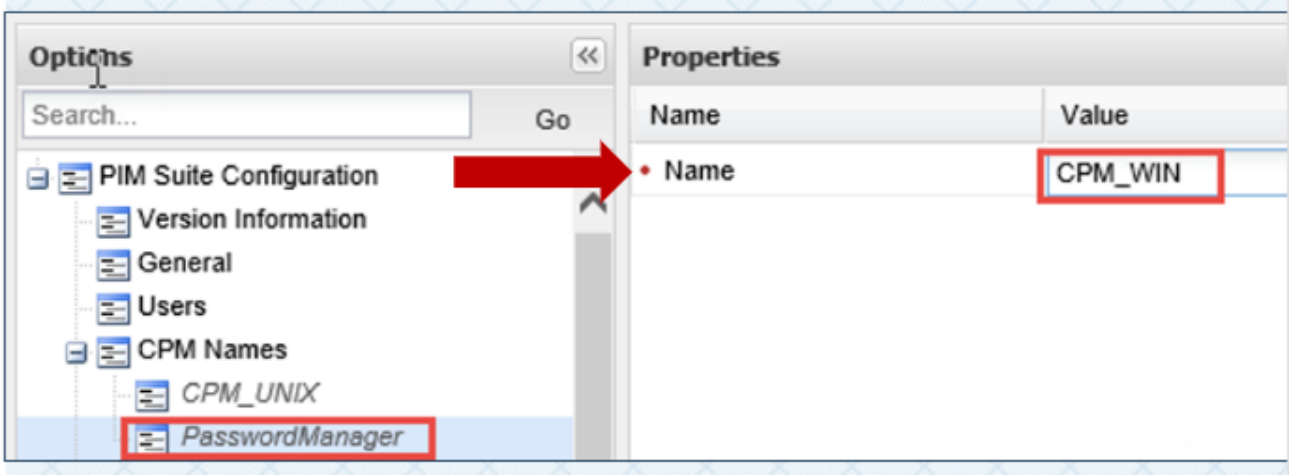
apikeymanager revoke -t <OldCPMUser> -u Administrator -a https://<PVWA direct URL>/passwordvault/api/

- Add the new key

apikeymanager add -f apikey.ini -t <NewCPMUser> -u Administrator -a https://<PVWA direct URL>/passwordvault/api/

The following step needs to be completed using PVWA Options:

6) Update <ExistingCPM> to the new CPM user name in PVWA (Options > CPM Names).



7) Restart CPM services.

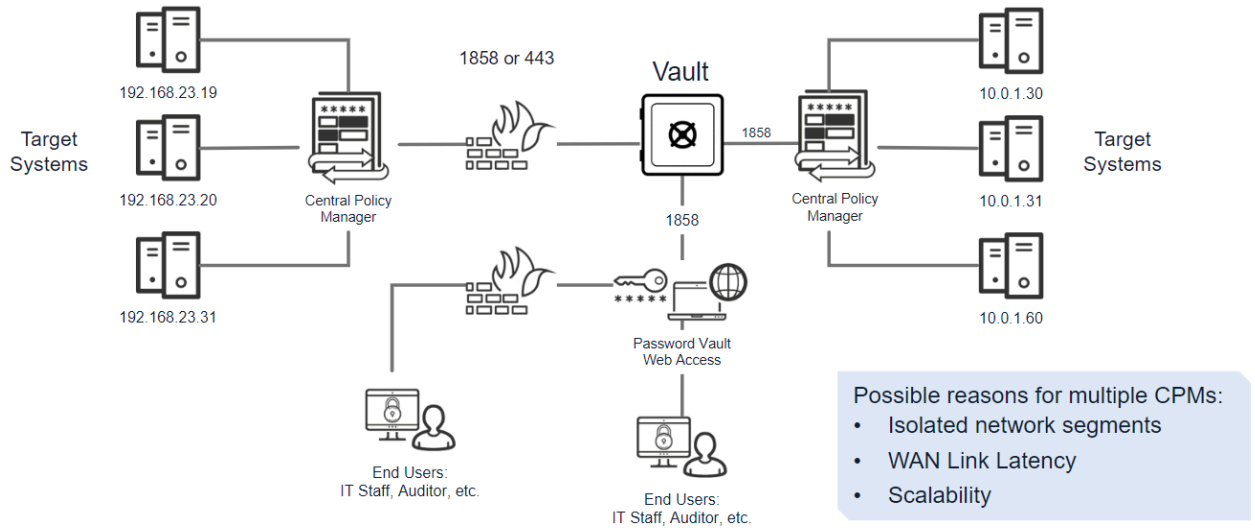
Evaluate and scope a customer environment to determine the number of CPMs required and their placement within the network

A CPM should be installed on the network with the fewest network hops in relation to the target systems the CPM is intended to manage privileged accounts. This will likely result in CPM network traffic traversing one or more network firewalls and routers when communicating with the Vault server.

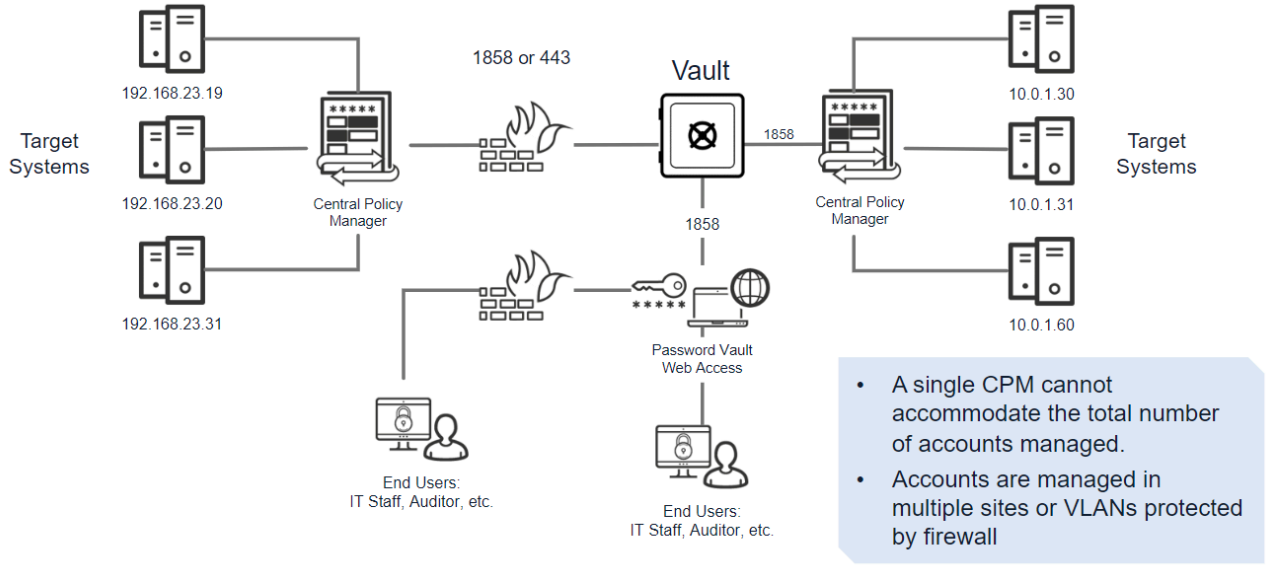
The CPM will effectively communicate to the Vault over the secure CyberArk VPN, tcp_1858 (preferred) or can be configured to use port 443 if preferred by the customer.

This recommendation reduces network traffic across WAN links and enables the CPM to operate at peak efficiency.

BASIC DEPLOYMENT, MULTIPLE SITES



USE CASES



Identify and describe Fault Tolerant Architecture components

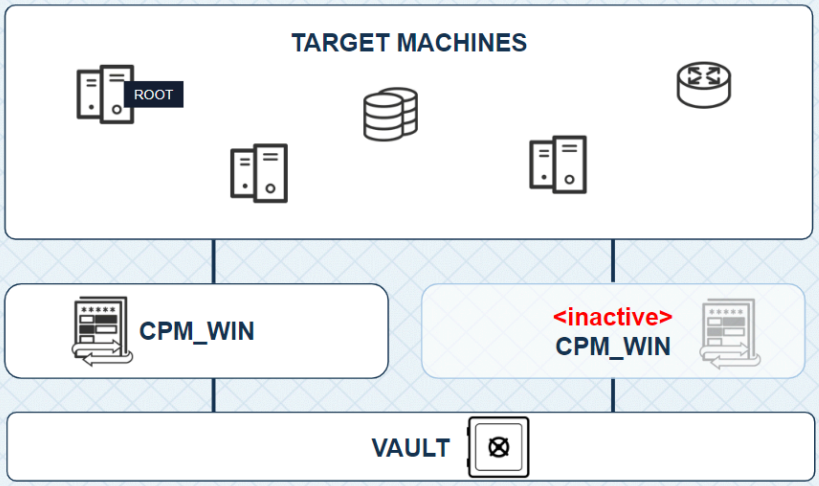
In order to prevent a scenario where the CPM is unavailable, you can set up a Disaster Recovery (DR) "active-passive" cluster by installing and configuring a second CPM instance.

If the primary CPM is down, you can manually switch over to the second instance, the DR CPM.

Only one instance of the CPM can be active at a given time, a manual procedure is required to transfer the license.

MULTIPLE CPM SERVERS – ACTIVE-PASSIVE

- CPM is installed at multiple locations, but only enabled at one
- Activating and deactivating CPMs is a manual process
- Inactive CPMs will need to assume a license from the active CPM. This is commonly seen in DR implementations.



Determine the quantities and locations of components needed to provide a fault tolerant architecture to meet customer needs

Identify and describe distributed architecture components

Determine the quantities and locations of components needed to provide a distributed architecture to meet customer needs

Deploy the Privileged Session Manager (PSM)

Identify and describe the steps to install the first and additional PSMs

The installation procedure consists of the following tasks:

- **Plan Capacity and machine sizing**
- **Ready the PSM server machine**
  - Install Remote Desktop Services (RDS) Session Host Role
  - Verify you have the required number of RDS CALs to enable you to access the RDS server
- **Automatic Installation via automatic installation tool will perform the following steps:**
  - Install prerequisites
  - Install Remote Desktop Services rules
  - Disable NLA authentication
  - Update the RDS security layer
  - Install PSM
  - Post Installation tasks
  - Hardening

- Registration

Run the installation tool

- From the installation CD, copy the PSM folder to the component server and unzip**.**
- Open CMD and run

```
CD <PSM CD-Image Path>\PSMAutoInstallationTool

PSMAutoInstallationTool /vaultip <Vault IP address> /vaultuser <Vault username for installation> -/accepteula yes
```

- Restart- The tool runs the PSM installation stages. When a restart is required, the user is prompted to press Enter, restarting the machine. When the user logs in to the machine again, the tool continues from the relevant step.

- Vault user credentials - If you are using a Vault username and password, after the last restart you are prompted to enter a password. Enter the password and click Enter. You can use the cred file to avoid entering the password interactively.

Identify and describe preparation considerations for PSM deployment

- **Plan Capacity**
  Determine the amount of storage required in the Vault or external storage device to store session recordings before installation.
- **Determine the hardware required for PSM**
  The number of required PSM severs depends on load-balancing, high availability and network topology considerations.

Evaluate and scope a customer environment to calculate the amount of storage that should be available to the PSMs for PSM recordings

SIZING CALCULATIONS (PSM SERVER)

$$(S_{PSM}) = (C_{session})(t_{session})(R_{session\ recording}) + 20GB$$

- SPSM = Required storage on PSM Server
- Csession = Maximum Number of Concurrent Sessions
- tsession = Average length of recorded session
- Rsession recording = Average bit rate of recorded video
  - 100 KB/min – average SSH session
  - 200 KB/min – average low activity RDP session
  - 300 KB/min – average high activity RDP session with rich wallpaper
- (25 sessions) x (180 minutes/session) x (300 KB/minute) + 20GB = 21.35GB

Evaluate and scope a customer environment to calculate the amount of storage that should be available to the Vault and PAReplicate for PSM recordings

3 info required:

- **Size of session recordings**
  Usually 250 kb/min
- **Activity in your enterprise**
  The number of concurrent sessions that PSM will create and store in the Vault determine the size of your implementation.
- **Recordings Retention Period**
  The length of time that recordings will be retained according to your enterprise audit policy.

Example

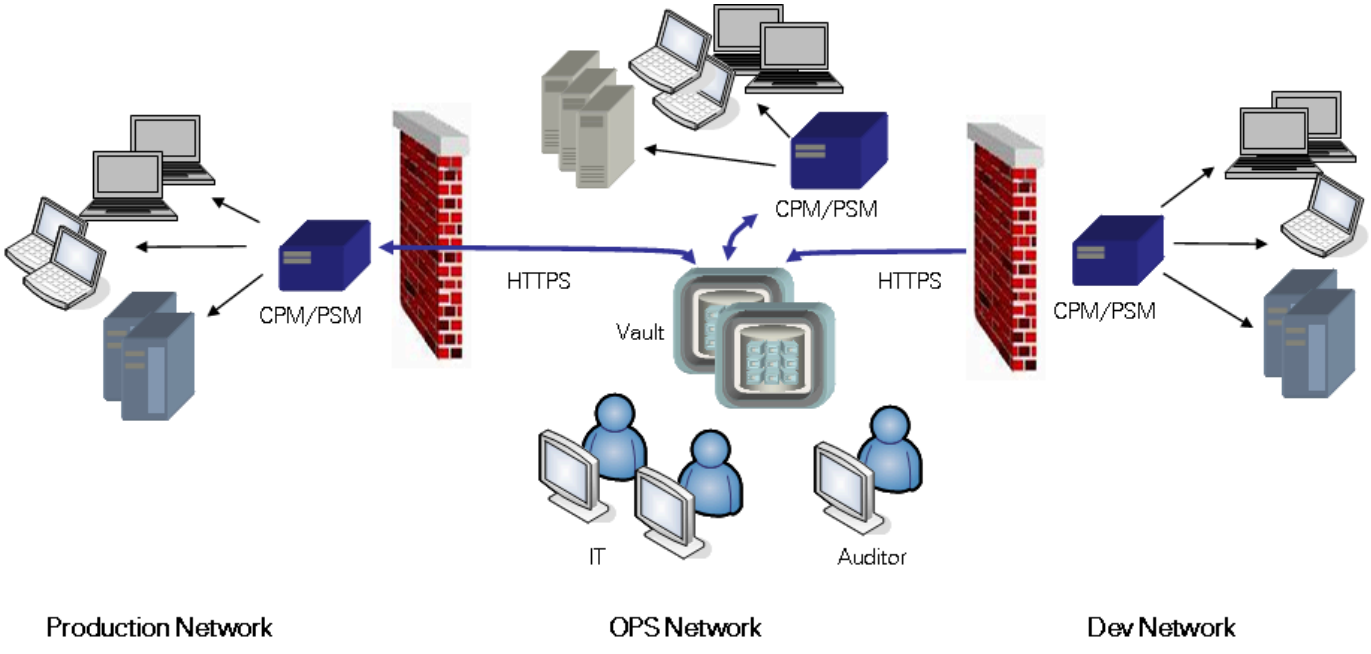
100 daily sessions of 10 minutes @250KB/Min with a retention period of 3 years:

100 x 10 x 365 x 3 x 250 = 273.750.000 KB = ~273 GB.

Evaluate and scope a customer environment to determine the appropriate number of PSMs and their placement within the network

The number of required PSM severs depends on load-balancing, high availability and network topology considerations.

PSM server can be installed in each network segment to communicate with the remote machines using native protocols and without the need to open the enterprise firewall, as shown in the following diagram.



PSM can also be installed on the same machine as the CPM or the PVWA, reducing the number of machines to maintain.

Identify and describe the steps to prepare a Windows server for PSM installation

Describe post-installation processes

- **Review PSMInstall.log** to ensure installation completed successfully.
- **Check that PSMConnect and PSMAdminConect users exists on PSM Machine**
- **Check that PSMShadowUsers group is created on PSM Machine**
- **Check that following safes have been created on Vault**:
    - PSM
    - PSMLiveSessions
    - PSMUnmanagedSessionsAccounts

  PSMRecording safe will be created dynamically when the first recording is created
- **Check that following users and groups are created on Vault**
    - PSMAppUsers
    - PSMMaster
    - PSMGW_<machine name>
    - PSMApp_<machine name>

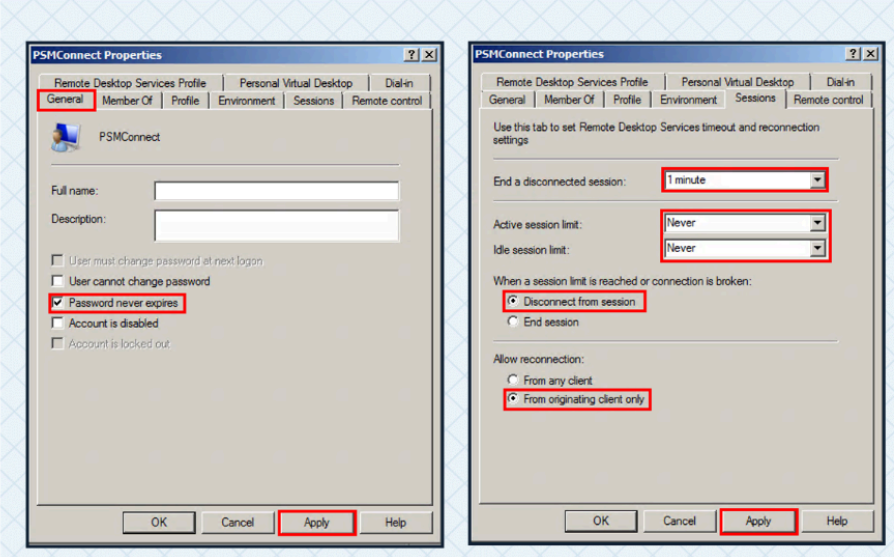
The post installation stage configures:

- Disables the screen saver for local PSM users
- Configures users for PSM sessions
- Enables PSM for web applications (optional)
- Enables users to print PSM sessions (optional)

Configure PSMuser sessions

CONFIGURE PSM USER SESSIONS

- "Active session limit" and "Idle session limit" must be set to Never.



Harden the server using the script

Run the AppLocker Script

Register the PSM

Enable and configure PSM in the Master Policy

Identify and describe the steps to complete an HTML5 Gateway installation

HTML5 Gateway Docker deployment

This section describes how to install the PSM HTML5 Gateway as a docker.

Copy the HTML5 Gateway\PSMGWDocker directory located in the CD image to the Linux host.

Go to that directory.

Run the following command to grant execution rights to the setup script.

```
chmod +x html5_installation.sh
```

Run the following command to execute the setup script

```
sudo ./html5_installation.sh localimage
```

Install PSM HTML5 Gateway using an RPM package

Install required libraries:

```
yum install cairo libpng libjpeg java java-devel openssl
```

- **Deploy the HTML Webapp**
- **Deploy the HTML5 service**
- **Secure the connection between guacd and the webapp**
- **Secure the webapp and JWT validation endpoint**
- **Hardening**
- **Secure the Tomcat server**
- **Secure the connection between the end user and Tomcat**
- **Secure the connection between guacd and PSM**

Identify and describe the steps to prepare a UNIX server for HTML5 Gateway installation

Describe various PSM load-balancing options

Installing multiple PSMs in a load balancing configuration offers you enhanced availability, improved performance and better utilization of hardware resources compared to an active-passive cluster.

The load balancing architecture relies on an external tool that reflects multiple PSM servers as a single IP or DNS address. PSM load balancing supports off-the-shelf load balancers.

PSM provides a service to determine the PSM service availability (health) and reports it, upon request, to the load balancer.

Describe how to correctly harden a PSM server

After using hardening scripts the followings additional steps are needed:

- **Disable the screen saver for the PSM local users**
- **Configure PSMConnect for PSM sessions**
    - In End a disconnected session, specify 1 minute.
    - In Active session limit, specify Never.
    - Select Disconnect from session, in the section When a session limit is reached or connection is broken
    - Select From originating client only, in the section Allow Reconnection
- **Configure the PSMAdminConnect user**
    - In End a disconnected session, specify 1 minute.
    - In Active session limit, specify Never.
    - In When a session limit is reached or connection is broken, select Disconnect from session
    - In Allow reconnection, select From originating client only.

Describe various PSM load-balancing options

Installing multiple PSMs in an load balancing configuration offers you enhanced availability, improved performance and better utilization of hardware resources compared to an active-passive cluster.

The load balancing architecture relies on an external tool that reflects multiple PSM servers as a single IP or DNS address. PSM load balancing supports off-the-shelf load balancers.

PSM provides a service to determine the PSM service availability (health) and reports it, upon request, to the load balancer.

A pre-requisite for this step is that PSM servers must have a virtual IP/DNS address.

- **Install the first PSM on the first PSM server, then install the second PSM on the second and any additional PSM servers.**
- **Log onto the PVWA as an administrator user and define the new PSM server. Reference the RDS farm DNS record as follows:**
    - Click ADMINISTRATION to display the System Configuration page, then click Options to display the Web Access Options parameters.
    - Display the Privileged Session Management parameters, then expand Configured PSM Servers
    - Copy an existing configured PSM Server and paste it in Configured PSM Servers to create an additional configured server that you can change.

      It is important to copy an existing PSM server and modify it, and not use the Add PSMServer option, so that you retain the same PSMProtocolVersion property for the PSM Farm and for the configured servers
    - Change the following properties
        - ID – The RDS farm name.
        - Name – The name of the PSM group server
    - Expand Connection Details, then select Server and specify the following properties
        - Address – Specify the virtual IP address of the cluster.
        - Safe - The Safe where the account for the logon account for the PSM Server is stored.
        - Folder - The folder where the account for the logon account for the PSM Server is stored

- Object - The name of the account that is used by the logon account for the PSM Server.
- AdminObject – An internal account used to facilitate live session monitoring. This account is created and managed automatically by the CPM and must not be managed manually.

- **In the PVWA, enable the PSM cluster with the relevant platform. For example, WindowsLocal**
  - Click ADMINISTRATION to display the System Configuration page, then click Platform Management to display a list of supported target account platforms.
  - Select the platform to configure for the PSM cluster, then click Edit.
  - Expand UI & Workflows, then select Privileged Session Management; the PSM parameters for this platform are displayed with their default values.
  - In the Properties list, specify the following property:
  - ID – The unique ID of the PSM cluster server. This ID is taken from the list of PSM Servers configured in Options.
  - Click Apply to save the new configurations.

Deploy the PSM For SSH

Identify and describe the steps to install the first and additional PSMs for SSH

The user who will create the environment for PSM for SSH in the Vault during the installation process must have the following permissions in the Vault:

- Add Safes
- Audit Users
- Add/Update Users
- Manage Server File Categories

If you are using PSM for SSH with AD Bridge, from the installation's Prerequisites folder run the following:

```
rpm –i libssh-<version>-<build_number>.<arch>.rpm
```

if InstallCyberArkSSHD= Yes or InstallCyberArkSSHD=No

```
rpm –i <rpm-file-name>
```

if InstallCyberArkSSHD = Integrated (this is the default method)

```
rpm –i <infra rpm location >/CARKpsmp-infra-<version>.<arch>.rpm

rpm –i <CARKpsmp rpm location>/CARKpsmp-<version>.<arch>.rpm
```

Describe how to configure usrmng accounts

PSM for SSH identifies the following users as maintenance users when they connect to the PSM for SSH server:

proxymng

proxymng<number>

Additional users that are specified in the PSMP_MaintenanceUsers parameter in the sshd_config configuration file.

Create a maintenance user when InstallCyberarkSSHD is set to Yes or No

Create an extra maintenance user, in addition to the built-in root user, so that a maintenance user can always connect to the PSM for SSH server to perform maintenance, even when remote access is forbidden to the root user.

You can configure more maintenance user names by adding the PSMP_MaintenanceUsers parameter to the sshd_config configuration file.

Create a maintenance user when InstallCyberArkSSH is set to Integrated:

In /etc/ssh/sshd_config, in the SSHD configuration file, add the following parameter:

AllowGroups PSMConnectUsers <MaintenanceGroupName1>..<MaintenanceGroupNameN>

Describe the process to correctly harden a PSM for SSH server

The PSM hardening procedure on the PSM for SSH server machine enhances PSM for SSH security.

The following table describes hardening methods for supported platforms.

Red Hat Linux, Centos automatic hardening during installation

SUSE Manual hardening

Describe how to prepare a UNIX server for PSM for SSH installation

- **Verify the Operating System**

  Make sure the operating system installed on your server is supported by PSM for SSH

- **Verify the installation package digital signature**
  - Import the RPM-GPG-KEY-CyberArk public key that is provided with the installation package using:

```
rpm --import RPM-GPG-KEY-CyberArk
```

- Verify the signature of the RPM package, by running the following command:

```
rpm -K -v <package_name.rpm>
```

Configure authentication methods

Method	Description
Privileged SSO	Users connect to target machines transparently, without being prompted for a username or password, using one of the following methods: • **Privileged SSO account using password** • **Privileged SSO account using SSH keys** • **Privileged SSO account using SSH certificate**
Non-privileged SSO	Users are prompted for logon credentials: • **Accounts can be created with a predefined username, but no password** - Users must supply the password before they can connect to the target machine. • **Accounts can be created without a username or a password** - Users must supply these logon credentials before they can connect to the target machine.

Describe the steps required to combine a Vault and a PVWA authentication method to create two-factor authentication

Configure a primary authentication method on PVWA

- In the System Configuration page, click Options, then expand Authentication Methods; a list of the supported configuration methods is displayed.
- Select an authentication method to display its configuration.
- Set any of the following parameters to modify the authentication method for users.
  - Id – The identifier of the authentication module. This parameter is configured automatically during installation.
  - DisplayName – The display name of the authentication method that will be displayed in PVWA.
  - Enabled – Whether or not the authentication module can be used. This is configured during installation, depending on whether or not the authentication method is selected.
  - LogoffUrl– A URL to redirect to on logoff. This cannot be set during installation and must be set manually afterwards. Specify the whole URL, including HTTP/HTTPS. For example, https://www.company.com.
- Click Apply to save the new configurations and apply them immediately.

Configure a secondary authentication method

The CyberArk Vault supplies the following secondary authentication features:

- LDAP Authentication
- RADIUS Authentication
- CyberArk Authentication

Secondary authentication is configured in the authentication parameters for each authentication method.

- In the System Configuration page, click Options, then expand Authentication Methods; a list of the supported configuration methods is displayed.
- Select an authentication method to set secondary authentication.
- Set any of the following parameters:

Parameter	Description
UseVaultAuthentication	Whether the user must provide the Vault user's password manually and the credentials will be passed to the Vault for authentication, without relying on a 3rd party authentication server. This can be used in conjunction with a 3rd party authentication to enforce two factor authentication (that is, require an additional Vault authentication in addition to the primary IIS authentication). ⓘ This cannot be disabled for CyberArk authentication
UseRadius	Whether or not RADIUS will be used to connect to the Vault. In order to enable this parameter as a secondary authentication method in addition to the IIS authentication method, the UseVaultAuthentication parameter must be enabled.
UseLDAP	Whether or not LDAP authentication will be used to authenticate users to the Vault. In order to enable this parameter as a secondary authentication method in addition to the IIS authentication method, the UseVaultAuthentication parameter must be enabled.

- Click Apply to apply the configuration changes immediately

Describe how to configure PKI authentication

During installation, the PVWA is automatically configured to support PKI authentication for users who select this authentication method.

Enable PKI in PVWA interface

- Using Notepad (not Notepad++), open the IIS configuration file. By default, this is

  %WinDir%\System32\Inetsrv\Config\applicationHost.config.

- At the end of the file, add the following lines:

```
<location path="Default Web Site/PasswordVault/api/auth/pki/logon">
    <system.webServer>
            <security>
                    <access sslFlags="Ssl, SslNegotiateCert, SslRequireCert" />
            </security>
    </system.webServer>
</location>
```

- Restart IIS server.

Describe how to configure RADIUS authentication

the Vault enables users to log on via Remote Authentication Dial-In User Service (RADIUS) authentication, using logon credentials that are stored in the RADIUS server. The Vault also supports RADIUS challenge-response authentication, where the server sends back a challenge prompting the user for more logon information, such as additional authentication information contained on external tokens.

Requirements

In order to enable users to authenticate using RADIUS authentication, you need the following:

■ RADIUS Server

■ Certificate – A Vault certificate to create an initial secured session prior to the RADIUS authentication. This certificate is optional, but recommended.

■ RADIUS Secret – A password known to only the RADIUS server and the CyberArk Vault. This password can contain up to 255 characters.

Configure RADIUS Authentication

Preparation

- **In the RADIUS server, define the CyberArk Vault as a RADIUS client/agent.**
- **Gather the following information from the RADIUS server:**
  - RADIUS server hostname, FQDN, or IP address
  - RADIUS server Port
  - Host name of the RADIUS client (Vault machine). This name must be identical to the name you entered for the RADIUS client/agent.
  - Password secret
- **Configure an organization SSL Certificate of the Vault Server**
- **Integrate the Vault with the RADIUS Server**
  - Stop the Vault server.
  - In the Vault installation folder, run **CAVaultManager** as administrator with the **SecureSecretFiles** command, as shown below, to create a file that contains an encrypted version of the RADIUS secret.

    You can specify the full path of the file that will contain the encrypted secret, and the secret itself. This file may be in DAT, INI, or TXT format.
  - Navigate to /Server/Conf and open DBParm.ini
  - Set the RadiusServersInfo parameter.

For RADIUS high availability**: You can specify more than one RADIUS server by separating the details of each server with a comma.**

```
RadiusServersInfo=radius1.mycompany.com;1812;vaulthostname;RadiusSecret_Radius1.dat,radius2.mycompany.com;1812;vaulthostname;RadiusSecret_Radius2.dat
```

- **Start the Vault server.**

Describe how to configure SAML authentication

SAML authentication enables you to implement an Identity Provider (IdP) solution and benefit from an SSO workflow across multiple domains.

After you configure SAML authentication, all users can use this authentication method. Whether they have been provisioned using LDAP integration or were created manually as CyberArk users.

PAM - Self-Hosted supports SAML version 2.0.

To configure SAML in PAM - Self-Hosted, you need to configure the PVWA and the PasswordVault web.config file.

To configure the PVWA:

- **Log on to the PVWA.**
- **Click Administration > Configuration Options > Options.**
- **In the Options pane, expand Authentication Methods, and click saml.**
- **In the Properties pane, set the following fields:**
  - Enabled Set to Yes.
  - LogoffUrl Specify the logoff page of your IdP.

    If your IdP does not have a logoff URL, clear this field. Users will remain authenticated to the PVWA as long as they are authenticated to the IdP.
- **In the Options pane, right-click Access Restriction, and then select Add AllowedReferrer.**
- **In the Properties pane, in BaseURL, specify the URL of your IdP.**
- **Click Apply to save the new configurations.**

To edit the configuration file:

- In the PasswordVault installation folder (the default location is \Inetpub\wwwroot\PasswordVault), make a copy of the saml.config.template file, and rename it to saml.config.
- Edit the saml.config file as follows:
  - Parameter Description
  - SingleSignOnServiceUrl The login URL of your IdP.
  - Certificate The base 64 text representation of the certificate that is configured for your IdP as the SAML response signing certificate.
    This is used by the PVWA to verify the authenticity of the responses.
  - PartnerIdentityProviderName Enter the IdP identifier that enables the PVWA to identify the IdP. Also known as the EntityId of the identity provider.
  - ServiceProvider Name The Issuer string that enables the PVWA to identify itself to the IdP. Also known as the EntityId of the service provider.

    It must be identical to the Audience defined in the IdP.

To support signed requests

Add the following to the ServiceProvider element:

```
<LocalCertificates>
   <Certificate FileName="<local certificate path>" Password="<the password you set for the certificate>" />
</LocalCertificates>
```

Add the following attribute to the PartnerIdentityProvider element:

```
SignAuthnRequest="true"
```

To support encrypted assertion:

Add the following within the ServiceProvider element:

```
<LocalCertificates>
   <Certificate FileName="<the exported certificate path>" Password="<the password you set for the certificate>" />
</LocalCertificates>
```

Supply the certificate's public key to the IdP to encrypt the assertion.

To support force authn

add the following attribute to the PartnerIdentityProvider element:

```
ForceAuthn="true"
```

Identify and describe the components that work with each authentication method

CyberArk Vault

- LDAP Authentication
- RADIUS Authentication
- CyberArk Authentication

Password Vault Web Access

- Password
- Windows
- Radius
- PKI
- LDAP
- Oracle SSO
- SAML
- Additional third-party authentication servers can be easily customized.

PrivateArk Client

- Password
- Radius
- LDAP

CPM

- Password
- Password with a certificate on a hardware token
- Radius
- PKI on Windows

PACLI

- Password
- Radius

Privileged Access Manager - Self-Hosted SDK

- Password
- Radius
- SAML
- PSM for SSH with SSH keys

Describe how to generate a custom connection component using the PGU

Perform integration tasks, including integrating with NTP, SMTP, SNMP, LDAP, and Syslog/SIEM

SMTP

The Event Notification Engine (**ENE**) automatically sends email notifications about PAM - Self-Hosted activities to predefined users. It is installed automatically as part of the Vault server installation as a service.

Enable the ENE

After installing the Vault, the ENE must be enabled so that you will be able to receive email notifications about the Vault activities.

The ENE is installed as part of the Vault server installation as a service called **Cyber-Ark Event Notification Engine.**

After the ENE has been configured, the ENE setup wizard will only be enabled if the SMTP address is set to 1.1.1.1. To rerun the ENE setup wizard, in the Notification Settings page, set the SMTP address to 1.1.1.1 then re-invoke the ENE setup wizard.

Before you begin:

- Log on to the PrivateArk Administrative Client as an administrator user.
- Make sure that the business email address of the user who will issue ENE notifications is specified in their user properties. This user must belong to the Vault Admins group. By default, this is the Administrator user.

Enable the ENE:

- Log on to the PVWA as an administrator user.
- Make sure that this user belongs to the VaultAdmins group so that you have the required permissions to enable ENE notifications.
- In the PVWA, click the Administration button, and then click Configuration Options.
- In the System Configuration page, click Setup Wizard.



- On the Vault setup page, select Email notifications, and then click Next.
- On the Configuration page, enter the following
    - SMTP address
    - Sender Email
    - Sender Display Name
    - SMTP Port
    - Recipients Domain
    - CA-PVWABaseURL (The URL of the machine where the PVWA is installed. For example, https://www.myserver.com.)
- Click Finish.

Authenticated and encrypted email notifications

After you have configured encryption for email notifications, you can add an additional level of security by configuring authentication too.

In the NotificationEngine Safe, create an account that will authenticate to your mail server. Make sure this account has permission to send from the mailbox specified in the Mail parameter.

In Administration > Notification Settings, expand EventNotificationEngineSendMethod > SendMethod > Security and set the following parameter:

SMTPAccountName The name of the account you created in step 1 and stored in the NotificationEngine Safe.

Note: This is not the username.

Configure encrypted email notifications

- In the SMTP server, export the trusted root certificate that issued the SMTP server's TLS certificate in Base-64 encoded X.509 format.
- Copy the exported certificate to the ENE server (also the Vault server).
- In Administration > Notification Settings, expand EventNotificationEngineSendMethod > SendMethod > Security and set the following parameters:
    - EnableTLS Yes
    - TLSRootCertificatePath the location of the certificate you stored on the ENE/Vault server in step 2
- In Administration > Notification Settings, expand EventNotificationEngineSendMethod > SendMethod > Servers > Server and set the following parameters:
    - CertificateAlias The value that appears in the "Issued to:" field in the SMTP server's TLS certificate.

SNMP

Configure Remote Monitoring

The Remote Monitoring uses SNMP to send Vault traps to a remote terminal. This enables users to receive both Operating System and Vault information, as follows:

- Operating System information:
- CPU, memory, and disk usage
- Event log notifications
- Service status
- Component-specific information:
- Password Vault and DR Vault status
- Password Vault and DR Vault logs

CyberArk provides two MIB files (for SNMP v1 and SNMPv2) that describe the SNMP notifications that are sent by the Vault. These files can be uploaded and integrated into the enterprise monitoring software. These MIB files are included in the PAM - Self-Hosted installation package:

CYBER-ARK-MIB-V1.txt – Used to implement SNMP v1.

CYBER-ARK-MIB-V2.txt – Used to implement SNMPv2.

Configuration

- **In the remote control agent configuration file, PARAgent.ini, specify the following parameters:**
    - **AllowedMonitoredServices** The name of the system services that can be monitored from a remote location. In the Service Properties window, specify the name of the service exactly as it appears in the Service Name field.
    - **MonitoredEventLogNames** The names of the event logs of activities that have taken place since the Server started, such as Application, Security, and System.
    - **SNMPHostIP** The IP address of the remote computer where SNMP traps will be sent. Separate multiple IP addresses with a comma.

- **SNMPTrapPort** – The port through which SNMP traps will be sent to the remote computer. You can specify either port 161 or 162. The default port is 162.
- **SNMPTrapInterval** – The number of seconds that pass between notifications. The default value is 30.
- **SNMPCommunity** – The name of location where the SNMP traps originated.
- **SNMPVersion** – The SNMP version that will be used to send SNMP notifications. Specify any of the following values:
  - v1 – The Vault will support SNMPv1 with a unique OID for each trap.
  - v2 – The Vault will support SNMPv2. This is the default value.
  - Compatibility – The Vault will send SNMP notifications using the format used in Vault versions prior to version 5.0

- **Specify the following parameters to enable users to receive SNMP notifications**.
  These values comprise interval in seconds between checks and the percentage in usage that would initiate a notification, as shown in the following example:

  SNMPTrapsThresholdCPU=30,80

  - SNMPTrapsThresholdCPU
  - SNMPTrapsThresholdPhysicalMemory
  - SNMPTrapsThresholdSwapMemory
  - SNMPTrapsThresholdDiskUsage
  - SNMPTrapsThresholdServiceStatus
- **From the Control Panel, display the available services, and restart the PrivateArk Remote Control Agent service**

LDAP

The LDAP integration parameters specify information required by the CyberArk Vault to recognize external directories and create User accounts and Groups. A different set of directory configurations define each external directory that the Vault will work with.

After each LDAP directory has been configured in the PVWA, these parameters are stored in the LDAPConf.xml in the VaultInternal Safe. Do not modify the parameters directly in these files.

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/LDAP%20Integration%20-%20Introduction.htm?Highlight=LDAP%20integration#LDAP

SIEM

CyberArk can integrate with SIEM to send audit logs through the syslog protocol, and create a complete audit picture of privileged account activities in the enterprise SIEM solution. These audit logs include user and Safe activities in the Vault, which are transferred by the Vault to various SIEM applications.

CyberArk supports the following out-of-the-box SIEM solutions :

- HP ArcSight
- RSA enVision

- IBM QRadar
- McAfee ESM

You can also use the sample XSL translator file or create a custom file, as described in Create a Custom XSL Translator File.

CyberArk's flexible configuration enables you to:

- Define one or more target syslog servers
- Specify dynamic format translators
- Filter the events that are sent to all the configured syslog servers over encrypted or non-encrypted protocols.

The configuration is built as a list of values. Each set of parameter values must be specified in correlation with the other parameter values in the configuration. This allows the system to determine the settings for each target server.

The Vault can use any of the following protocols to send messages:

Type	**Protocol**
Encrypted protocols	TLS
Non-encrypted protocols	TCP
	UDP

https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/DV-Integrating-with-SIEM-Applications.htm

NTP

Note: Time synchronization is critically important in CyberArk PAS architecture. Even more so when implementing the CyberArk Cluster Vault Management solution. In the following exercise we will integrate both nodes of the cluster vault with an external time source.

- **Logon as Administrator to the passive node of the cluster.**
- **Using Windows File Explorer navigate to 'C:\Program Files(x86)\PrivateArk\Server\Conf'.**
- **Edit the dbparm.ini file adding the following line to the end of the file. This will create inbound and outbound firewall rules that will allow the vault to communicate to the NTP server.**

```
[NTP]
AllowNonStandardFWAddresses=[10.0.0.2],Yes,123:outbound/udp,123:inbound/udp
```

- **Enable the Windows Time service using the Windows Services applet .**
- **Double click “Windows Time” to display the service properties.**
- **Update the Startup type to Automatic (Delayed Start) and click OK.**
- **Start the Windows Time service.**
- **If needed repeat the above procedures on the active node of the cluster before proceeding.**
- **To commit the changes made to the DBParm.ini file, we must restart the PrivateArk Server service.**

Performance tune the solution

Identify and describe the steps to convert a platform from PMTerminal to TPC

Migrate from PMTerminal to TPC

This section contains information about migrating plugins and platforms from PMTerminal to TPC, and describes the differences between PMTerminal and TPC.

PMTerminal was an engine used to develop plugins for terminal cases over SSH or Telnet, or when running a script. TPC is a newer engine that provides enhanced capabilities and was developed to replace PMTerminal.

CyberArk strongly recommends that you migrate your plugins and platforms from PMTerminal to TPC. PMTerminal reached its end of support date on December 31, 2021.

When you migrate a plugin, you need to migrate both the plugin and the platforms that use the plugin. During the migration, the plugin is modified to run over TPC instead of PMTerminal, and the platform's configuration is modified to use the TPC EXE file instead of the PMTerminal EXE file.

TPC supports all functionality that exists in PMTerminal, with a few exceptions. There are also cases where TPC implements features differently from PMTerminal in a plugin.

You can migrate platforms using the Platform Migration tool, which automatically migrates multiple platforms at one time. Or you can migrate platforms manually, one-by-one, using the PVWA.

Perform the following steps for each platform that you want to migrate.

Using Platform Migration tool (The user running the tool must be a member of the Vault Admin group)

Option 1 - Migrate all platforms from PMTerminal to TPC automatically

- Download the tool from the marketplace.
- Unzip the tool file.
- Update the Vault.ini file with the address of the Vault.
- In a Command window, enter .\PMTerminalToTPCTool.exe Vault.ini ConvertAll <username> <password>.
- Review the results in the updated CSV file, and resolve any errors that occur.
- Test the migrated platforms to make sure the plugins run as expected with TPC by triggering a password change and/or password verify using each plugin.

Option 2 - Scan and review existing platforms, and migrate platforms from PMTerminal to TPC

- **Step 1: Scan and review existing platforms**
  - Download the tool from the marketplace.
  - Unzip the tool file.
  - Update the Vault.ini file with the address of the Vault.
  - Scan for platforms with PMTerminal. In a Command window, enter .\PMTerminalToTPCTool.exe Vault.ini RunScan <username> <password>.
  - A CSV file is created that contains a list of all platforms with PMTerminal
- **Step 2: Migrate platforms from PMTerminal to TPC**
  - Select the platforms that you want to migrate. In the CSV file created by the scan in Step 1 above, enter **Yes** in the **Convert column** for each platform that you want to migrate to TPC.
  - Migrate the platforms. On every CPM machine, in a Command window, enter .\PMTerminalToTPCTool.exe Vault.ini UpdatePlatforms <username> <password> <Updated CSV filename>.
    A new results CSV file is created with an additional column that indicates the migration status of each platform
  - Review the CSV file, and resolve any errors that occurred during the migration process.
  - Test the migrated platforms to make sure the plugins run as expected with TPC by triggering a password change and/or password verify using each plugin.

Manual Migration

- Log in to the PVWA as a Vault Administrator.
- Under Administration, select Platform Management.
- Locate the relevant platform, click the Ellipsis on the right side of the platform's row, and select Edit.
- Go to Target Account Platform > Automatic Password Management > CPM Plug-in.
- Change the value of the ExeName parameter from PMTerminal.exe to CyberArk.TPC.exe.
- Click OK.
- Test the migrated platforms to make sure the plugins run as expected with TPC by triggering a password change and/or password verify using each plugin.

Identify and describe how to correctly configure Interval and concurrent settings

The following parameters, in Server Settings, configure PSM server activities:

- MaxConcurrentTSSessions # of allowed concurrent PSM sessions
- MaxConcurrentUploaders number of allowed concurrent processes to upload recording files to the Vault.
- ConfigurationRefreshInterval interval in seconds between each configuration refresh process
- ClearUserProfilesInterval The number of days between processes that clear user profiles. Specify '0' (zero) to disable. The default value is 30.

Identify and describe how to correctly configure the Allowed Safes parameter

Target account platforms can be restricted to accounts stored in specific Safes. This feature is especially relevant if you implement the reconciliation functionality to prevent automatic reconciliation being performed on every Safe and giving unauthorized users access to passwords.

In large-scale environments, it is very important to enable the CPM to focus its search operations on specific Safes, instead of scanning all Safes it is allowed to see in the Vault.

Limit a platform to a specific safe

- In the list of supported target account platforms, select the platform that you want to modify, and then click Edit.
- The Target Account platform settings page appears.
- Expand Automatic Password Management, and then select General.
- The list of General properties is displayed.
- In the AllowedSafes parameter, specify the name(s) of the Safe(s) where this platform is used. The default value is .*, which allows the platform to be applied in all Safes. (up to 700 char)
- Apply or Save

Evaluate and scope a customer environment to correctly size the servers to meet customer needs

Install and deploy on a public cloud

Identify best practices agnostic to public cloud deployments

Identify and describe different cloud architectures

AWS

All-in-the-Cloud deployment

- Everything on VPC (virtual private cloud)

Hybrid deployment

- Vault and pvwa on prem others on cloud
- Vault only on prem

AZURE

All-in-the-Cloud deployment

- Everything on VPC (virtual private cloud)

Hybrid deployment

- Vault only on prem

Describe key management considerations in a public cloud

The following passwords must be accessible to the Vault administrator. They should also be written in a notebook and stored in a physical Vault with the Master CD.

User	Password
Local Windows Administrator	The password of the local Windows Administrator account on the Vault and DR Vault servers
Administrator	The predefined administrator user's password. **Note**: This should be attached to a password policy managed by the CPM that specifies that this is a one-time password.
Remote Control Agents	The remote control agent passwords for the Vault and for the DR Vault

These files are configured for your Enterprise Password Vault specifications during installation. It is important to store them in the Vault for future reference and safekeeping.

Feature	Files
Transparent user management	• LDAP certificate • local hosts file • LDAPDirectory.ini
Windows authentication	'For Client' and 'For Agent' keys
PKI authentication	PKI certificates for the Vault, the PrivateArk Client, and PVWA
Radius authentication	Radius secret file
RSA SecurID authentication	sdconf.rec
HA Cluster	The keys that are copied from the first node to the second node during configuration: • Backup.key • VaultUser.pass • ReplicationUser.pass • VaultEmergency.pass
Configuration	Any other configuration file that you consider to be relevant.

As the Vault configuration files are not backed up during Vault replications, copy the configuration files and store them in the Vault for safekeeping and possible future reference.

Identify and describe various cost reduction strategies when deploying into a public cloud