Privileged Access Management Install & Configure v12.6 Lab Guide

Scenario

The ACME Corporation has recently purchased CyberArk's **Privileged Access Management** (PAM) Core suite of software. You have been assigned the task to guide and assist The ACME Corporation in its deployment and configuration of the CyberArk PAM software with the goal of meeting the business requirements. This document details the customer's specific requirements regarding the use of PAM in their environment.

CyberArk's documentation online at docs.cyberark.com is available for reference to complete your tasks. All CyberArk documentation is available on the web at 'https://docs.cyberark.com/ (https://docs.cyberark.com/)'. This PAM I&C v12.6 Exercise guide provided by CyberArk University should be used in the training environment only. For production deployments use CyberArk published documentation at docs.cyberark.com for the version you are installing.

EPV Instructions

The ACME Corporation has purchased CyberArk's Privileged Access Management solution to protect and manage their privileged accounts. End users are required to authenticate to CyberArk using two factor authentication.

<u>You are required to:</u>

1. Install a standalone Vault
2. Install 2 PVWA Servers (Load Balanced, and configured for automatic failover to the DR vault)
3. Install 2 CPM Servers (one for managing Windows accounts and one for managing Unix and Oracle)
4. Install 2 PSM Servers in a Load Balanced configuration
5. Install 1 PSM for SSH Server
6. Install the Disaster Recovery and Vault Backup components
7. Integrate CyberArk with the Customer's LDAP, SMTP and SIEM solutions
8. Implement 2 Factor Authentication
9. Test the PAM EPV implementation. Add test accounts on the following target systems; Windows Domain, Windows Server, Linux, and Oracle and execute password management and PSM operations.

<u>Default Passwords</u>

All user accounts including local Administrator and ACME.CORP domain accounts are *Cyberark1*.

<u>Network Resources</u>

The following table lists the network resources provisioned by ACME Corporation for the CyberArk PAM Suite of software. The Windows Domain Controller for 'ACME.CORP' must always be powered on when working in your Skytap Lab environment.

Network	Server Name	Is domain member?	IP Address / DNS
Windows	DC01	Domain Controller ACME.CORP	10.0.0.2 / DC01.acme.corp
	Comp01A (PVWA-CPM)	Yes	10.0.20.1 / comp01a.acme.corp
	Comp01B (PVWA-CPM)	Yes	10.0.21.1 / comp01b.acme.corp
	Comp01C (PSM)	Yes	10.0.22.1 / comp01c.acme.corp
	Comp01D (PSM)	Yes	10.0.23.1 / comp01d.acme.corp
	Vault	No. Workgroup	10.0.10.1 / vault.acme.corp
	DR	No. Workgroup	10.0.14.1 / drvault.acme.corp
Linux	PSM for SSH	Linux	10.0.1.16 / psmp.acme.corp
	CentOS-target	Linux	10.0.0.20 / centos.acme.corp
	RADIUS	Linux	10.0.0.6 / radius.acme.corp

Vault Installation

This exercise provides detailed instructions on installing the **CyberArk Digital Vault** server and client software and is broken down into three sections:

- Preparation
- Vault Server Installation
- PrivateArk Client Installation

Preparation

Objective: Preparation. It is important to copy all CyberArk software, License.xml and any other files needed to the Vault server prior to EPV installation and hardening.

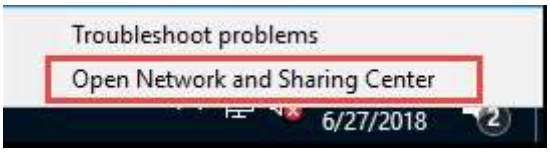
Note: Ensure that all Virtual Machines (VM's) are started in your Skytap lab before proceeding, (except for the DR VM).

1. Sign into the VAULT server. Username *Administrator*; Password Cyberark1

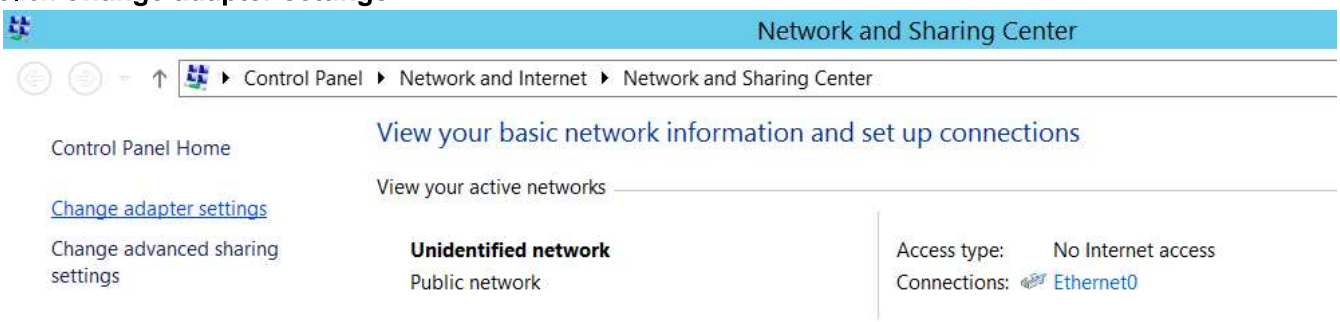
2. Open File Explorer and navigate to the shared resource folder, *"Z:\"*. If the Z: drive is not mapped, map Z: to "\\dc01\shared".
    a. Navigate to *"Z:\CyberArk PAM Solution\v12.6\"*. Copy folders "*\Vault Installation Files*" and "**\License and Operator Keys**" to "***C:\CYBR_Files***".
    b. Do not copy any other folders or files.

Objective: A stand-alone **Vault** server only requires TCP/IPv4 for network communication. In preparation to install the **Vault** server software, we will first remove all NIC protocols, clients and services not required for **Vault** functionality.

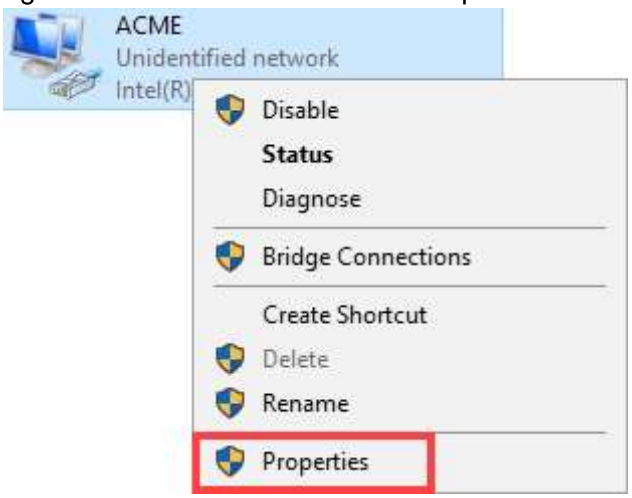
1. Right click the **Network** icon in the system tray and select Open Network and Sharing Center.



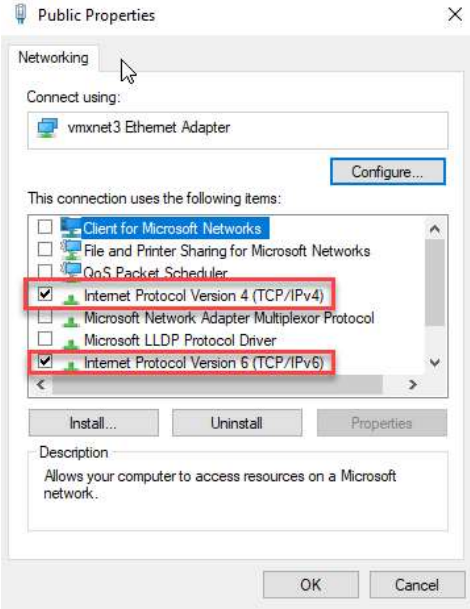
1. Click **Change adapter settings**.



2. Right click on the ACME Network Adapter and choose Properties.



3. Confirm Internet Protocol Version 6 (TCP/IPv6) is selected.
4. Select Internet Protocol Version 4 (TCP/IPv4*)* and select Properties.
    a. Ensure the static IP address (10.0.10.1), Subnet mask (255.255.0.0) and Default gateway (10.0.255.254) are defined.
    b. Remove all DNS server addresses and select the Advanced... button.
    c. In the DNS tab, deselect "Register this connections addresses in DNS".
    d. In the WINS tab, deselect "Enable LMHOSTS lookup".
    e. Select Disable NetBIOS over TCP/IP.
    f. Select OK twice to return to the ACME Properties dialog.
5. Deselect all services, clients and protocols except for Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6).

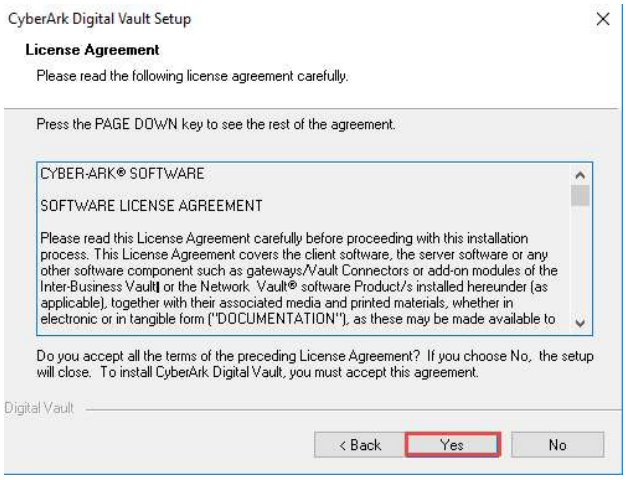


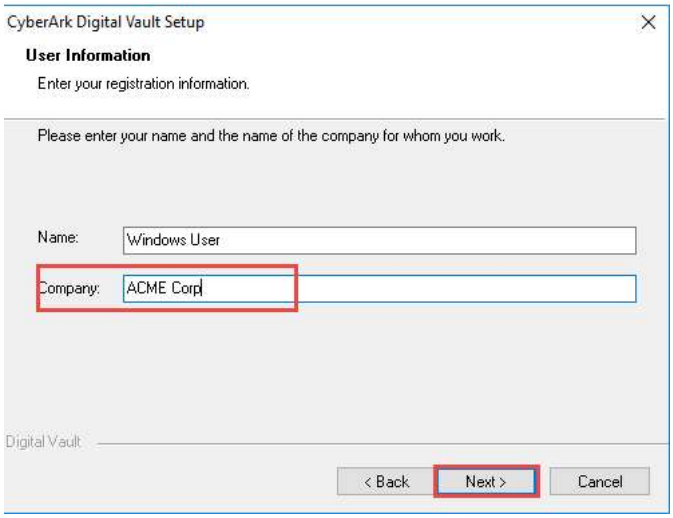
Vault Server Installation

Objective: This exercise provides detailed, step-by-step instructions on installing the **CyberArk Digital Vault** server and **Private Ark Client** software. On the lab server, the files copied from the shared drive in the pre-requisite steps are required to complete the installation.

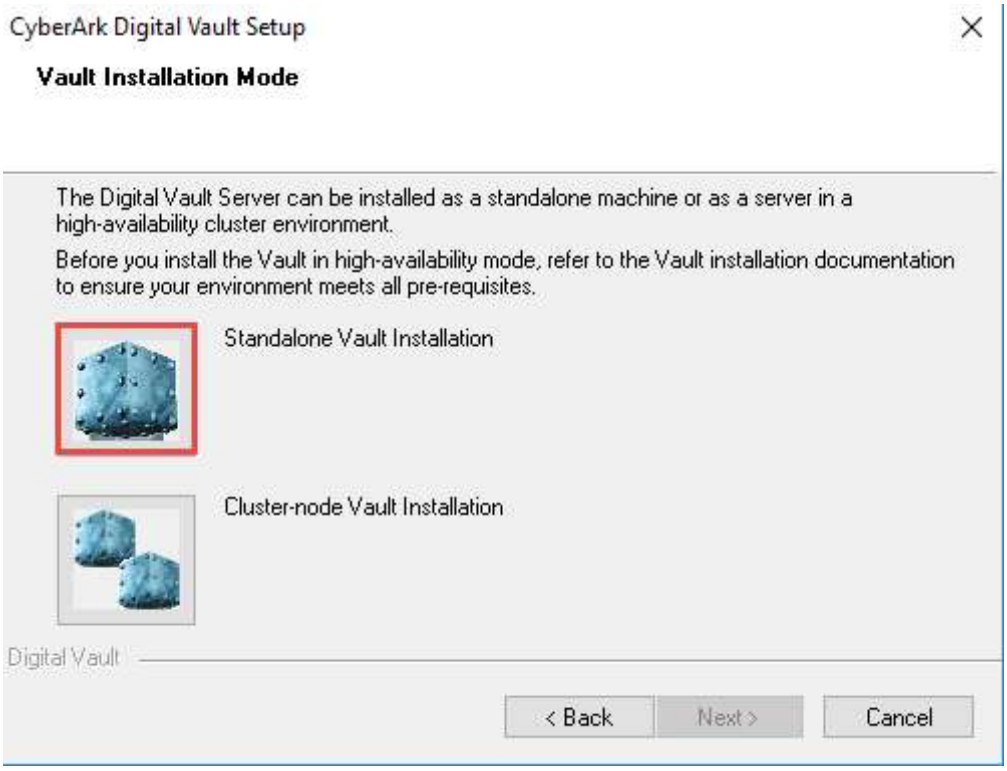
Note: We highly recommend that you turn on Filename Extensions on the Vault server.

1. Sign into the Vault server as Administrator. Using File Explorer, navigate to “C:\CYBR_Files\Vault Installation Files\”. Install Microsoft Visual C++ Redistributable 2015-2022 by launching “*VC_redist.x64.exe*”. Follow the prompts as required.
2. Using File Explorer, navigate to “**C:\CYBR_Files\Vault Installation Files\Server**”. Right click on setup.exe and choose “Run as Administrator”.
3. Accept the default options on the next three windows, including your company name (e.g. ACME Corp) on the Customer Information page.

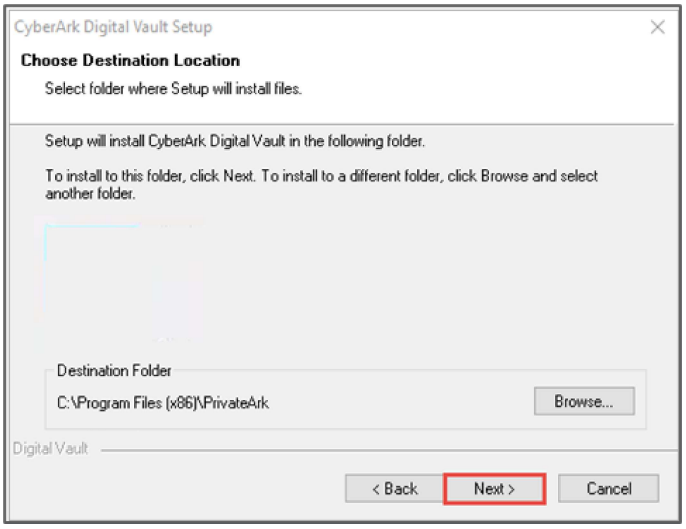




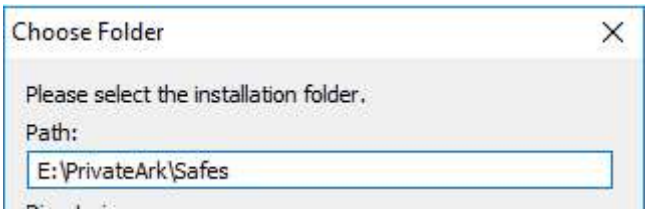
1. Select the Standalone Vault Installation option to install the Vault as a stand-alone server.



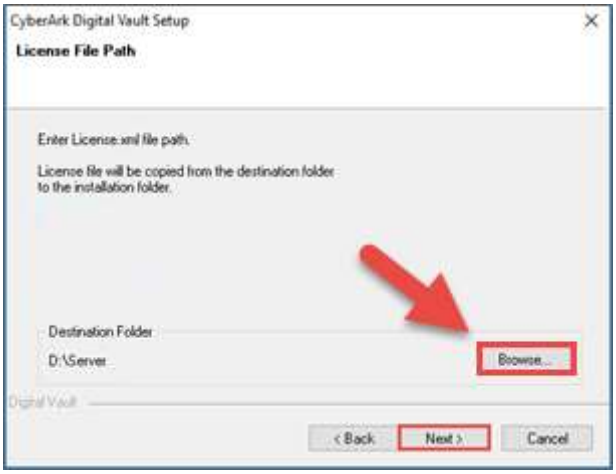
2. Press Next to accept the default installation location.



1. Select Browse to select a custom Safes location. Change the drive letter 'E:\PrivateArk\Safes' as shown then select Next to continue.



1. Select Browse to select a custom license file path.



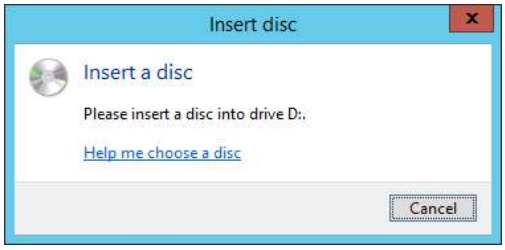
1. Click OK and then Cancel on the Insert disc pop-up to browse to the correct location.

Note: Because the software is configured to look for the license file on the CD/DVD drive by default, you will receive an error message regarding the *D:* drive.

1. In the Choose folder pop-up, browse to "*C:\CYBR_Files\License and Operator Keys\License*", press OK and then press Next.

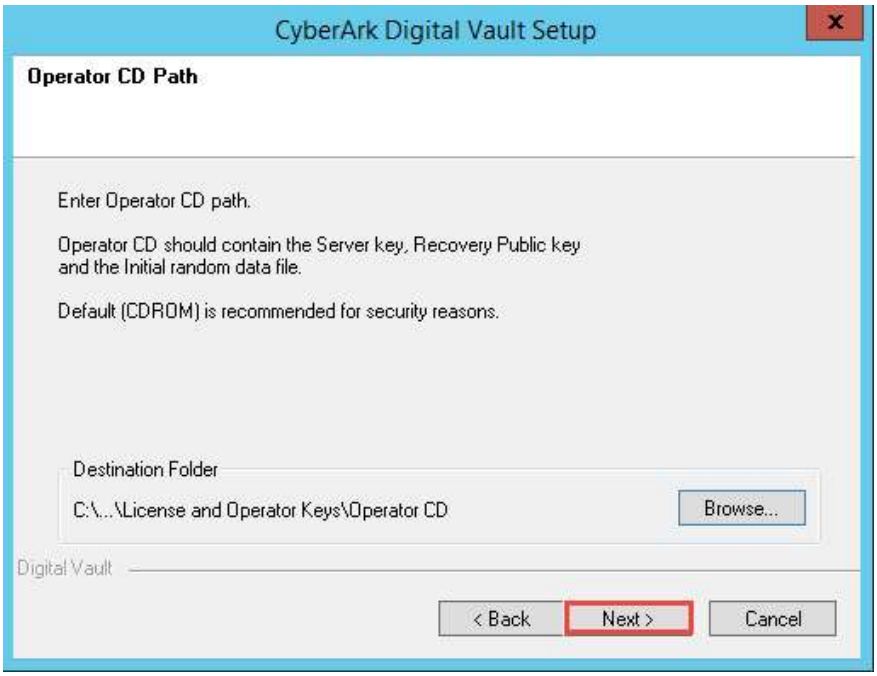
1. The same procedure is required for the Operator CD. Press Browse to select a custom Operator CD path.

1. You will receive the same error message regarding the D: drive. Click OK and then Cancel on the Insert disc pop-up to browse to the correct location.

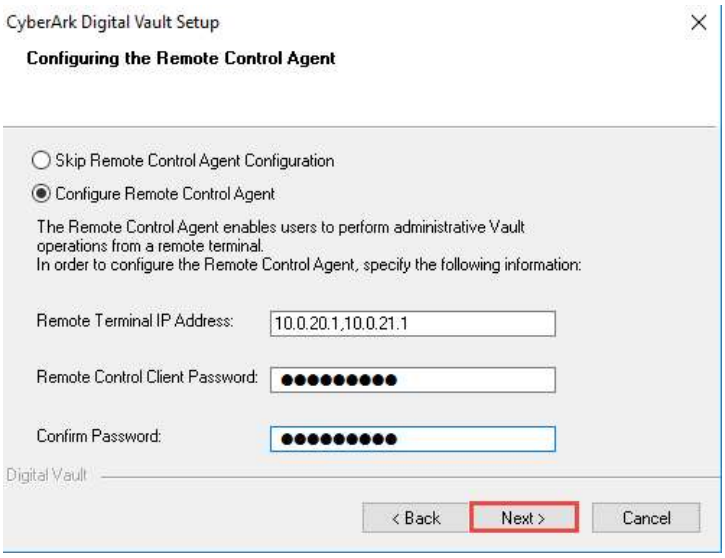


1. Browse to the "C**:\CYBR_Files\License and Operator Keys\Operator CD**" directory and click OK and then and press Next.

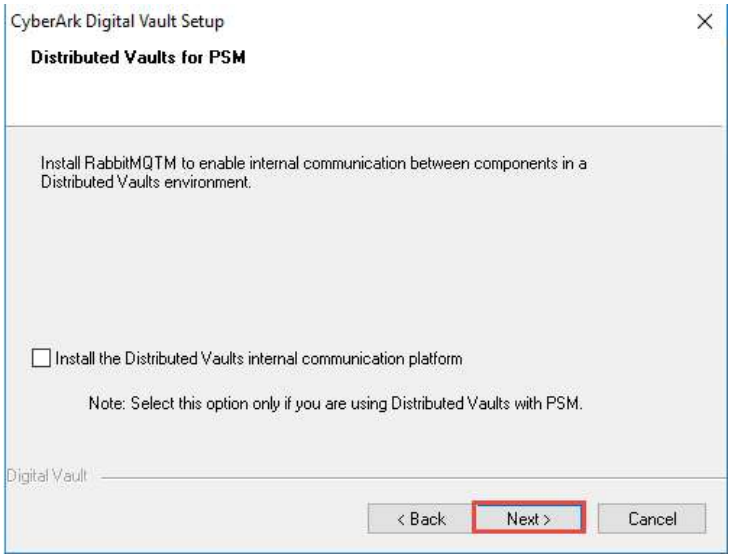
Note: These files must be accessible to the ***PrivateArk Server*** service to start the **Vault**. A Hardware Security Module (HSM) is the recommended method for key storage. If these files are to be stored on the file system, it is highly recommended that the keys and encrypted files be stored on separate media. If stored on attached storage, the Operator Keys should be located on an NTFS drive.



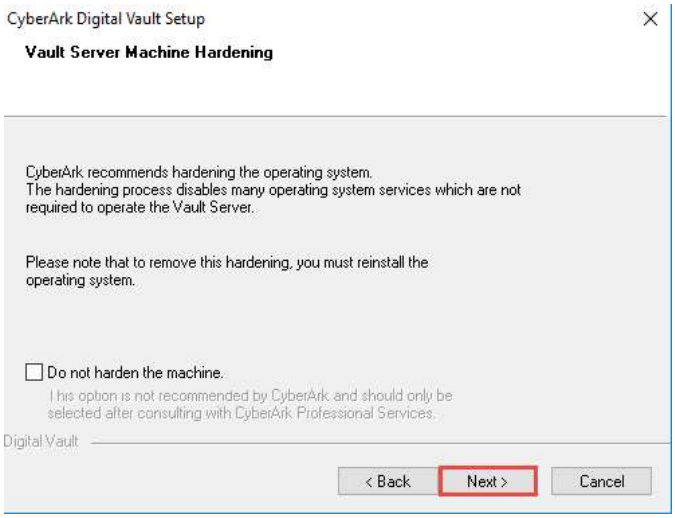
1. Enter the IP address(es) of your *Component* servers in the Remote Terminal IP Address field – 10.0.20.1,10.0.21.1 and Cyberark1 – in the password fields and press Next.



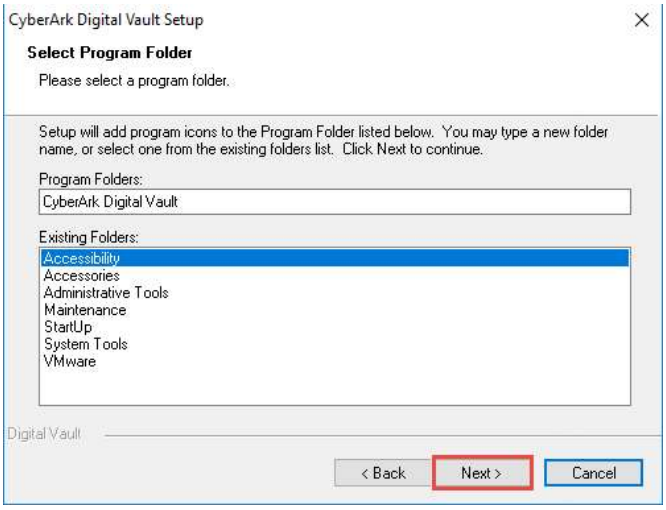
1. We will not be using Distributed Vaults with PSM in this lab. Select Next without selecting “Install the Distributed Vaults internal communication platform”.



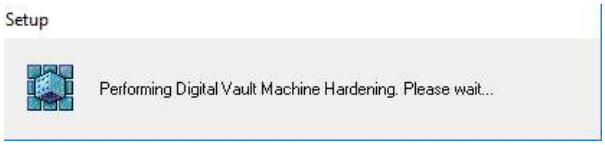
1. Press Next to allow CyberArk to harden the CyberArk Digital Vault machine.



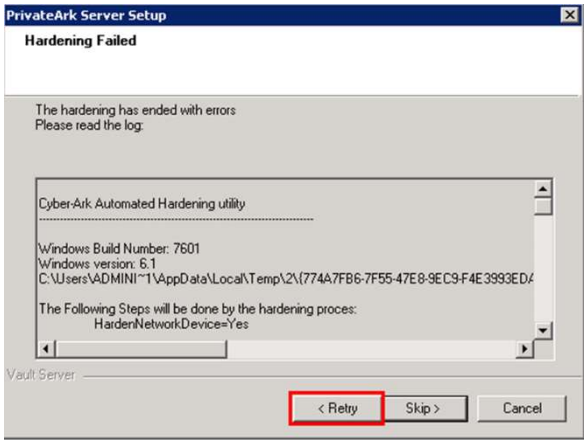
1. Press Next to accept the default Program Folder.



1. The Performing Vault Server Machine Hardening window will appear. This may take a few minutes.

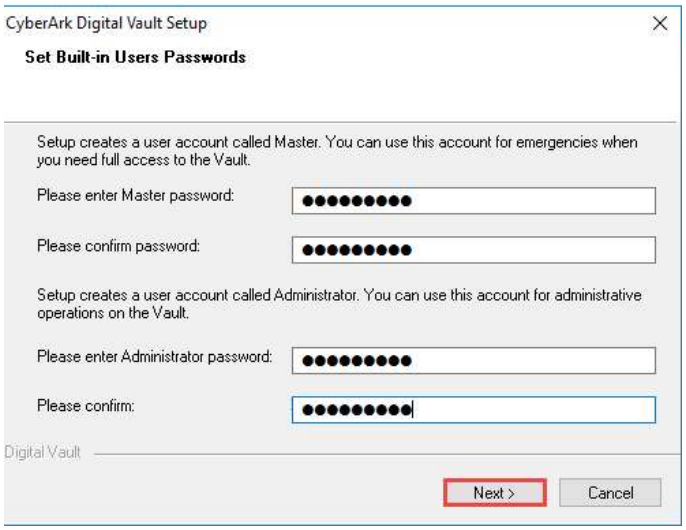


Note: In the **SkyTap** environment, you may receive a message that the hardening process failed. A failure is usually caused by a timeout in stopping services. If you receive the following “Hardening Failed” error, press the **Retry** button.



1. Set Built-in Users Passwords - Set passwords for the Master and Administrator; enter Cyberark1 in all the password fields and press Next.

Note: Enter the password ‘*Cyberark1*’ as the default password. It is recommended to set a stronger password in a production environment.



C

1. Choose “No, I will restart my computer later” and press Finish.

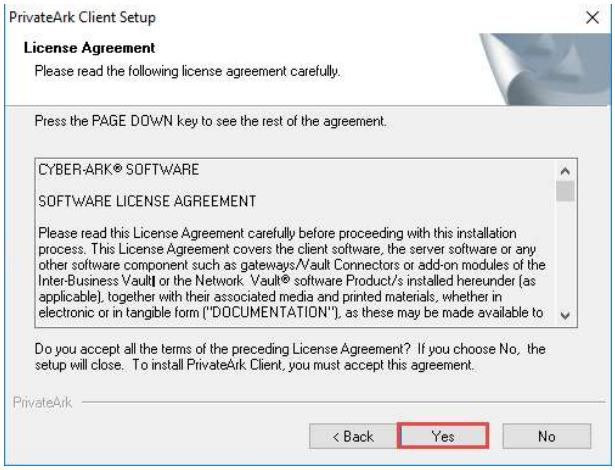
PrivateArk Client Installation

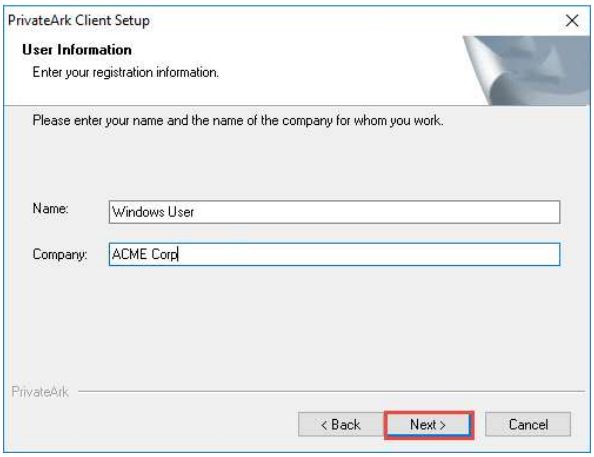
Next, we will install the **PrivateArk Client** on the **Vault** server.

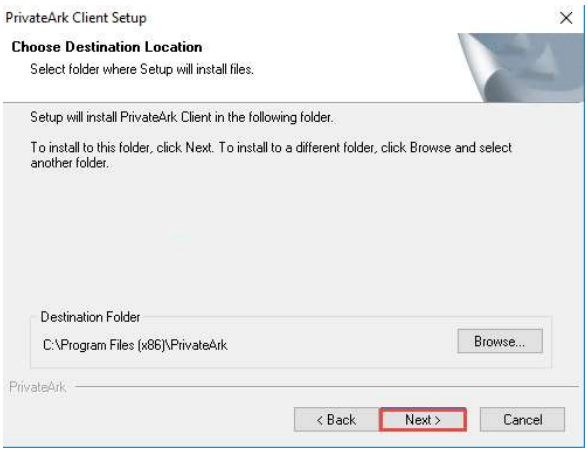
1. In File Explorer go to "***C:\CYBR_Files\Vault Installation Files\Client***". Right click setup.exe and choose "Run as administrator".

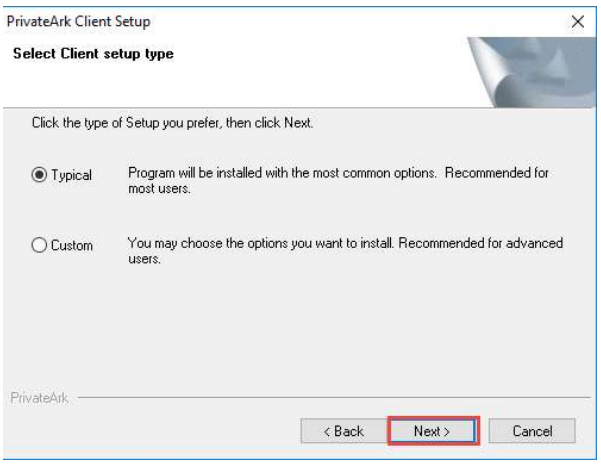
Note: If the message "Windows SmartScreen can't be reached right now" appears, click "Run anyway".

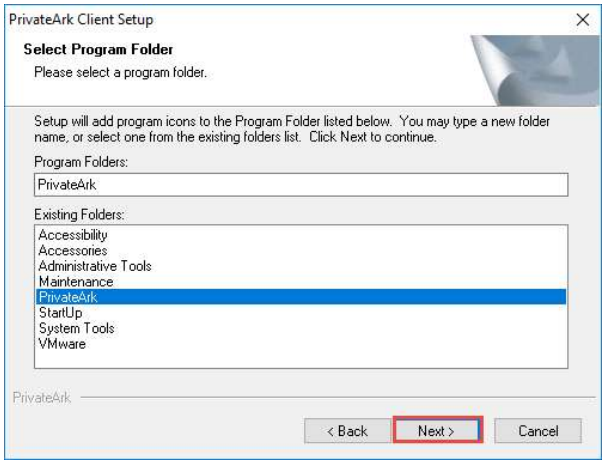
1. Accept the default options in each of the next six windows. In the **User Information** dialogue, enter your name and company or simply "Windows User" and "CyberArk"



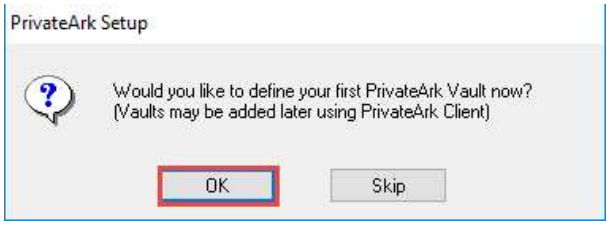




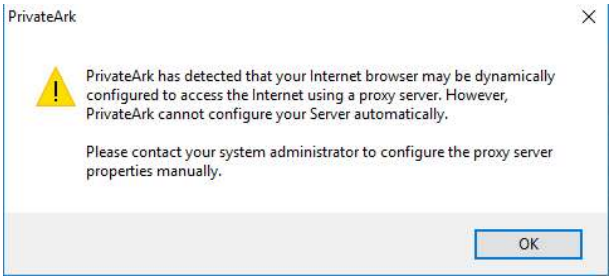




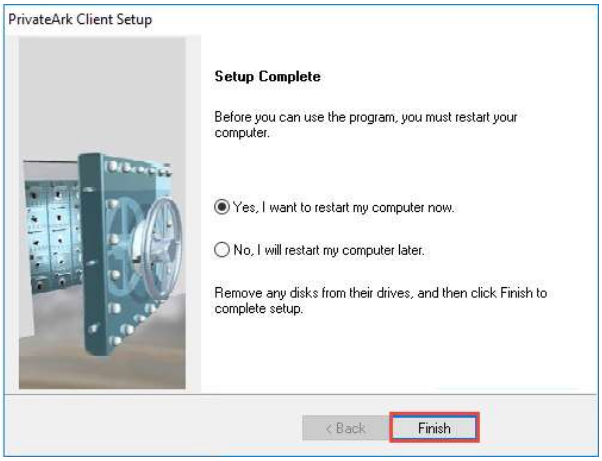
1. Press **OK** to define your first connection to the PrivateArk Vault. This will create a shortcut to your Vault within the PrivateArk Client.



1. Enter the following information and click OK to save.
   a. Server Name = Vault
   b. Server Address = 10.0.10.1
   c. Default User Name = Leave Blank or enter Administrator (blank means the client will remember the last logged on username)
   d. Click **OK** to acknowledge the informational proxy server message.



1. Select *Yes, I want to restart my computer now* and press Finish.



Post Vault Installation

1. Login to the **VAULT** server and double-click the “PrivateArk Server” shortcut on the desktop to open the Server Central Administration utility. Confirm there are no errors, and “ITADB313I Server 12.6.0 (12.6.0.9) is up” informational message appears.
2. Launch the PrivateArk Client from the desktop. Double click the Vault shortcut and login as **Administrator/Cyberark1**.
    a. Ensure that the 3 default safes exist, System, VaultInternal and Notification Engine. If any of these 3 safes do not exist stop and inform the instructor.

a. Logoff and close the PrivateArk Client.

1. Open Windows Services and check that the following services have been installed and started.
    a. Cyber-Ark Event Notification Engine[1]
    b. Cyber-Ark Hardened Windows Firewall
    c. CyberArk Logic Container
    d. PrivateArk Database
    e. PrivateArk Remote Control Agent
    f. PrivateArk Server

Note: The **CyberArk Enterprise Password Vault** is now installed.

Install Password Vault Web Access

Objective: Install the PVWA on both component servers, Comp01A and Comp01B.

More information is available online at docs.cyberark.com. See **“PVWA Installation Overview** (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/PVWA-install-overview.htm?tocpath=Installation%7CInstall%20PAS%C2%A0on-premise%7CInstall%20PVWA%7C_____1)**”**

Password Vault Web Access software will be installed manually however, Prerequisites and Hardening procedures will be configured using PowerShell Automation scripts.

Install IIS Pre-requisite Software using Automatic prerequisites script

Note: CyberArk provides a script to automate PVWA prerequisites. These scripts install the Web Server role and features, creates a self-signed web certificate and configures the HTTPS binding. Sign in to Comp01A as VaultAdmin01@acme.corp.

Note: Ensure that all Virtual Machines (VM’s) are started in your Skytap lab before proceeding, except for the DR VM.

1. Sign in to 'Comp01A' VM as ACME domain user with local admin privileges, i.e., VaultAdmin01@acme.corp.
2. Open File Explorer and navigate to the shared resource folder, *"Z:\CyberArk PAM Solution\v12.6\"*. If Z: is not mapped, map a drive to "\\dc01\shared".
    a. Copy "Password Vault Web Access-Rls-v12.6.zip" and "Client-Rls-v12.6.zip" files to ***"C:\CYBR_Files"***. If the destination folder does not exist, create it. Do not copy any other files.
    b. Extract the zip archives to the default folder.
3. Navigate to "*C:\CYBR_Files\Password Vault Web Access-Rls-v12.6\InstallationAutomation*".

Disable PVWA_Verify_IIS_Settings

Optional: The following 4 step procedure is required only if the Web Server role is not already installed. If this step is skipped, an error will be displayed in the log file, i.e., "*The following step failed : PVWA_Verify_IIS_Settings*". The error should be ignored.

1. Select and open by double clicking, file "***C:\CYBR_Files\Password Vault Web Access-Rls-v12.6\InstallationAutomation\PVWA_Prerequisites.zip***".
2. Select and copy file "PVWA_Prerequisites_Config.xml". Paste the file to the desktop and edit using a text editor, such as Notepad++.
3. Update step "PVWA_Verify_IIS_Settings " to Enable=No.
4. Save the file, then copy and paste it to back into the archive file "PVWA_Prerequisites.zip", ensuring that the original file is overwritten.

Install the Web Server Role

1. Open Windows PowerShell as an Administrator in "*C:\CYBR_Files\Password Vault Web Access-Rls-v12.6\InstallationAutomation*" and execute the following three PowerShell commands. Select Yes when prompted.

Get-ExecutionPolicy (Result should be "Restricted")

Set-ExecutionPolicy Bypass -Scope Process

.\PVWA_Prerequisites.ps1

Note: The PVWA Prerequisites script will take a few minutes to complete.

1. Look for validation; "Operation Succeeded" and "IsSucceeded": 0," that the script completed successfully.
2. Review Script.log found in the "*C:\CYBR_Files\Password Vault Web Access-Rls-v12.6\Installation Automation\{date_time}*"
3. Open the IIS Manager console and verify that IIS was installed, that a self-signed certificate was generated and that incoming HTTPs requests are using the certificate.
    a. Navigate to the "Default Web Site", select Edit Site, Bindings. Edit the HTTPS Binding and confirm the self-signed SSL certificate is assigned.

```
The following step had been completed successfully: PVWA_IIS_SSL_TLS_Settings
finish execute step Setting IIS SSL TLS Configuration
*****************************************************************
*****************************************************************
                    Operation Succeeded
*****************************************************************
*****************************************************************
                PVWA Prerequisites script execution ended.
*****************************************************************
Cleanup - Delete files except logs and backup
Finish Execution
{
    "isSucceeded":  0,
    "errorData":  "Step Verify .Net Version Skipping prerequisites check.\nStep PVWA Install Web Server Roles Skipping p
rerequisites check.\nStep Disable IPV6 Skipping prerequisites check.\nStep PVWA Config Self Certificat Skipping prerequi
sites check.\nStep Setting IIS SSL TLS Configuration Skipping prerequisites check.\n                Operation Succeede
d",
    "logPath":  "C:\\CYBR_Files\\Password Vault Web Access-Rls-v12.1\\InstallationAutomation\\prerequesites_2021-12-09_1
3-15-03\\Script.log"
```

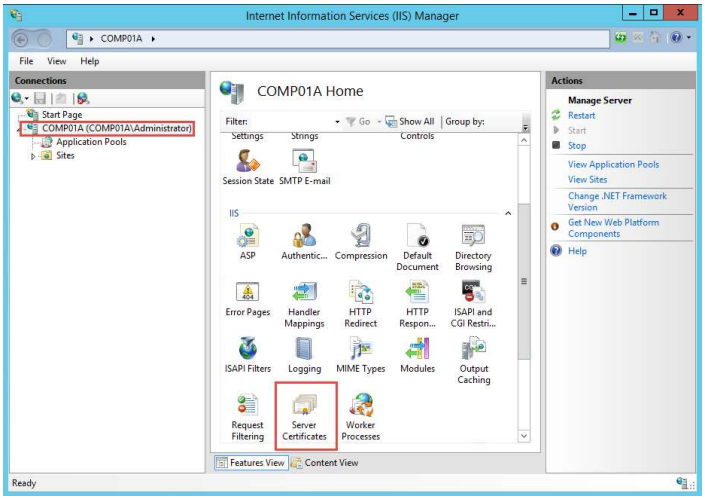
Note: The PVWA_Prerequisties script creates a self-signed certificate and uses this certificate for binding HTTPs incoming requests. In a production environment, we recommend updating the HTTPS binding with a certificate provided by a Trusted Certification Authority.

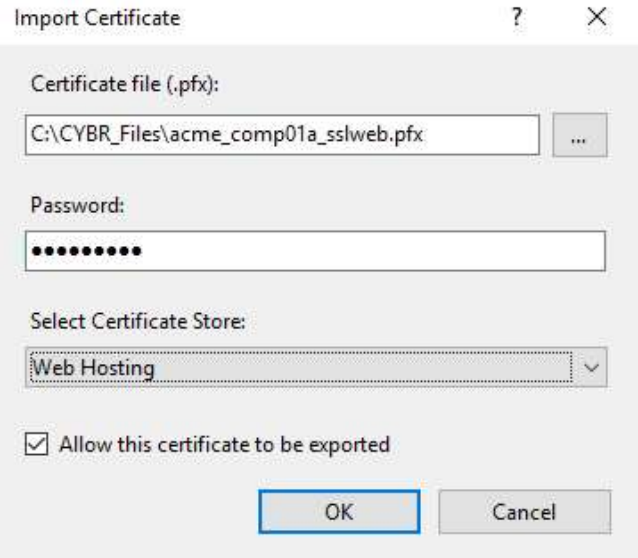
Note: Online instructions for the deployment of PVWA pre-requisites please refer to PVWA Installation Overview (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/PVWA-install-overview.htm?tocpath=Installation%7CInstall%20PAS%7CInstall%20PVWA%7C_____1)

Import Trusted Certificates for WebHosting

Objective: In the following procedure you will replace the self-signed certificate created by the Prerequisites script with a Web Certificate provisioned by the ACME Certificate Authority. Certificates have been provided for both PVWA Servers; Comp01a and Comp01b.

1. Sign in to PVWA Server Comp01a as VaultAdmin01@acme.corp (mailto:VaultAdmin01@acme.corp).
2. Launch Internet Information Services (IIS) Manager from the Start Menu > Administrative Tools. Under Connections, select the Host name then double click “Server Certificates”, as shown in the graphic.
3. Select “Import…” from the Actions menu and then the ellipsis to search for the Certificate file (.pfx).
4. Navigate to *C:\CYBR_Files* and select the comp01a_sslweb.pfx file and click Open. Enter the password “Cyberark1”, select Certificate Store: Web Hosting. Select “Allow this certificate to be exported”.
5. Under Connections, expand Sites and select Default Web Site. In the Actions column, select Bindings…
6. Double click the https binding. Select the imported certificate “COMP01AWebCert_2022”.
7. Click OK and Close.

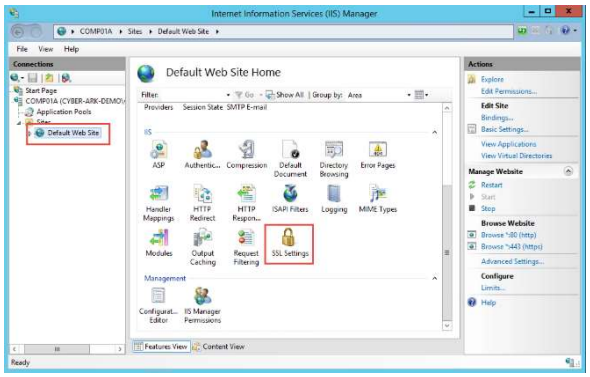




Require HTTP over SSL (PVWA)

Objective: In this section we will configure IIS to **require** connections over SSL. **Note:** This is also a prerequisite for later authentication sections.

1. Begin by launching IIS Manager (INETMGR) from the Start Menu > Administrative Tools on your Component server.
2. Go to Default Web Site and double click SSL Settings (golden padlock). Select Require SSL and click Apply in the Actions menu.
3. Validate the IIS installation. This is an important step to confirm that the IIS server is functioning correctly prior to the PVWA software installation. Open Internet Explorer and attempt to connect to the default web site on the component server with http and https URL's. What is the expected behavior of each?
   a. "*https://comp01A.acme.corp/* (https://comp01A.cyber-ark-demo.local/)"
   b. "*http://comp01A.acme.corp/* (http://comp01A.cyber-ark-demo.local/)"



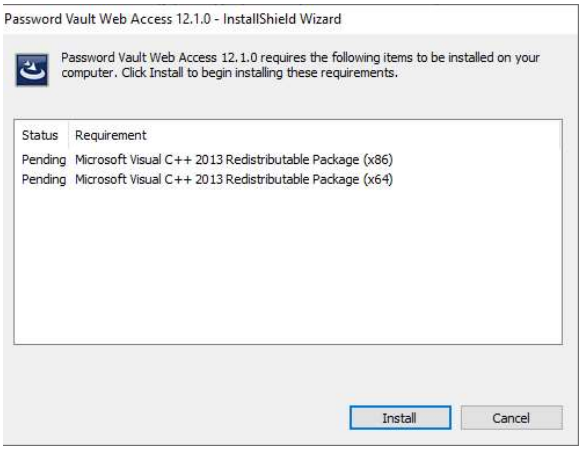
Install PVWA

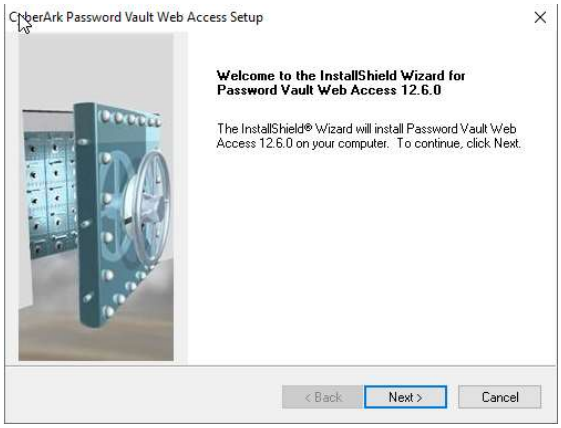
Objective: Install the **Password Vault Web Access** component on Comp01A.

Note: It is recommended to gracefully restart each component server prior to running the Installation Automation PowerShell scripts.

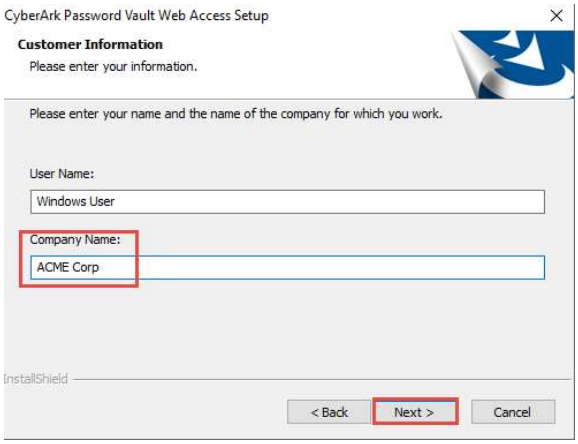
1. Signed into the component server with local admin rights, open File Explorer, navigate to folder "***C:\CYBR_Files\Password Vault Web Access-Rls-v12.6***".
2. Right click setup.exe and "run as Administrator".

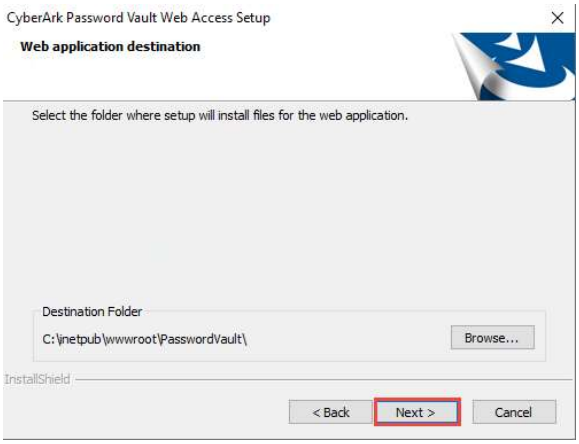
3. If prompted, select to install the Microsoft Visual C++ 2013 Redistributable Packages.
4. Press the Next button, then click Yes to agree to the license agreement.



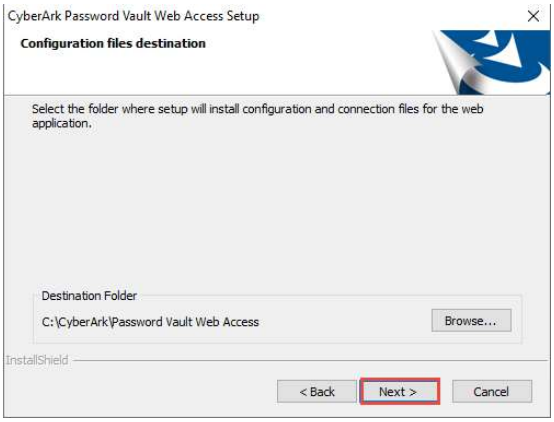


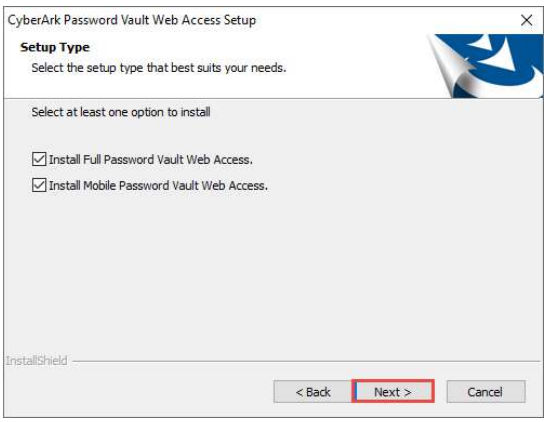
1. Enter a Company name, press Next.



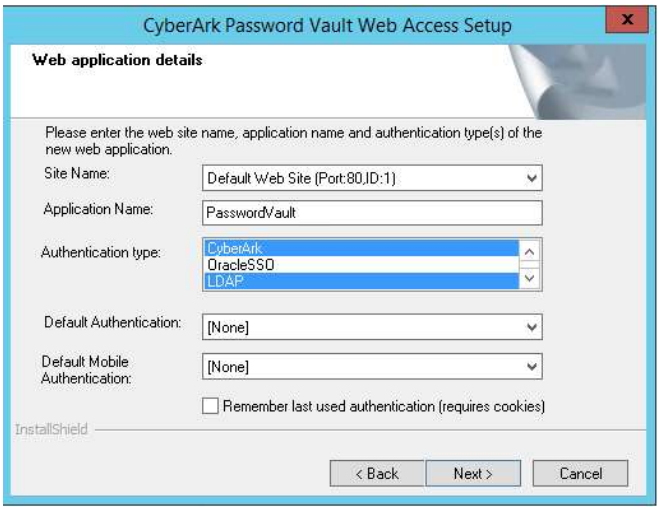


1. Press Next to accept the default Configuration files destination and Web application destination.

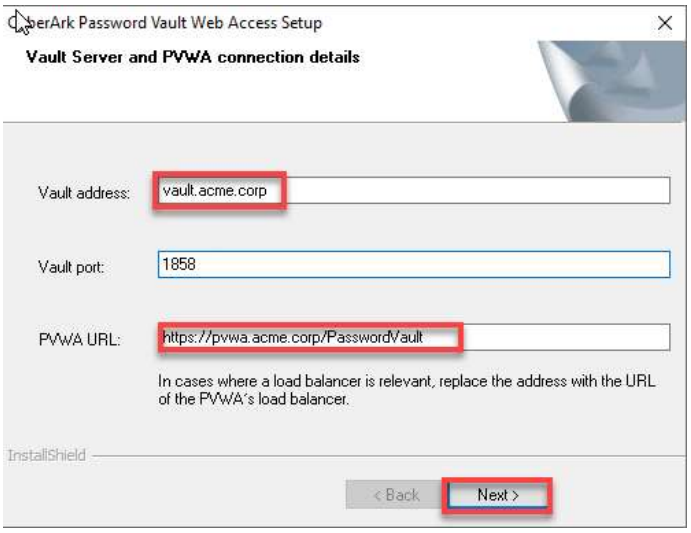




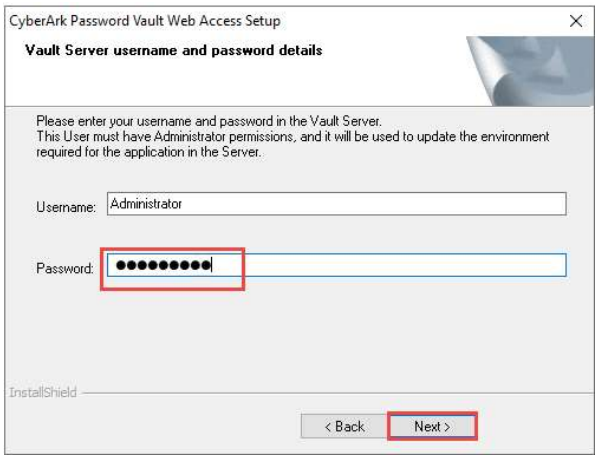
1. Press Next to accept both Setup Type options.
2. On the Web application details window…
    a. Select CyberArk and LDAP as the Authentication Type.
    b. Choose None in Default Authentication and Default Mobile Authentication fields and press Next to continue.

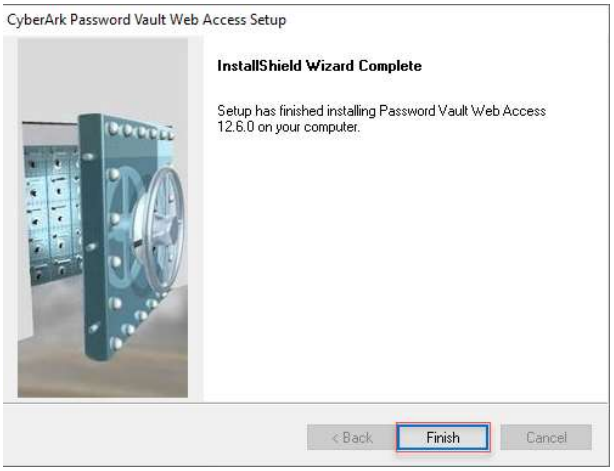


1. On the Vault Server and PVWA connection details window…
    a. Enter the Vault DNS host name or IP address, i.e., vault.acme.corp OR 10.0.10.1
    b. We will be load balancing PVWA servers in this lab. Update the PVWA URL: field with the URL to the load balancer. Update the URL as follows; “https://pvwa.acme.corp/PasswordVault (https://pvwa.acme.corp/PasswordVault)” and press Next.



1. Enter UserName = Administrator and Password = Cyberark1 and select Next. On the InstallShield Wizard Complete window, click the Finish button.





1. Post PVWA installation:
   a. Check the PVWAInstall.log. File can be found by choosing Run and entering %temp%.
   b. Open Chrome and connect to the PVWA. Use URL https://comp01a.acme.corp/PasswordVault (https://comp01a.acme.corp/PasswordVault)/v10/logon and confirm that the PVWA login page is displayed. This step validates that the PasswordVault application is communicating with the PrivateArk Server.
   c. Sign in to the PVWA using CyberArk Authentication as Administrator. Validate tabs Policies, Accounts, Applications, Reports and Administration display correctly.
   d. Logout of the PVWA.

Hardening the CyberArk PVWA Server

Hardening the PVWA server ensures that your PVWA server meets CyberArk's security standards in 'In Domain' deployments as well as in 'Out of Domain' deployments. CyberArk Component Server hardening is a combination of enforcing security policy (via GPO or INF), manual tasks plus automated procedures using Installation Automation PowerShell scripts.

Note: Most of the PVWA hardening procedures can be accomplished with a PowerShell script although each procedure can be performed manually. See PVWA Installation Overview (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/PVWA-install-overview.htm?tocpath=Installation%7CInstall%20PAS%7CInstall%20PVWA%7C_____1) for a checklist when installing the PVWA in a production environment.

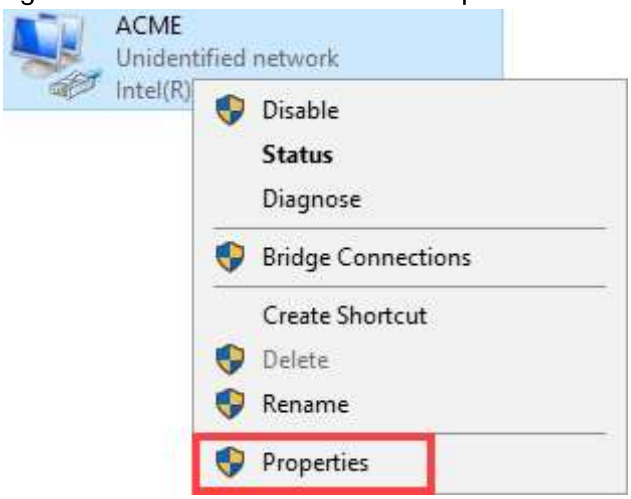
Note: Not all configurations can be scripted. Some hardening procedures require manual steps. The following procedure instructs the student how to harden the Network Interface manually, then proceeds using the Installation Automation PowerShell scripts. More information can be found online at "PVWA Hardening (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/PVWA-hardening-intro.htm?tocpath=Installation%7CInstall%20PAS%C2%A0on-premise%7CInstall%20PVWA%7CPVWA%20Hardening%7C_____0)".

Manual Hardening

Objective: A PVWA or CPM server only requires Client for Microsoft Networks, File and Printer Sharing for Microsoft Networks and the TCP/IPv4 network protocol. We will disable all other NIC protocols, clients, and services.

1. Right click on the Start Menu, select Network Connections > Change adapter options.

1. Right click on the ACME Network Adapter and choose Properties.



2. Only the following network protocols, services or clients are required for a CPM and or PVWA Component Server:
    a. Client for Microsoft Network
    b. File and Printer Sharing for Microsoft Network
    c. Internet Protocol Version 4 (TCP/IPv4)
    d. Disable all other default protocols, services and clients as shown in the graphic.
    e. Restart the server.

Installation Automation Hardening

1. Sign in to the Comp01A server as local Administrator or ACME Domain user with Local Admin privileges, i.e., VaultAdmin01. Navigate to "***C:\CYBR_Files\Password Vault Web Access-Rls-v12.6\InstallationAutomation***"
2. Open Windows PowerShell as an Administrator in the folder specified in step 1 and execute the following PowerShell commands. Select Yes when prompted.

Get-ExecutionPolicy (Result should be "Restricted")

Set-ExecutionPolicy Bypass -Scope Process

.\PVWA_Hardening.ps1

Note: "Get-ExecutionPolicy" will display the current Execution Policy "ExecutionPolicy Restricted" is the default Execution Policy for ACME.Corp

"ExecutionPolicy Bypass -Scope Process" sets the Execution Policy to Bypass for the current PowerShell session but does not change the default execution policy for PowerShell

".\PVWA_Hardening.ps1" will launch the PowerShell hardening script

1. Look for validation "Operation Succeeded" and "IsSucceeded: 0," that the script completed successfully.
2. Review the Script.log that was created in "*C:\CYBR_Files\Password Vault Web Access-Rls-v12.6\InstallationAutomation\timestamp*"

```
*****************************************************************
                    Operation Succeeded
*****************************************************************
start IIS service
Start CyberArk Scheduled Tasks service
WARNING: Waiting for service 'CyberArk Scheduled Tasks (CyberArk Scheduled Tasks)' to start...
WARNING: Waiting for service 'CyberArk Scheduled Tasks (CyberArk Scheduled Tasks)' to start...
WARNING: Waiting for service 'CyberArk Scheduled Tasks (CyberArk Scheduled Tasks)' to start...
WARNING: Waiting for service 'CyberArk Scheduled Tasks (CyberArk Scheduled Tasks)' to start...
=================================================================
                  PVWA_Hardening script execution ended.
=================================================================
Cleanup - Delete files except logs and backup
Finish Execution
{
    "isSucceeded":  0,
    "errorData":  "Step Importing INF Configuration Skipping prerequisites check.\nStep Validate Server Roles Skipping p
rerequisites check.\nStep PVWA IIS Anonymous Authentication Skipping prerequisites check.\nStep PVWA IIS Registry Shares
 Skipping prerequisites check.\nStep PVWA IIS Directory Browse Skipping prerequisites check.\nStep PVWA IIS WebDAV Skipp
ing prerequisites check.\nStep PVWA IIS MimeTypes Skipping prerequisites check.\nStep PVWA IIS SSL TLS Settings Skipping
 prerequisites check.\nStep Disable ScreenSaver Skipping prerequisites check.\nStep Advanced Audit Policy Configuration
Skipping prerequisites check.\nStep Remote Desktop Services Skipping prerequisites check.\nStep EventLog Size And Retent
ion Skipping prerequisites check.\nStep Registry Audits Skipping prerequisites check.\nStep Registry Permissions Skippin
g prerequisites check.\nStep FileSystem Permissions Skipping prerequisites check.\nStep FileSystem Audit Skipping prereq
uisites check.\nStep Disable Services Skipping prerequisites check.\nStep PVWA Post Installation Skipping prerequisites
check.\n                    Operation Succeeded",
    "logPath":  "C:\\CYBR_Files\\Password Vault Web Access-Rls-v12.1\\InstallationAutomation\\hardening_2021-12-09_13-46
-10\\Script.log"
}
```

Final Manual Hardening Configuration for PVWA Deployments

Objective: Remove unneeded Application Pools.

IIS Hardening

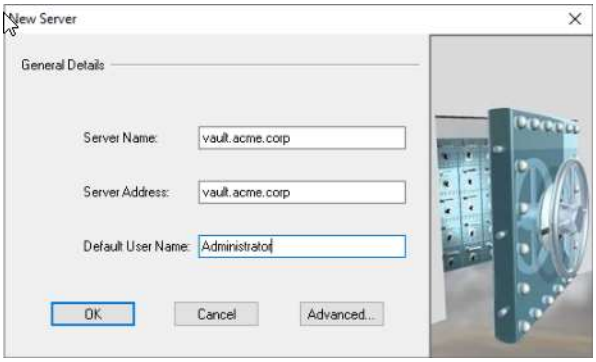
1. Application Pool. Open IIS Configuration Manager.
2. In Connections, navigate to Application Pools. Keep the following application pools only. Delete all other existing Application Pools:
   a. DefaultAppPool (Managed Pipeline Mode = Integrated)
   b. PasswordVaultWebAccess (Managed Pipeline Mode = Integrated)

Install the PrivateArk Client on the Component server

Objective: In this section, you will repeat the steps for installing the **PrivateArk Client** on the Comp01A server.

1. Using File Explorer navigate to "***C:\CYBR_Files\Client-Rls-v12.6\Client***". Right click on setup.exe and run as Administrator.
2. When prompted, enter the Server Name and Server Address as shown.

3. Restart when prompted.



Note: Repeat the “Install Password Vault Web Access” procedures beginning on page 26 to install the PVWA on **Comp01B**

Ensure the following steps are completed on Comp01B

1. INSTALL IIS PRE-REQUISITE SOFTWARE USING AUTOMATIC PREREQUISITES SCRIPT
2. IMPORT TRUSTED CERTIFICATES FOR WEBHOSTING
3. REQUIRE HTTP OVER SSL (PVWA)
4. INSTALL PVWA
5. Hardening the CyberArk PVWA Servers
    - Manual Hardening
    - iNSTALLATION AUTOMATION HARDENING
6. iNSTALL THE PrivateArk Client oN THE COMPONENT SERVER

Test PVWA Load Balancing

Note: Your CyberArk lab is using a DNS Round Robin configuration to simulate an external hardware Load Balancer. The IP address for each PVWA server (10.0.20.1,10.0.21.1) has been added to the load balanced pool of servers by the ACME Network Administrator. The URL is *“**https://pvwa.acme.corp/PasswordVault**”* or select the shortcut on the Chrome Bookmarks Bar, CAU LAB Links > PVWA.

Sign in to the Comp01A/B server as a domain user, e.g., VaultAdmin01 with password=Cyberark1 to test the Load Balancer. ***IF you sign in to the COMP01A/B servers as a local Administrator you may experience certificate errors!***

Install CPM (distributed)

Install 1st CPM

Objective: In this section you will install and perform hardening tasks on the CPM server. More information is available online at docs.cyberark.com. See **“CPM Installation Overview** (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/CPM-install-overview.htm?tocpath=Installation%7CInstall%20PAS%C2%A0on-premise%7CInstall%20CPM%7C_____1)**”**

Note: Ensure that all Virtual Machines (VM's) are started in your Skytap lab before proceeding (with the exception of the DR and PSM for SSH VM).

1. Sign in to the Comp01A server as VaultAdmin01.
2. Open File Explorer and navigate to the shared resource folder, "Z:\CyberArk PAM Solution\v12.6\". If Z: is not mapped, map a drive to "\\dc01\shared".
3. Copy "Central Policy Manager-Rls-v12.6.zip" to "C:\CYBR_Files". Extract the zip archives on the Component Server. Do not copy any other files.
4. Using File Explorer, navigate to "C:\CYBR_Files\Central Policy Manager-Rls-v12.6\InstallationAutomation".

1. Open Windows PowerShell as an Administrator in the folder specified in step 4 and execute the following PowerShell commands. Confirm by entering the character 'Y'.

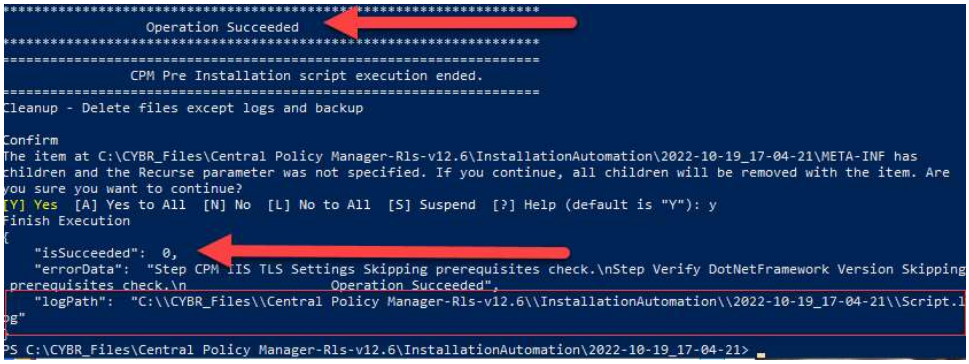
Get-ExecutionPolicy (Result should be "Restricted")

Set-ExecutionPolicy Bypass -Scope Process

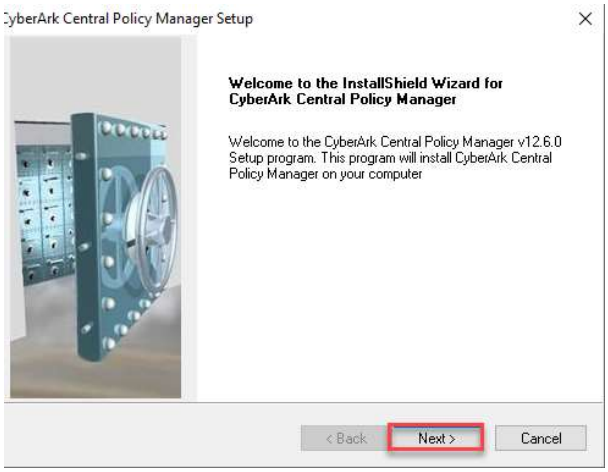
.\CPM_Preinstallation.ps1

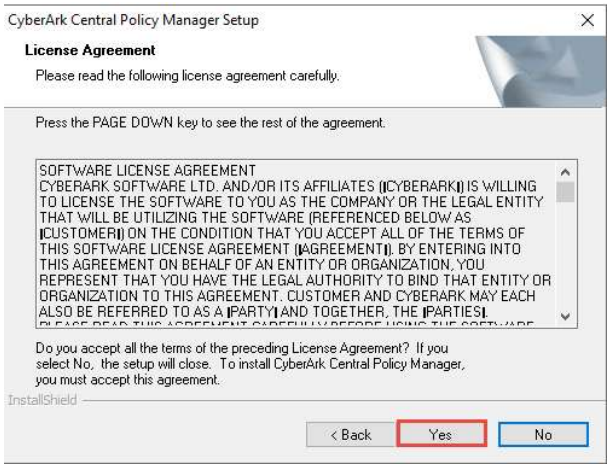
a. Accept the default "Y" at the prompt.

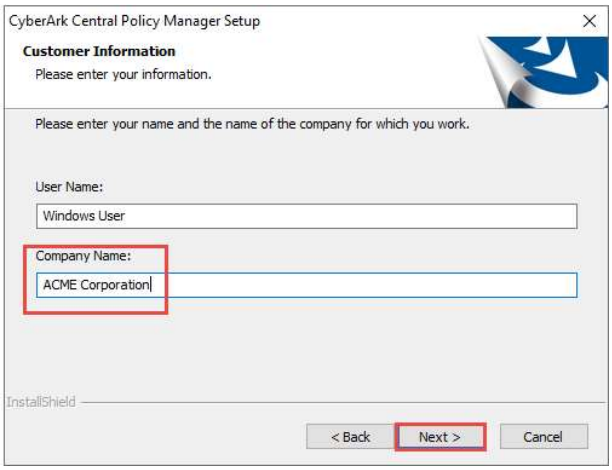
1. Look for validation "Operation Succeeded" and "IsSucceeded: 0," that the script completed successfully.

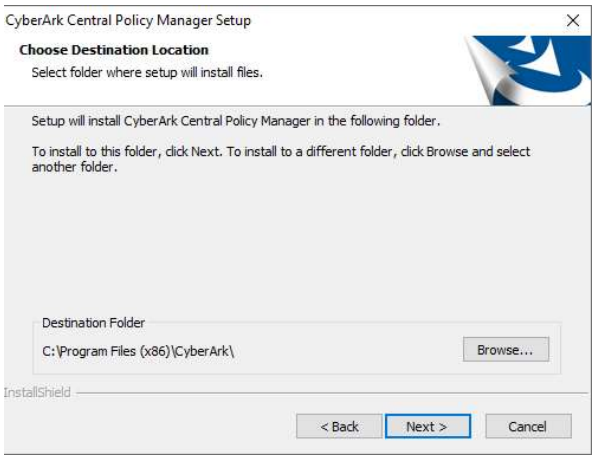


1. Verify the script completed successfully by reviewing the Script.log found in the "C:\CYBR_Files\ Central Policy Manager-Rls-v12.6\Installation Automation\{date_time}
2. In File Explorer open the extracted \Central Policy Manager-Rls-v12.6 folder. Right click setup.exe and choose "Run as Administrator".
3. If applicable, select Install to install the required Windows redistributable package.
4. Accept the default options on the next four windows, including your company name (e.g. CyberArk) on the Customer Information page.

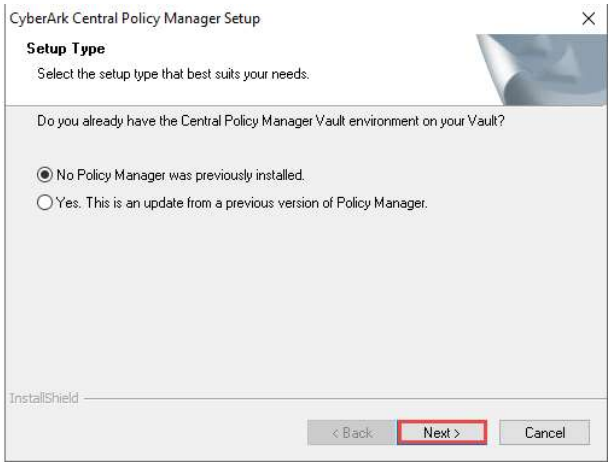






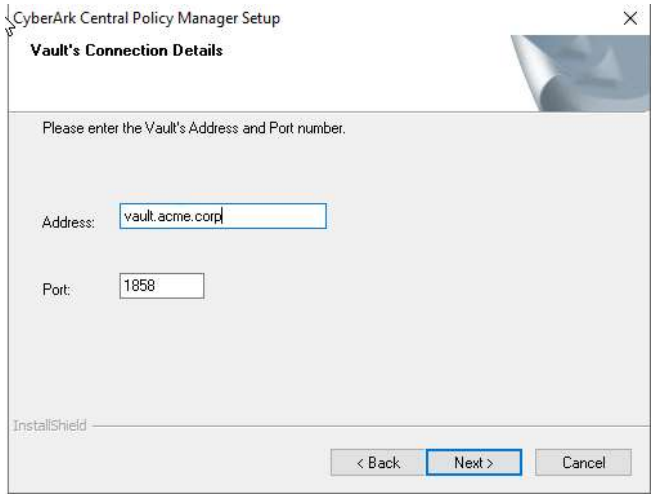


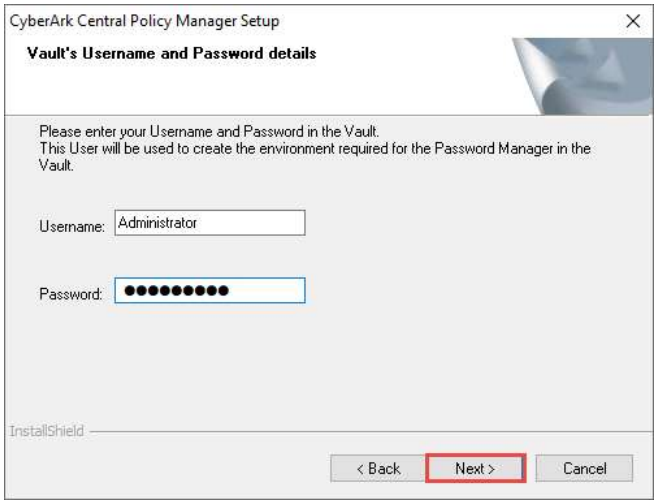
1. Accept the default option, “No Policy Manager was previously installed” and press Next.



Note: This question relates to installing **CPM software** using an existing licensed CPM user or installing an additional CPM that will consume a new license.

1. In the following 2 prompts, enter the IP Address of your Vault (i.e., vault.acme.corp or 10.0.10.1), then enter Administrator as the Username and Cyberark1 for the Password. Then press Next.





1. You <u>may</u> receive the following error: “CPMEM038E Error while trying to import platforms…”. This is common in the Skytap environment. Please ignore and select Next to continue.
2. Press the Finish button to complete the installation.

1. Immediately following the CPM installation, review the CPMInstall.log file created in “C:\Users\Administrator\AppData\Local\Temp\”. To access this directory, in the File Explorer address window, type %appdata%, then in the address bar, change from Roaming to Local and navigate to the \Temp directory. This file contains a list of all the activities performed when the CPM environment in the Vault is created during the installation procedure.

Post CPM Installation

Review the following.

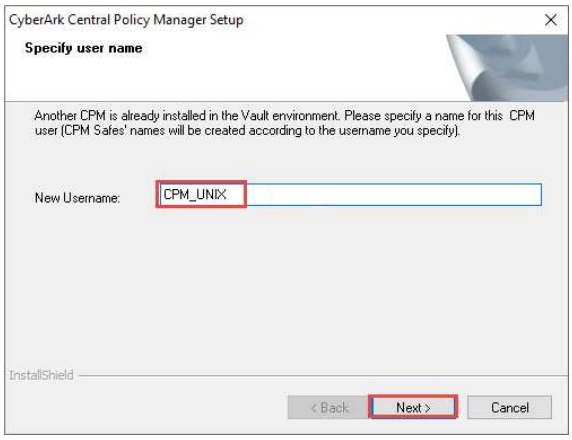
1. Navigate to “C:\Program Files (x86)\CyberArk\Password Manager\Logs”. Check the pm.log and pm_error.log file for errors.
2. Confirm that the CPM services are installed and running.
    a. CyberArk Password Manager Service.
    b. CyberArk Central Policy Manager Scanner.

-

Install 2nd CPM

Objective: Install the CPM component on COMP01B server. You will now repeat the steps followed in section **Install 1st CPM** until prompted for the CPM Name.

1. Respond to the prompts from the CPM Installer until “Specify Username”. The installer will ask you to specify a username for this CPM, since another CPM has already been installed on this Vault. Enter CPM_UNIX in the New Username field, then complete the installation



Post CPM Installation

Review the following.

1. Navigate to “C:\Program Files (x86)\CyberArk\Password Manager\Logs”. Check the pm.log and pm_error.log file for errors.

1. Confirm that the CPM services are installed and running.
    a. CyberArk Password Manager Service.
    b. CyberArk Central Policy Manager Scanner.

Harden the CPM server(s)

Objective: Hardening the CPM server ensures that your CPM server meets CyberArk’s security standards for 'In Domain' deployments as well as in 'Out of Domain' deployments. CPM server hardening is automated via a combination of an applied Group Policy for in-domain deployments and PowerShell scripts. Both are necessary. CPM and PVWA GPO’s have been applied during the PVWA hardening phase earlier in this lab.

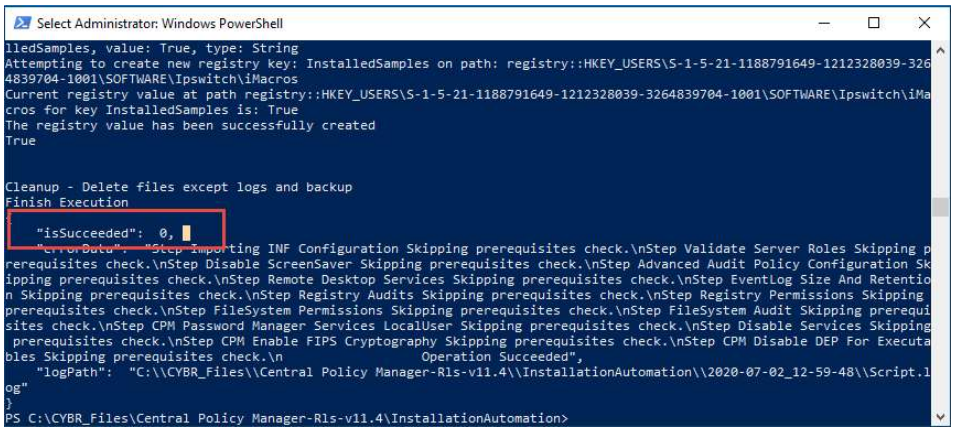
1. Sign in to the Comp01A server as local Administrator or as an ACME Domain user with Local Admin privileges, i.e., VaultAdmin01. Navigate to “C:\CYBR_Files\Central Policy Manager-Rls-v12.6\InstallationAutomation”.
2. Open Windows PowerShell as an Administrator in the folder specified in step 1 and execute the following PowerShell commands. Confirm by entering the character ‘Y’ when prompted.

Get-ExecutionPolicy (Result should be “Restricted”)

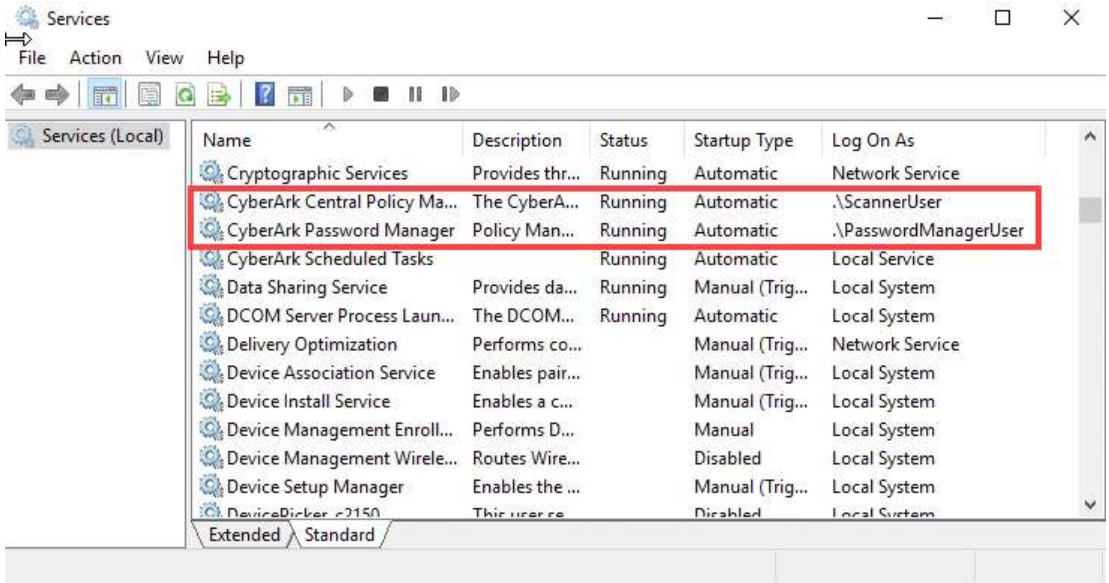
Set-ExecutionPolicy Bypass -Scope Process

.\CPM_In_Domain_Hardening.ps1

1. Wait until the script completes. “isSucceeded”: 0” represents confirmation of the successful completion of the hardening script.
   a. Logs detailing the actions taken by the PS script can be found in a subfolder of “…\InstallationAutomation\{date-time}”.
2. Open the Windows Administrative Tools > Computer Management.
   a. Select Services and Applications > Services. Check the status of “CyberArk Password Manager” and “CyberArk Central Policy Manager Scanner” Windows services.
   b. Confirm that the services are now running under the credentials of the local users

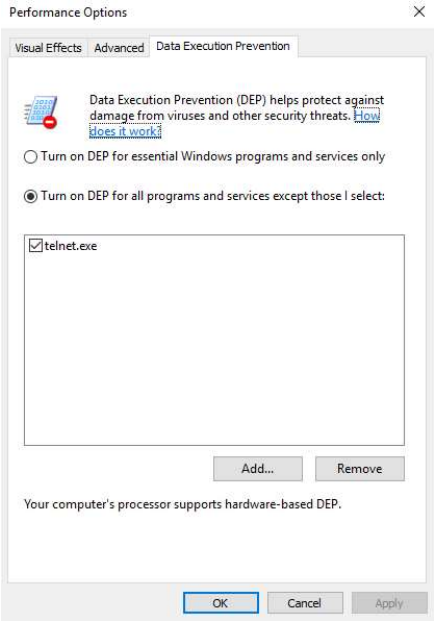


Service	Local Service Account
CyberArk Central Policy Manager Scanner	ScannerUser
CyberArk Password Manager	PasswordManagerUser



Note: Confirm that telnet.exe is defined as exceptions to Data Execution Prevention.

a. At the Start Menu, Run command, type “sysdm.cpl”. Navigate to Advanced > Performance > Settings > Data Execution Prevention.



Note: The CPMHardening.ps1 script attempts to add the above exception automatically. If the exception is not created, this is a clue that the CPM_Hardening.ps1 script was not run in an “**Administrators: PowerShell Window**”. If hardening manually this step is required to support terminal based CPM plugins.

1. Repeat section “**Harden the CPM server**” on the Comp01B server.

-

-

Automated Hardening: Group Policy Enforcement

PVWA / CPM Group Policy hardening enhances CyberArk component security by defining a highly secured Windows server. Enabling and enforcing the PVWA / CPM Group Policy Object is included as part of the PVWA and CPM installation and hardening procedures.

Note: CyberArk provides a Group Policy Object specifically for dedicated PVWA or CPM Component Servers and a separate GPO for PVWA/CPM co-hosted Component Servers. In this lab the CyberArk Component Servers Comp01A and Comp01B will co-host both the PVWA and CPM components. The Group Policy Object has already been imported to the Group Policy Management Console for the ACME.CORP domain.

For additional instructions on importing the GPO to an Active Directory domain, follow this link, Hardening PVWA servers in a domain (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/PVWA-hardening-in-domain.htm?tocpath=Installation%7CInstall%20PAS%C2%A0on-premise%7CInstall%20PVWA%7CPVWA%20Hardening%7CHardening%20PVWA%20servers%20in%20a%20domain%7C_____0)

Objective: Enable the PVWA Hardening GPO for the PVWA/CPM Servers in Active Directory Group Policy Management.

1. Sign in to the DC01 Virtual Machine as Administrator/Cyberark1.
2. On the Desktop, double click the Group Policy Management Console.
3. Expand acme.corp > Servers > CyberArk and select the CPM-PVWA Organizational Unit.
4. Right click the CPM-PVWA Organizational Unit and select “Link an Existing GPO…”
5. Select “CPM-PVWA Hardening” GPO and click OK.

Note: The CPM-PVWA Hardening GPO has been edited to allow the local service account **PasswordManagerUser, PluginManagerUser** and **ScannerUser** the “Logon as a service” right. **These rights must be configured and enforced to enable successful Password Management operations**. A customer’s organization may have additional requirements.

1. In the “Linked Group Policy Objects” tab, right click “CPM-PVWA Hardening” and select “Enforced”.
2. Select OK to confirm.
3. If desired, select the Group Policy Object “CPM-PVWA Hardening”
    - Select the Settings tab and a report of all settings applied to the CPM/PVWA servers will be displayed.
    - When finished, close Group Policy Management Console and sign out of DC01 server.
4. Sign in to the Comp01A server as ACME Domain user with Local Admin privileges, i.e., *VaultAdmin01*.
5. Right click on the Start Menu and select “Windows Powershell (Admin). Select Yes to the User Account Control popup window. Type the following command
    - gpupdate /force
6. repeat steps 9 and 10 on COMP01B.

Integrations

LDAP Authentication (over SSL)

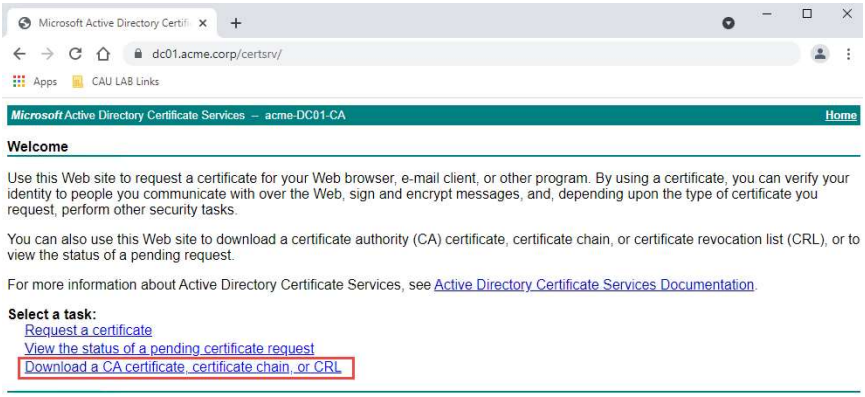
Objective: To configure the vault to use LDAP over SSL connections, you must import the Certificate Authority's root Certificate into the Windows Trusted Root Certificate Store on the Vault Server. The following procedure will guide you through transferring the certificate file from the component server, to the vault server where it can be imported.

Note: Ensure that all Virtual Machines(VM's) are started in your Skytap lab before proceeding (with the exception of the DR VM).

Install the CA ROOT Certificate on the Digital Vault

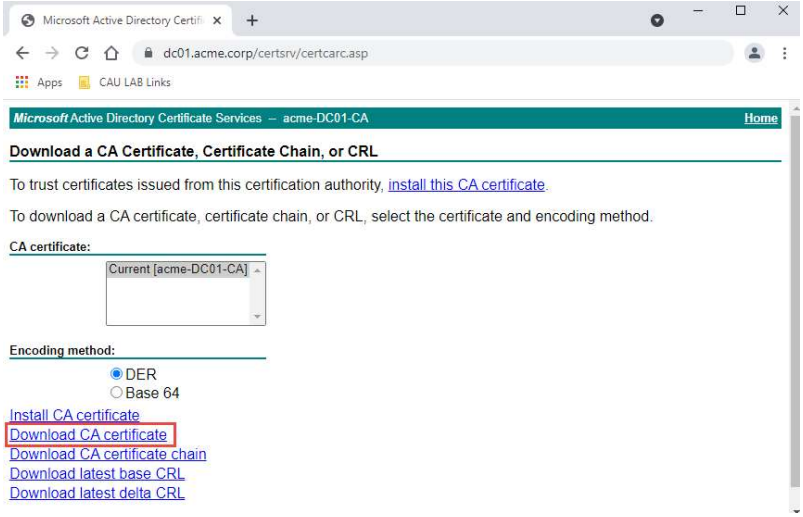
1. Sign in as vaultadmin01 on server Comp01A or Comp01B server. Open a Chrome Browser.
2. From the Favorites Bar, select **"CAU LAB Links" > "ACME Certificate Services"** or browse to https://dc01.acme.corp/certsrv (https://dc01.cyber-ark-demo.local/certsrv).
   a. If prompted, log into the web page as *Administrator/Cyberark1*.

3. Click on Download a CA certificate, certificate chain, or CRL.

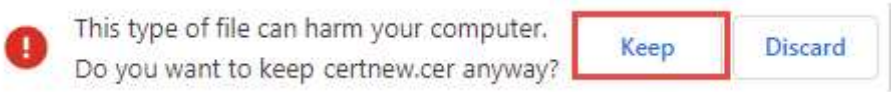


4. If prompted, click Yes to allow this operation.

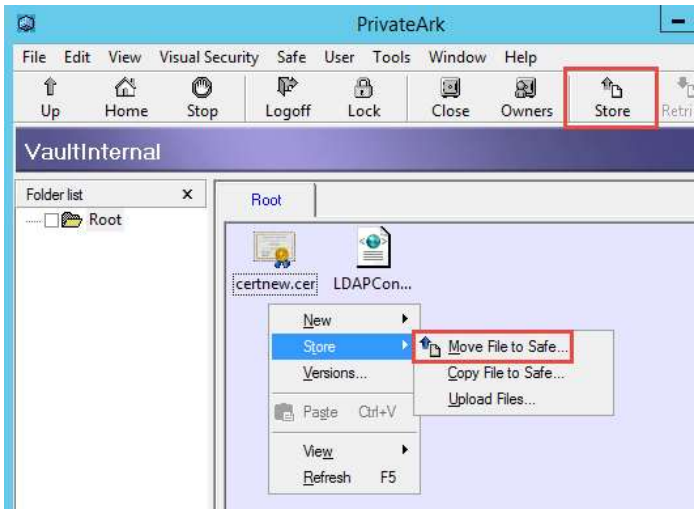
5. Click Download CA certificate.



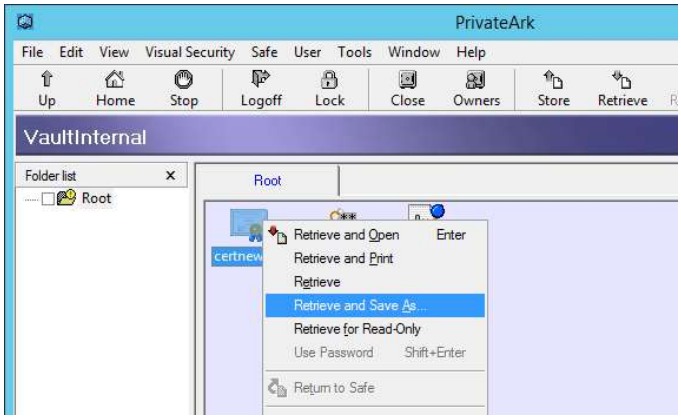
6. Select **Keep,** to store the certificate in the Downloads folder.



7. Log into PrivateArk Client as Administrator. You may need to add a new shortcut to the Vault server.
8. Open and Enter the VaultInternal safe.
9. Click the Store menu option, or right click in the body of the safe, and select Store, Move File to Safe.
    a. Navigate to the Downloads folder and select the file just downloaded, certnew.cer.



10. Logoff from PrivateArk Client on the Components Server.
11. Sign into the **VAULT server** as Administrator.
12. Login to PrivateArk Client as Administrator.
13. Open and Step into the VaultInternal safe.
14. Right click certnew.cer and click Retrieve and Save As…



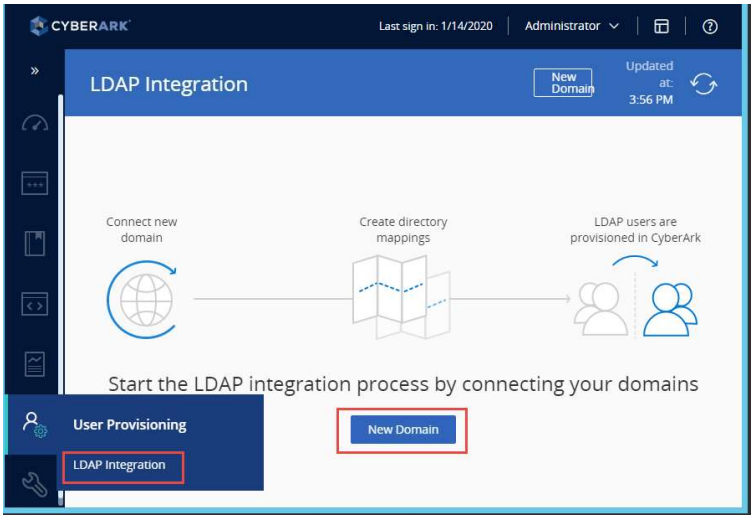
15. Save the file to the Desktop and logoff PrivateArk Client.
16. Right click on the Start Menu and select Run. Type **CERTLM.MSC** and click OK.
17. Expand Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates.
18. From the Action menu, select All Tasks > Import ...; the Certificates Import Wizard appears.
19. Click Next to display the File to Import window. Browse to select the certificate file saved to the Desktop. Click Next to display the Completing the Certificate Import Wizard window appears.
20. Select Place all certificates in the following store, Certificate store: "Trusted Root Certification Authorities" then click Next to display the Completing the Certificate Import Wizard window.
21. Review the settings and select Finish.

Update the HOSTS file to Enable Host Name Resolution

1. In File Explorer, navigate to directory, "***C:\Windows\System32\drivers\etc***"
2. Select the File menu > Open command prompt as administrator. Select Yes at the User Account Control popup window.
3. At the Administrator: Command Prompt, type "Notepad hosts" and press enter.
4. Add the following line to the end of the file and save it.

10.0.0.2 dc01.acme.corp dc01

5. Sign out of the Vault Server and sign in to either the Comp01A or Comp01B Server as VaultAdmin01@acme.corp.
6. Using the Chrome Browser, sign in to the PVWA as Administrator using CyberArk authentication and display the User Provisioning > LDAP Integration page.
7. Select **New Domain** to display the LDAP Integration Wizard.



8. Proceed through the LDAP Integration Wizard using the following parameters.

Domain Name:	acme.corp
Connect via:	Secure connection (SSL)
Address:	dc01.acme.corp
Bind user name:	bindaccount@acme.corp
Bind user Password:	Cyberark1
Domain Base Context:	dc=acme,dc=corp

9. Select the domain controller listed; dc01.acme.corp and select **Connect**.

Note: In a production implementation it is recommended to configure 2 Domain Controllers at the company's primary site, and 2 additional Domain Controllers at the company's Disaster Recovery site.

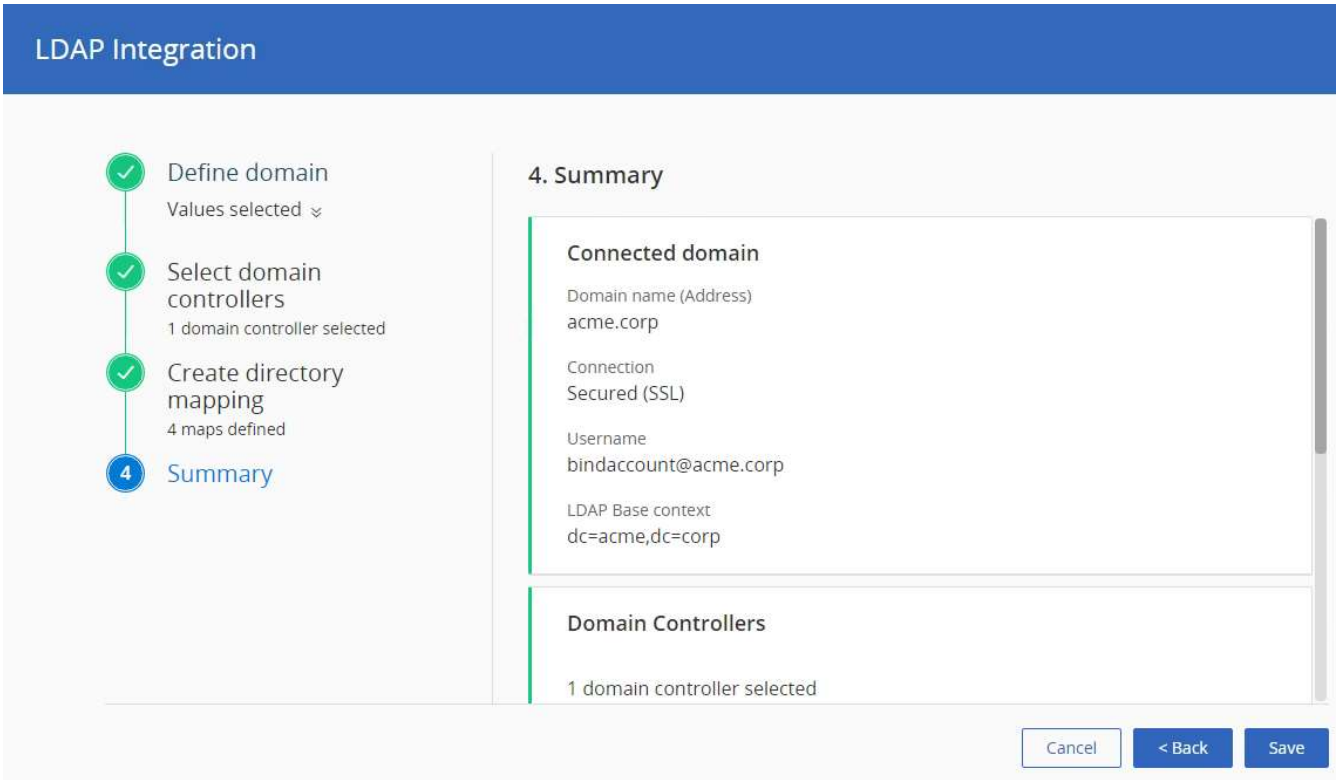
10. In Create directory mapping option, click **Define map** to the right of each user group name and specify the name of the user or group.

Note: **Do not select 'Next' until all 4 directory maps have been defined.**

a. Select the appropriate group for each field.
b. When complete, click Next.

Define Vault Admin Group:	CyberArk Vault Admins
Define Safe Managers Group:	CyberArk Safe Managers
Define Auditors Group:	CyberArk Auditors
Define Users Group:	CyberArk Users

11. Review the summary and select Save.



12. Test your LDAP/S integration by signing in to the PVWA as **vaultadmin01/Cyberark1** using **LDAP Authentication.**

-

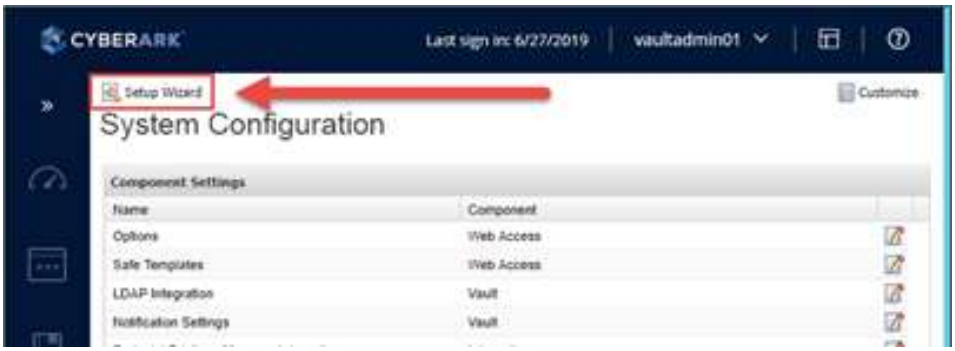
SMTP Integration

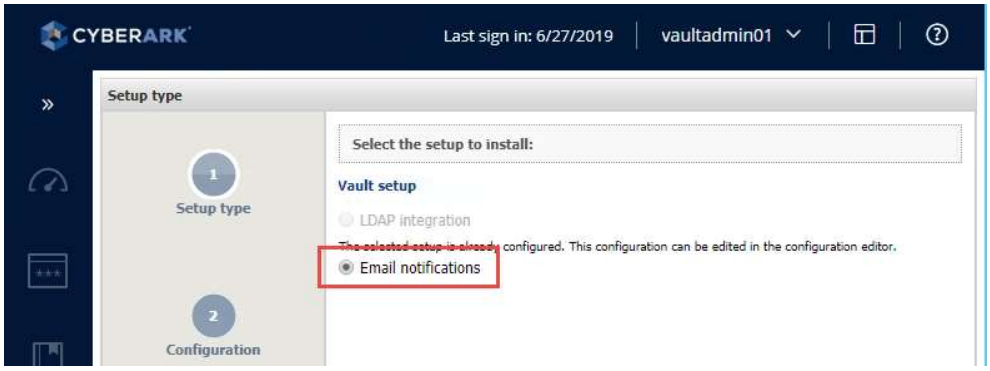
Objective: Configure SMTP integration

Note: Prior to setting up the SMTP integration, verify that the *CyberArk Event Notification Engine (ENE)* service is running on the **Vault**. This service may not start if the Vault VM has been suspended, then reanimated.

1. On Comp01A or B Server, launch the PVWA, select **LDAP** as the Authentication method and sign in as vaultadmin01.

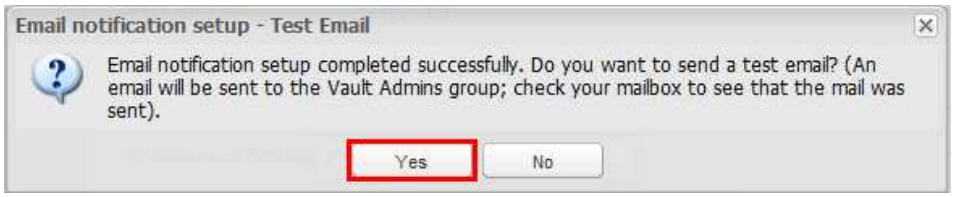
1. Go to **ADMINISTRATION > Configuration Options** and click the Setup Wizard.
2. Select **Email Notifications** and click Next.
3. Enter the following:

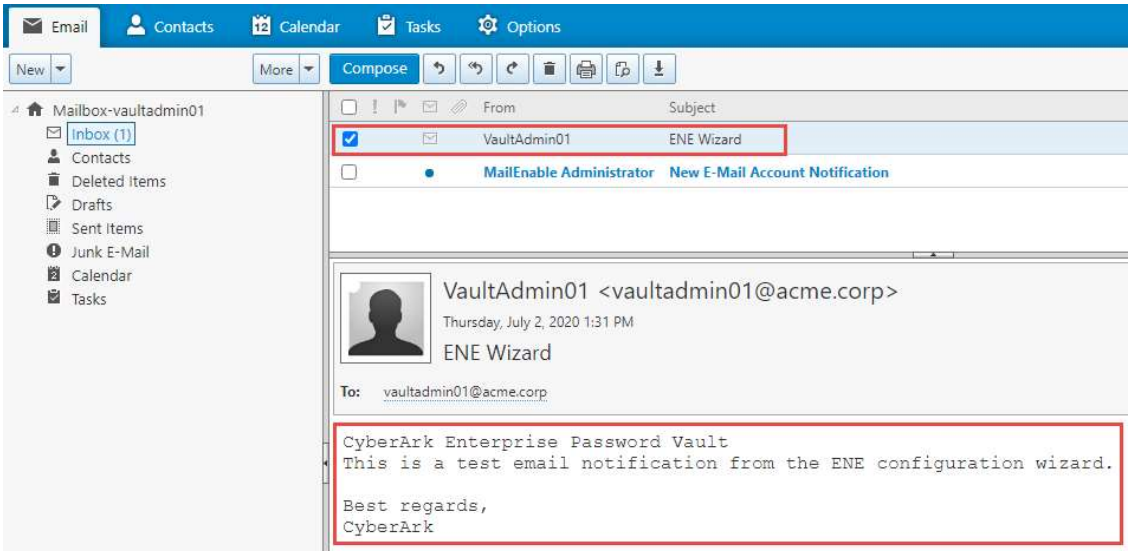




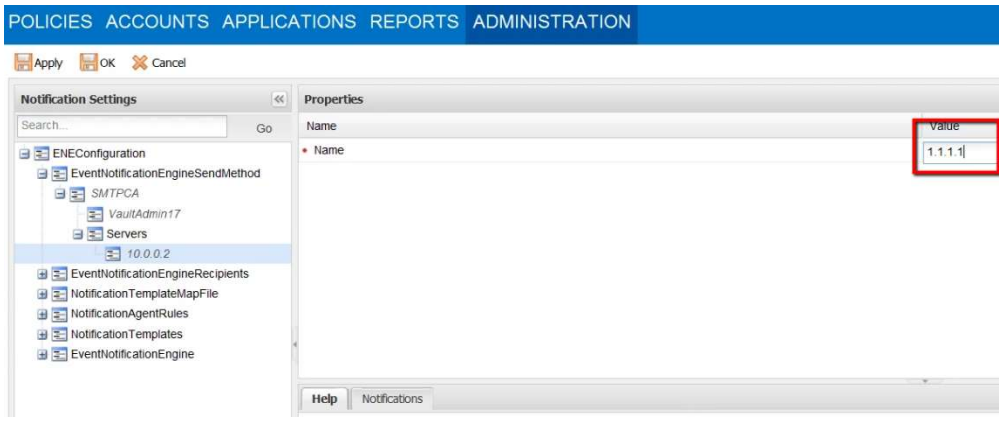
SMTP address:	*10.0.0.2*
Sender Email:	*vaultadmin01@acme.corp* (mailto:vaultadmin01@acme.corp)
Sender Display Name:	*VaultAdmin01*
SMTP Port:	*25*
PVWA URL:	*<Accept* (http://127.0.0.1) *the default>*
Recipients Domains	*Leave blank*

1. Press **Finish**.
2. Press **Yes** to send a test e-mail.
3. Using the Chrome Browser, select CAU Lab Links > ACME WebMail (http://webmail.acme.corp/Mondo/lang/sys/Login.aspx (http://webmail.cyber-ark-demo.local/Mondo/lang/sys/Login.aspx)).
    a. Login as *vaultadmin01* / Cyberark1.
    b. Ensure that you receive the email from the ENE Wizard.
4. Close the Webmail application.





Troubleshooting*:* If you need to run the wizard again, you can change the IP address of the SMTP server to *1.1.1.1* and save, as shown in the graphic below. Also ensure that the Event Notification Engine service is running on the Vault Server.



Note: CyberArk's Digital Vault supports authenticated and encrypted email notifications. For more information, search docs.cyberark.com (https://docs.cyberark.com) for "Authenticated and encrypted email notifications (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/Event-Notification-Engine.htm?Highlight=Authenticated%20and%20encrypted%20email%20notifications#Authenticatedandencryptedemailnotifications)"

.

SIEM Integration

Objective: Configure the **Vault** server to communicate with a SIEM. This section will demonstrate how to forward audit records to a SYSLOG server, such as *Arcsight* or *enVision*.

Note: Ensure all Virtual Machines are running!

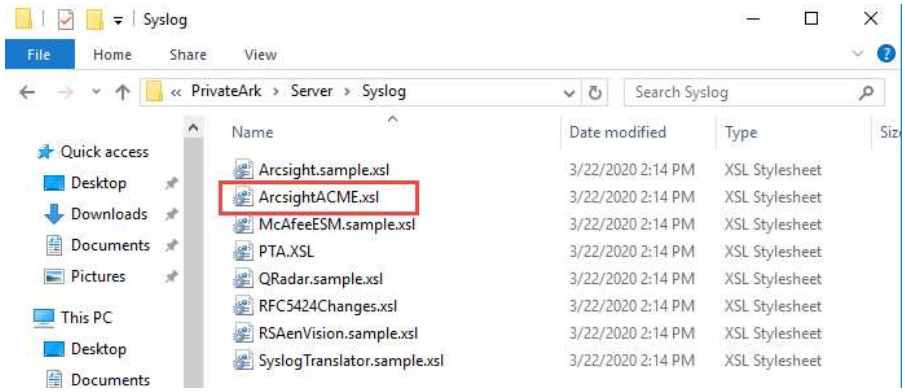
<u>Prepare the Vault</u>

Note: The Vault supports encrypted protocols to the SIEM. For more information, search for "Security Information and Event Management (SIEM) Applications (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASIMP/DV-Integrating-with-SIEM-Applications.htm?

Highlight=SIEM%20Integration)" online at docs.cyberark.com.

1. Sign in to the **Vault** server as Administrator / Cyberark1.
2. Open Windows File Explorer and navigate to: C:\Program Files(x86)\PrivateArk\Server\Syslog.

1. Make a copy of the file *Arcsight.sample*.xsl and rename it to *ArcsightACME.xsl*.



1. Navigate to C:\Program Files(x86)\PrivateArk\Server\Conf.
   a. Edit the DBPARM.sample.ini file. Copy the entire [SYSLOG] section.
   b. Edit the dbparm.ini file. Paste the contents of the clipboard overwriting the existing [SYSLOG] section.
   c. Edit the [SYSLOG] section as shown below, removing the comment "*" from the beginning of each line and modifying the parameters as shown.

```
[SYSLOG]
SyslogTranslatorFile=Syslog\ArcSightACME.xsl
SyslogServerPort=514
SyslogServerIP=10.0.0.20
SyslogServerProtocol=UDP
SyslogMessageCodeFilter=0-999
SyslogSendBOMPrefix=NO
UseLegacySyslogFormat=yes
SendMonitoringMessage=No
```

Note: The default [SYSLOG] section copied from DBPARM.SAMPLE.INI is an example that illustrates how to configure the Vault to forward SYSLOG message to multiple endpoints. Observe that each parameter is separated by a comma. In this lab we are only forwarding to a single SYSLOG endpoint.

Note: The settings above will forward all *syslog* messages to the SYSLOG server. See Vault Audit Action Codes (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PASREF/Vault%20Audit%20Action%20Codes.htm?tocpath=Administration%7CReferences%7C_____3) on docs.cyberark.com for instructions on filtering these messages if required.

1. Save and exit the file.
2. Restart the PrivateArk Server service to read the changes made to dbparm.ini into memory. It is best to do this from the Windows Services applet.

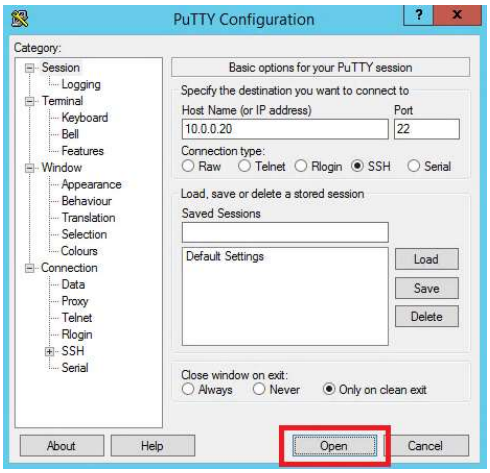
IMPORTANT: Check the ITALOG.log to validate success and identify any possible syntax errors.

-

Confirm SYSLOG Configuration

1. Sign in to either Comp01A or Comp01B server as local Administrator.
2. Launch **putty** from the Windows Taskbar.

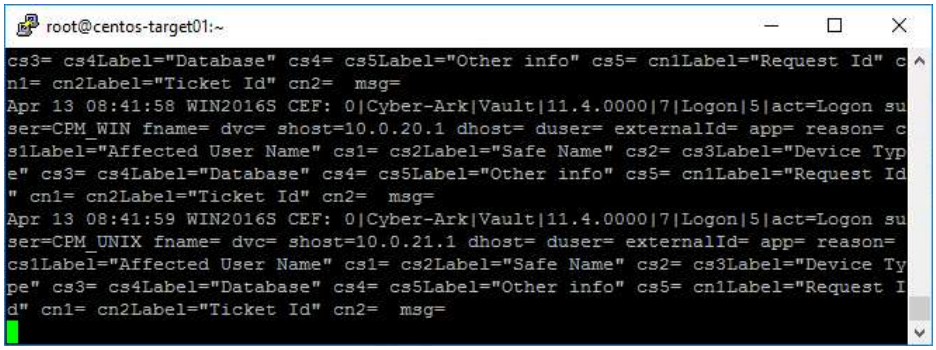
1. Enter *10.0.0.20* as the Host Name or IP address) and click Open to launch an SSH connection.
2. Click **Yes** to accept the server's key, if prompted.
3. Login as *root01* with the password Cyberark1. Accept any security warning you may receive.
4. Enter one of the following commands to view SYSLOG messages received.



cat /var/log/messages | grep VAULT

Or to view the running activity log of your Vault.

tail -f /var/log/messages | grep VAULT

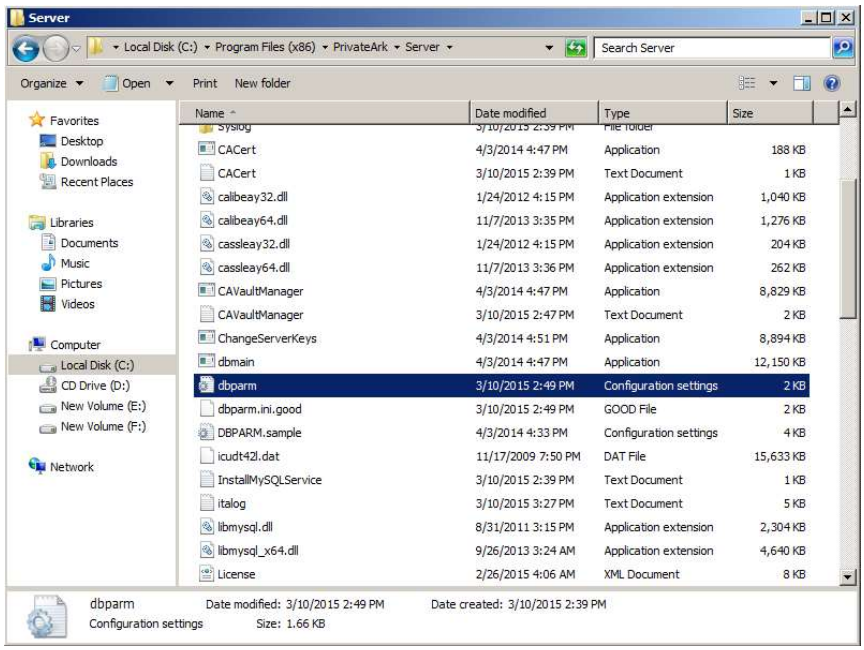


NTP Integration

Objective: Configure the Vault Servers system clock to synchronize with an internal (to the company) time source.

Note: Time synchronization is critically important in CyberArk PAM architecture. In the following exercise we will integrate the Vault Server with an external time source.

1. Sign into your Vault Server as Administrator.
    a. Using Windows File Explorer navigate to 'C:\Program Files(x86)\PrivateArk\Server\Conf' and edit the dbparm.ini file.
2. Add the following lines 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.



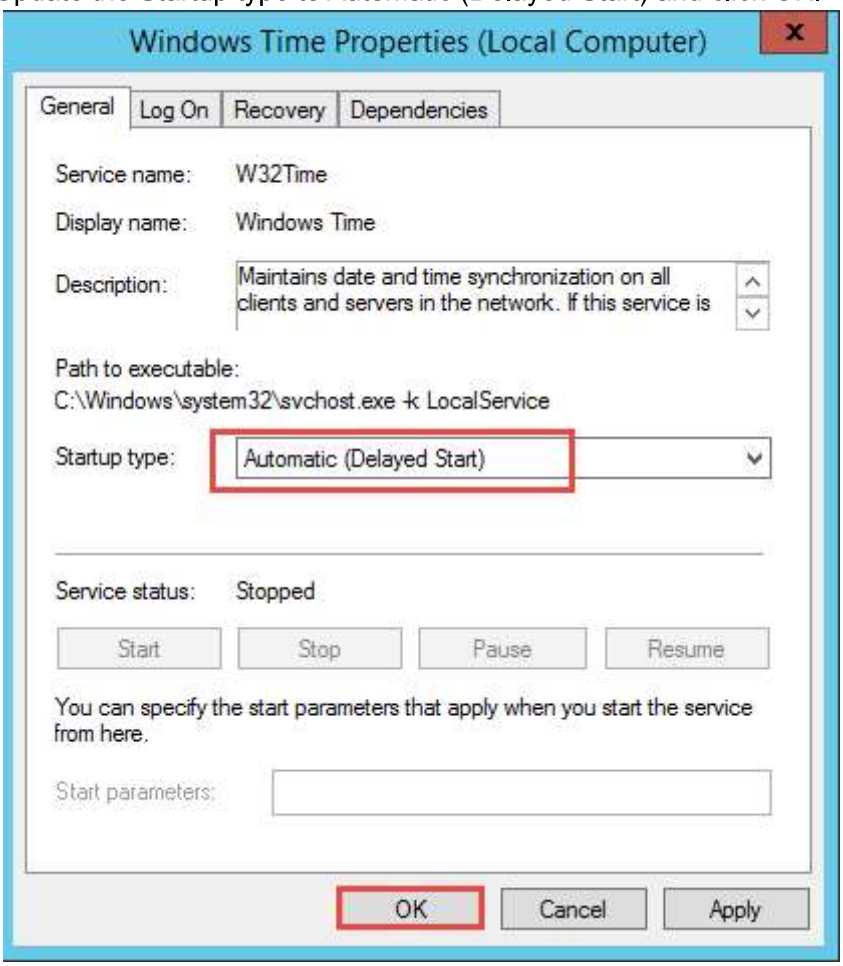

```
[NTP Firewall Rule]
AllowNonStandardFWAddresses=[10.0.0.2],Yes,123:outbound/udp
```

1. To commit the changes made to the DBParm.ini file, restart the PrivateArk Server service.

IMPORTANT: Check the ITALOG.log to validate success and identify any possible syntax errors.

1. Next we must confirm the Windows Time service is running. Open Windows Services applet from the Taskbar.
2. Double click "Windows Time" to display the service properties.

3. Update the Startup type to Automatic (Delayed Start) and click OK.



4. Start the Windows Time service or restart if already running.

Tip: Set the system clock back 5 minutes manually before proceeding. After entering the following command, the system clock should sync with the time source to provide validation that time synchronization is successful.

1. Open an Administrative Command prompt and run the following command:

W32tm /config /manualpeerlist:10.0.0.2 /syncfromflags:manual /reliable:YES /update

1. The system clock should adjust and display the correct time.

Authentication Types

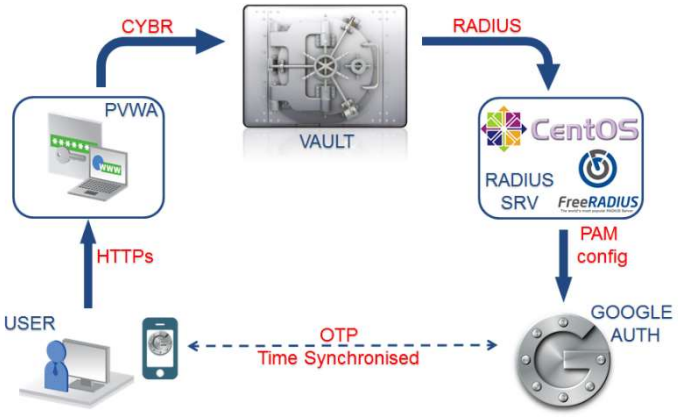
In this section you will configure multiple authentication methods. Detailed information on authentication can be found by searching for “Authentication” on docs.cyberark.com.

RADIUS Authentication

Note: Ensure that all Virtual Machines(VM’s) are started in your Skytap lab before proceeding (with the exception of the DR VM).

Objective: Enable RADIUS authentication, and test 2 Factor Authentication.

You will have the option to download the application “Google Authenticator” on your smartphone to generate a RADIUS token. If you do not wish to install the app on your phone you have the option to use the emergency scratch code tokens, provided to you when you register a user in Google Authenticator.

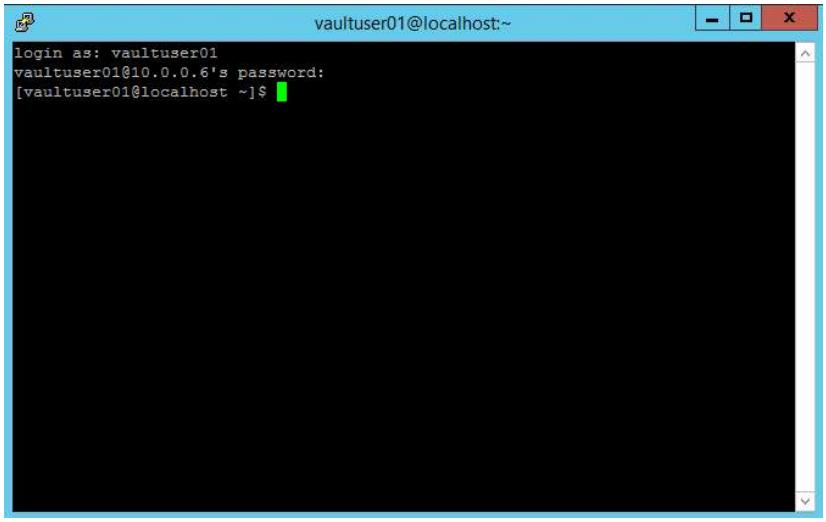


-

-

Enroll User in RADIUS

1. Sign in as VaultAdmin01@ACME.Corp (mailto:VaultAdmin01@ACME.Corp) to Comp01A or Comp01B server.
2. Launch Putty from the Taskbar and establish an SSH terminal session to the RADIUS server (10.0.0.6).
   a. Login with *vaultuser01/Cyberark1*.
3. Next, run the following command as shown to register your vaultuser01 account:



google-authenticator

a. Respond to the following prompts as indicated

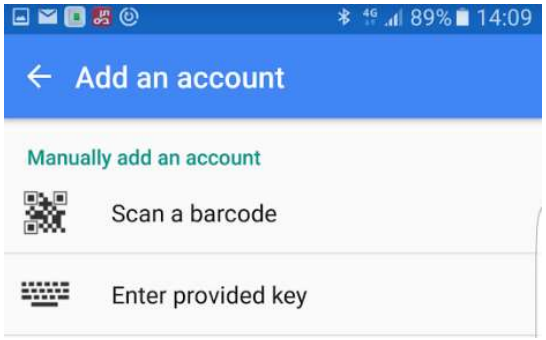
- Do you want authentication tokens to be time-based (y/n) Y
- Do you want me to update your "/home/vaultuser01/.google_authenticator" file (y/n) Y
- Do you want to disallow multiple uses of the same authentication token? This restricts you to one login about every 30s, but it increases your chances to notice or even prevent man-in-the-middle attacks (y/n) N

- By default, tokens are good for 30 seconds and in order to compensate for possible time-skew between the client and the server, we allow an extra token before and after the current time. If you experience problems with poor time synchronization, you can increase the window from its default size of 1:30min to about 4min. Do you want to do so (y/n) Y
- If the computer that you are logging into isn't hardened against brute-force login attempts, you can enable rate-limiting for the authentication module. By default, this limits attackers to no more than 3 login attempts every 30s. Do you want to enable rate-limiting (y/n) Y

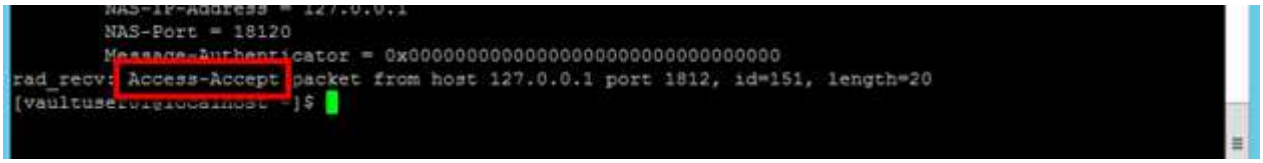
1. Select the context menu in the terminal window (top left corner) > Copy All to Clipboard, then paste into Notepad for future reference.

Note: If you do not want to install Google Authenticator on your smart phone, skip to step 7 and use the scratch codes provided during RADIUS registration in step 2.

1. Copy the URL displayed by Google Authenticator and paste it into your browser.
2. Scan the code using the Google Authenticator App on your phone.
3. This app will present you with a new OTP every x seconds to be used to authenticate as this user.
4. Verify the radius integration works locally, use the following command. Use a scratch code for the token, or generate a token from the Google Authenticator application on your phone. Verify you receive Access-Accept in the reply:



radtest vaultuser01 <token> localhost 18120 testing123



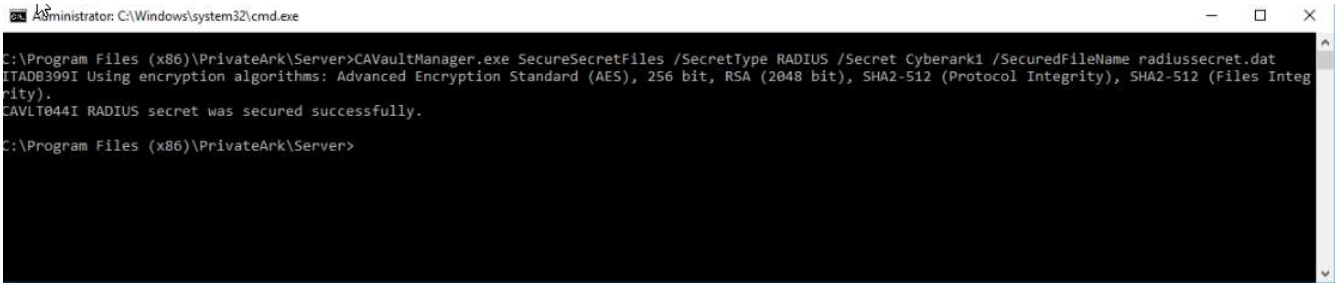
Note: The VAULT server has been added as a RADIUS Client by the RADIUS Administrator. The RADIUS Administrator has also chosen a RADIUS Secret and provided it to you, the Vault Administrator. The RADIUS Secret enables the Vault to authenticate to the RADIUS server. The RADIUS Secret provided is “Cyberark1” without the double quotes.

<u>Configure the Vault Server to use RADIUS Authentication</u>

Objective: Configure the Vault Server to use RADIUS Authentication

1. Sign in to VAULT server as Administrator/Cyberark1 and open a Command Prompt(or Windows PowerShell) as Administrator in folder “C:\Program Files (x86)\PrivateArk\Server”.
2. Enter the following command to save the RADIUS Secret to the encrypted file name, radiussecret.dat.

CAVaultManager.exe SecureSecretFiles /SecretType RADIUS /Secret Cyberark1 /SecuredFileName radiussecret.dat



1. Remain at the Command Prompt. Change directories to \Conf. Type “notepad dbparm.ini” and add the following two lines to the end of the file. Save the changes to the dbparm.ini and restart the PrivateArk Server.

[RADIUS]

RadiusServersInfo=10.0.0.6;1812;VAULT;radiussecret.dat

1. Restart the PrivateArk Server service using services.msc, to read the changes made to dbparm.ini into memory.
    a. Check the ITALOG.LOG for possible warnings or errors.

-

-

-

-

-

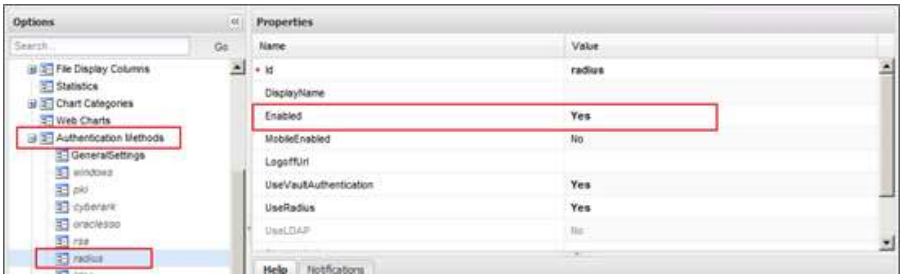
-

-

-

Enable RADIUS Authentication in the PVWA

1. Sign in to the PVWA from Comp01A or Comp01B, as VaultAdmin01.
2. Navigate to Administration > Configuration Options > Component Settings > Options > Authentication Methods > radius. Change the Enabled parameter to Yes.
    a. You can also add a custom entry for “PasswordFieldLabel” to notify the user they need to authenticate using the token. Save your changes.



1. Sign out of the PVWA.
2. Using the PrivateArk Client, logon to the Vault as Administrator.

Note: You may need to add a new Vault server definition. In the PrivateArk Client select **File** > New > Server and complete the New Server form using the Vault's IP address 10.0.10.1

1. Navigate to Tools > Administrative Tools > Directory Mapping.
2. Update Directory Map "Users_acme.corp".
3. Edit the User Template, changing the authentication method to RADIUS Authentication.

Note: Changing the authentication type required in the User_acme.corp directory map will require **new vault users** from the group defined in the Directory Map Rule to use RADIUS authentication. Existing users will not be affected.

1. Logoff the PrivateArk Client.
2. At the PVWA login, attempt to login as **vaultuser01** using RADIUS authentication. Verify you can login using a scratch code, or the token provided by google-authenticator.

Note: Scratch codes can only be used once. Select a scratch code that was not previously used to test enrollment with the radtest command.

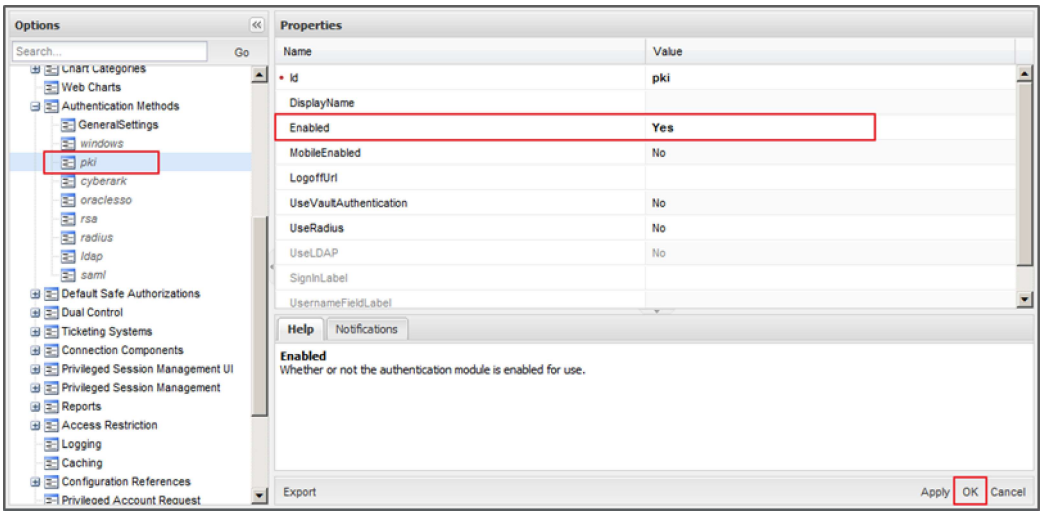
PKI Authentication

Objective: Provision a User Digital Certificate from a Certificate Authority and save it in the Windows Personal Certificate Store.

Configure the PVWA to authenticate using PKI.

Enable PKI Auth in PVWA

1. Sign in to the PVWA using LDAP authentication as Vaultadmin01.
2. Navigate to Administration > Configuration Options > Component Settings > Options > Authentication Methods > pki.
3. Select Enabled = Yes and save the changes.
4. Sign out of the PVWA.

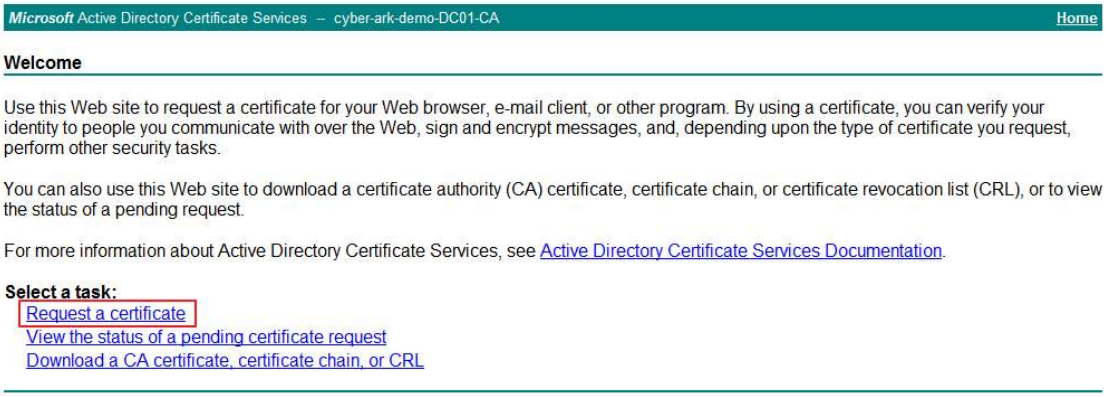


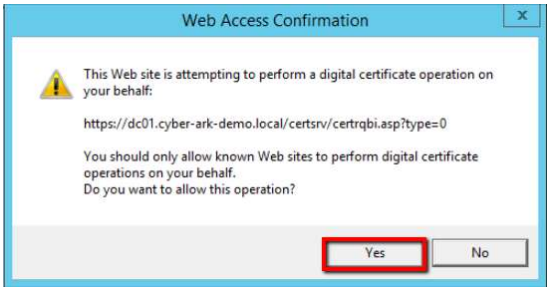
Provision a User Digital Certificate

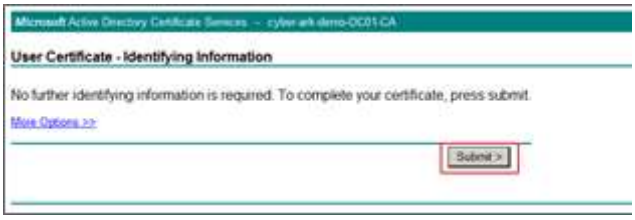
1. Sign in to the Comp01A/B server as VaultAdmin01@acme.corp

2. Using Internet Explorer (not FF or Chrome) browse to https://dc01.acme.corp/CertSrv (https://dc01.cyber-ark-demo.local/CertSrv). If prompted login as vaultadmin01/Cyberark1.

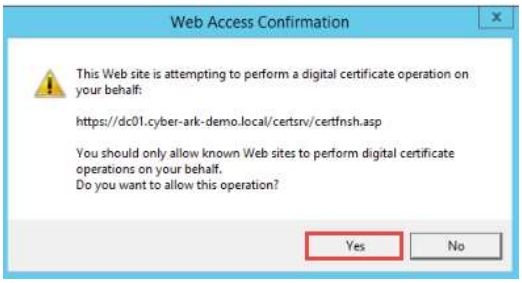
1. Click Request a certificate.
2. Click User Certificate.
3. Click yes to the warning, then click Submit.



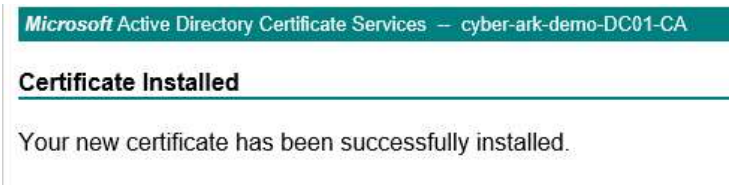




1. Click yes to the warning, then click “Install this certificate”.



1. You should receive the following successful message.



-

-

Configure PVWA Support for PKI

Objective: Configure the PVWA to support PKI authentication. The following procedure is further explained in CyberArk KB article 00004569 titled *"PKI logon to v10 interface fails with error: Missing mandatory parameter [certificate]"*

1. Using File Explorer, navigate to C:\Windows\System32\Inetsrv\Config\.
2. Use Notepad (not Notepad++) edit file, applicationHost.config.
   a. Locate towards the end of the file the following snippet of text.

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

1. Modify the value of "location path=" as shown here:
   a. From: "Default Web Site/PasswordVault/auth/pki/"
   b. To: "Default Web Site/PasswordVault/api/auth/pki/logon"
2. Save the file.
3. Open Windows PowerShell as Administrator and run IISRESET.
4. Repeat bullets 1-5 on all PVWA servers.

Sign in to PVWA using PKI

1. Login to the PrivateArk Client as Administrator.

Note: You may need to add a new Vault server definition. In the PrivateArk Client select **File** > New > Server and complete the New Server form using the Vault's IP address 10.0.10.1

1. Navigate to Tools, Administrative Tools, Users and Groups. Locate and delete user, VaultAdmin01.

Note: Deleting the Transparent user VaultAdmin01 will allow the PKI authentication attempt to create a new VaultAdmin01 transparent user with a DN value that will support the users certificate.

1. Sign in as VaultAdmin01 on the PVWA server where the certificate was issued. Using Google Chrome browse to the PVWA at URL https://pvwa.acme.corp/passwordvault/v10/logon/

(https://pvwa.acme.corp/passwordvault/v10/logon/) and choose PKI. This step must use Chrome or IE.

2. A note on the behavior of PKI Authentication using IE on Windows.
    a. If the URL is in the Intranet Zone and the certificate is valid, the user will be authenticated successfully and passed directly to the accounts page.
    b. If the URL is in the Trusted Sites Zone and the certificate is valid, the user will be prompted to confirm the certificate.

-

Two Factor Authentication (2FA)

In CyberArk There are 2 groups of authentications.

PVWA (IIS) level (Primary) authentication	• Windows, Oracle SSO, PKI (Client Certificate) RSA, SAML.
Vault level (Secondary) authentication	• CyberArk • LDAP, RADIUS

Challenge: Attempt to configure 2-Factor authentication combining PKI (IIS level) with LDAP Authentication (Vault Level). Note: Reset the Users Directory Map authentication requirement to LDAP and delete any users from the PrivateArk Client.

EPV Testing and Validation

Objective: Create several accounts to validate and test the basic features and functionality of the installed components.

Sign in to the PVWA using VaultAdmin01.

Note: Ensure that all Virtual Machines(VM's) are started in your Skytap lab before proceeding (with the exception of the DR VM).

Add Windows Domain Account

1. Create safe 'Windows Accounts'
    a. Assign to CPM : PasswordManager
    b. Add Safe Member: Search ACME.CORP domain and add LDAP group 'WindowsAdmins' with default permissions
2. Duplicate the Windows Domain Accounts platform and name it "ACME Windows Domain Accounts".
3. Create Admin01 LDAP account.
    a. Store in safe 'Windows Accounts' and assign it to the platform created in step 2
    b. Address equals "acme.corp"
    c. Select the "Logon To:" parameter and click "Resolve" to populate the field
    d. Password equals Cyberark1
4. Perform a Verify and Change operation.

Add Windows Server Local Account

1. Duplicate the ‘Windows Server Local Accounts’ platform and name it, “ACME Windows Server Local Accounts”.
2. Create account localadmin
    a. Store in safe ‘Windows Accounts’ and assign it to the platform created in step 1.
    b. Address equals “comp01c.acme.corp”
    c. Select “Log On To:” and enter “COMP01C” to populate the NetBIOS name.
    d. Password is unknown. Leave the password field blank.
3. Click on additional details & actions, reconcile account and associate admin01 account as the reconcile account for LocalAdmin.
4. Execute a Reconcile operation.

Add Linux Root Account

1. Create a safe to store Unix accounts named “Linux Accounts”
    a. Assign CPM: CPM_UNIX
    b. Assign default permissions to ldap group ‘LinuxAdmins’
2. Duplicate the ‘Unix via SSH’ platform. Name it “ACME Unix via SSH Accounts”
3. Create the Unix account root01 in safe ‘Linux Accounts.
    a. Assign to “ACME Unix via SSH Accounts” platform created in a prior step
    b. Address = centos.acme.corp
    c. Password = Cyberark1
4. Perform a Verify and Change operation

Add Oracle Database Account

1. Create a safe to store Oracle accounts named ‘Database Accounts’
    a. Assign CPM: CPM_UNIX
    b. Assign default permissions to ldap group ‘OracleAdmins’.
2. Duplicate the ‘Oracle Database’ platform and name it ‘ACME Oracle Database Accounts’. Change the status to Active.
    a. Edit the “ACME Oracle Database Accounts” platform.
    b. Navigate to Automatic Password Management > Generate Password. Update the MinSpecial parameter to a value of -1.
    c. Save the changes.
3. Create the Oracle account dba01 in ‘Database Accounts’ safe
    a. Assign to ‘ACME Oracle Database’ platform.
    b. Address = centos.acme.corp
    c. Database = xe
    d. Port = 1521
    e. Password = Cyberark1
    f. Save the changes.
4. Perform a Verify and Change operation.

Note: After completing the above tasks, you should have four test accounts whose passwords have been verified and changed by a CPM; localadmin, admin01, root01 and dba01.

Ensure the Users_acme.corp Directory Mapping authentication requires LDAP

1. Sign in to the PVWA using the following LDAP users to ensure they can access the appropriate accounts,
    a. winadmin01
    b. linuxadmin01
    c. oracleadmin01

Install PSM

The Customer has purchased CyberArk's **Privileged Session Management** (PSM) to monitor and record activity related to privileged accounts in the network:

PSM	2 servers Comp01c.acme.corp (10.0.22.1) Comp01d.acme.corp (10.0.23.1)

-

Note: Ensure that all Virtual Machines (VM's) are started in your Skytap lab before proceeding with the exception of the DR VM.

Objective: Install and configure 2 Standalone PSM Servers in a Load Balanced Configuration.

Install a Standalone PSM Server

The PSM installation is divided into several configurable stages: setup (prerequisites), installation, post installation, Hardening and registration.

Note: To learn more about the actions performed by the CyberArk PowerShell scripts described in this section, please refer to **docs.cyberark.com**

PSM Installation Prerequisites

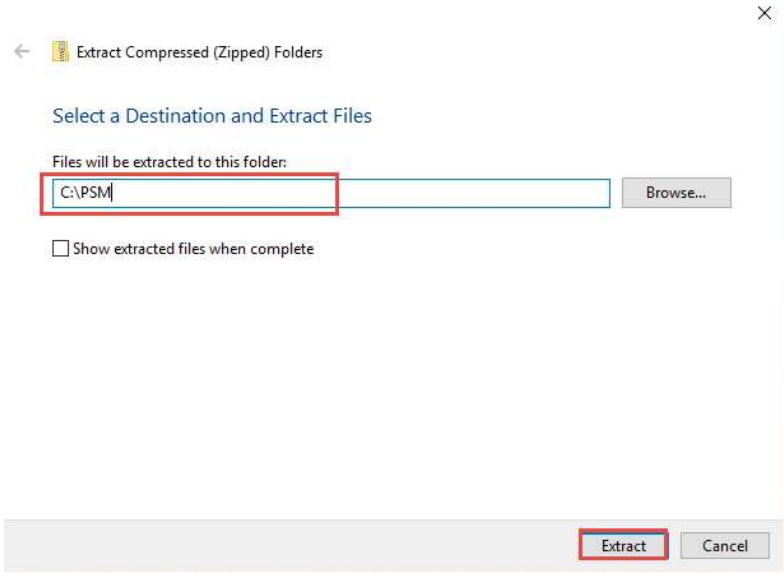
Objective: Execute PowerShell scripts to install Remote Desktop Session Host on Windows. It is recommended to perform a graceful restart of the component server prior to installation to clear any pending restarts and software updates.

1. Sign in to the Comp01C server as Admin02@acme.corp/PW=Cyberark1.

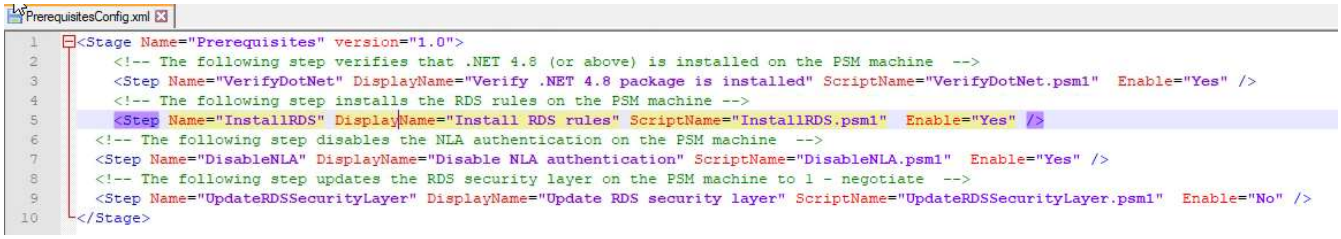
1. Open File Explorer and navigate to the shared resource folder, Z:\. If the drive is not mapped, map a network drive to Z: at \\dc01\shared.
    a. Navigate to "Z:\CyberArk PAM Solution\v12.6". Copy the following zip files to "C:\CYBR_Files".
        - "Privileged Session Manager-Rls-v12.6.zip"
        - "Client-Rls-v12.6.zip"

Note: The installation folder for PSM must not be in a deep directory structure. Shorten the directory path of the extracted folders as follows.

a. Extract all files from "Privileged Session Manager-Rls-v12.6.zip" to the destination folder "C:\PSM" as shown below.



1. In File Explorer, navigate to “C:\PSM\InstallationAutomation\Prerequisites”.
2. Open **PrerequisitesConfig.xml** using Notepad. Review the options but make no changes. Accept the defaults and continue.
3. Open Windows PowerShell as Administrator. Change directories to **“**C:\PSM\InstallationAutomation”.
4. Execute the following commands.



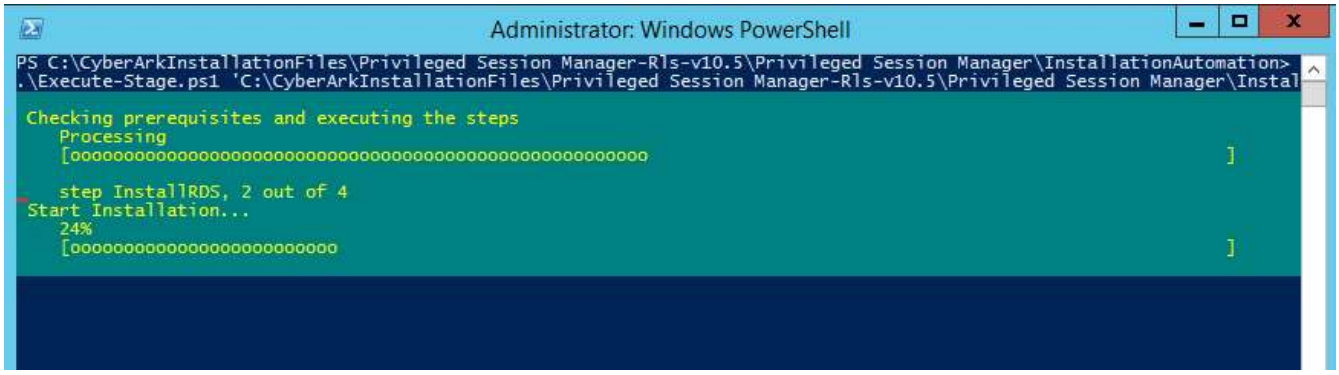
Get-ExecutionPolicy (Result should be “Restricted”)

Set-ExecutionPolicy Bypass -Scope Process

1. Then launch the Execute-Stage.ps1 script with the location of the PrerequisitesConfig.xml as the argument. Example:

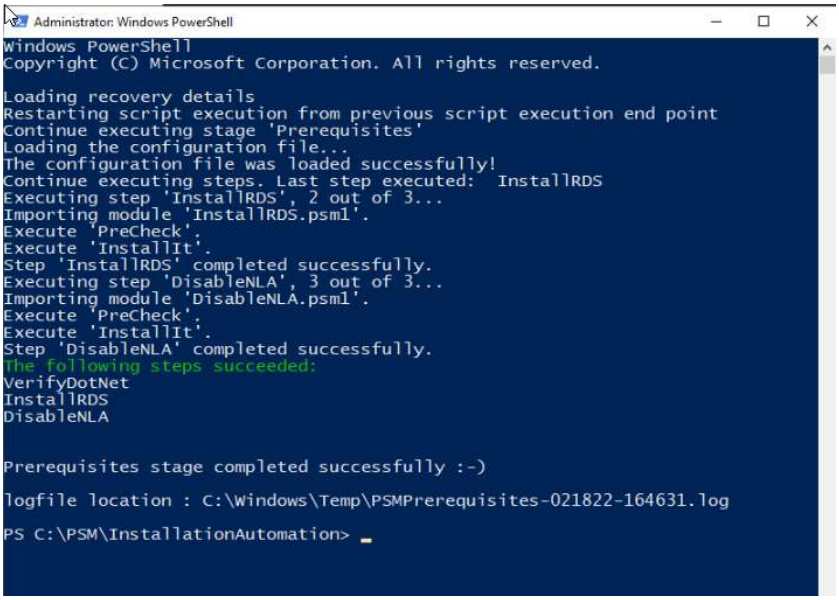
.\Execute-Stage.ps1 “C:\PSM\InstallationAutomation\Prerequisites\prerequisitesConfig.xml”

1. Several scripts will be executed during this process.
2. When prompted in PowerShell, restart the server.
3. After the server restarts, sign in with the same credentials used in step 1, admin02@acme.corp/Cyberark1.



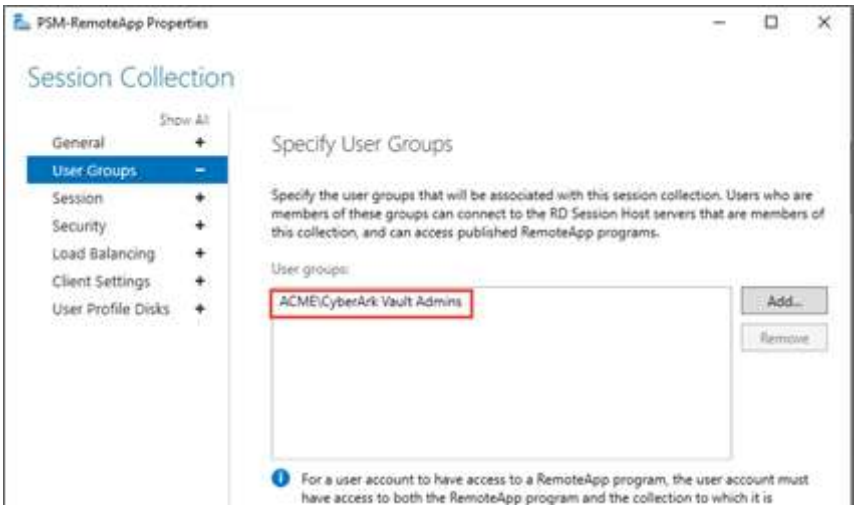
Note: Customer requirements are a PSM 'In Domain' installation to enable RemoteApp program features, thus the PSM installation prerequisites must be completed while signed in as a domain user with local Administrator rights.

1. The PowerShell script will launch immediately to complete the prerequisite installation. Allow the script to complete, then exit PowerShell.
2. Review the PSMPrerequisites<date><time>.log file located in C:\Windows\Temp directory.
3. A final step before PSM Installation is to assign an appropriate Domain Group access to the Session Collection. Open Server Manager and navigate to Remote Desktop Services -> Collections -> PSM RemoteApp > Properties > TASKS > Edit Properties -> User Groups.



Note: Please be patient. It may take a few minutes for the session collection to appear in Server Manager -> Remote Desktop Services.

a. Add **ACME\CyberArk Vault Admins** and remove ACME\Domain Users, as shown.



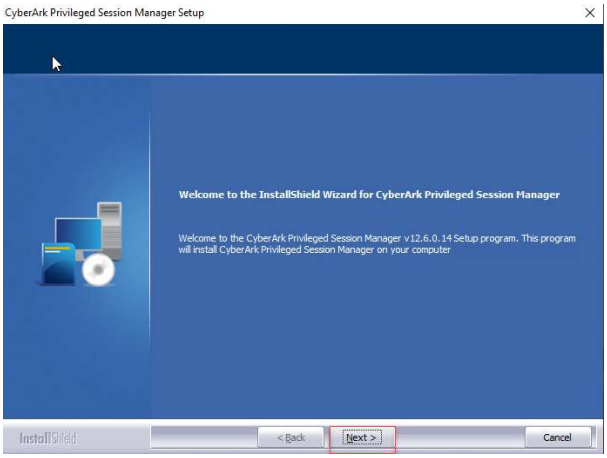
-

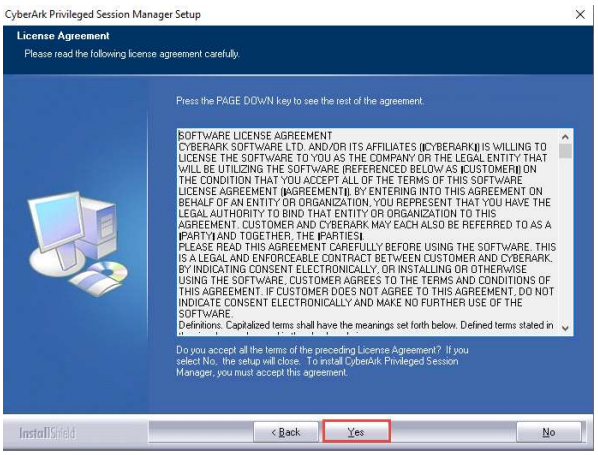
PSM Installation

Note: To enable RemoteApp program features, PSM installation must be completed while signed-in as a domain user with local Administrator rights. Install the PSM signed-in as Admin02@acme.corp

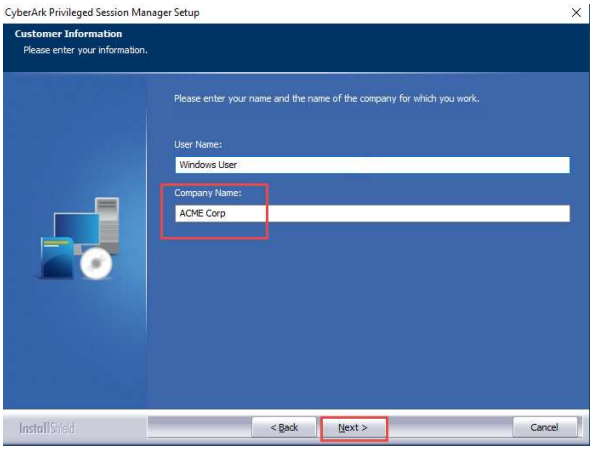
1. Sign-in to the Comp01C server as Admin02@acme.corp/PW=Cyberark1
2. Using File Explorer, navigate to "*C:\PSM*". Right click setup.exe and choose "Run as administrator".

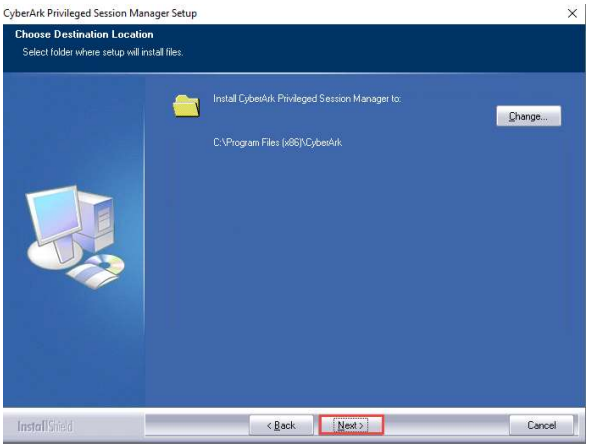
1. Select to install the Microsoft Visual C++ Redistributable Packages.
2. Click Next on the welcome screen, then Yes to agree to the license agreement



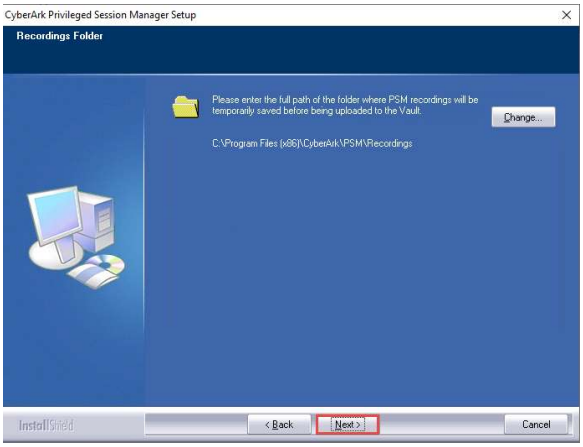


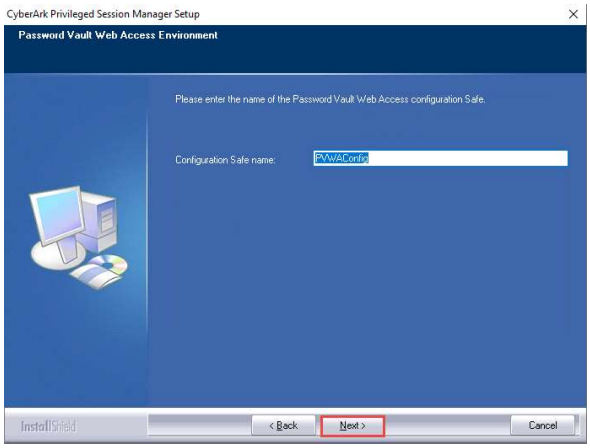
1. Enter a company name, click Next, then accept the default destination folder and click Next.



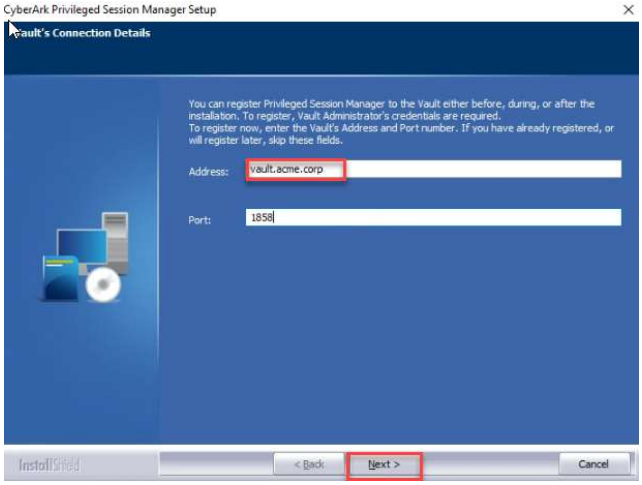


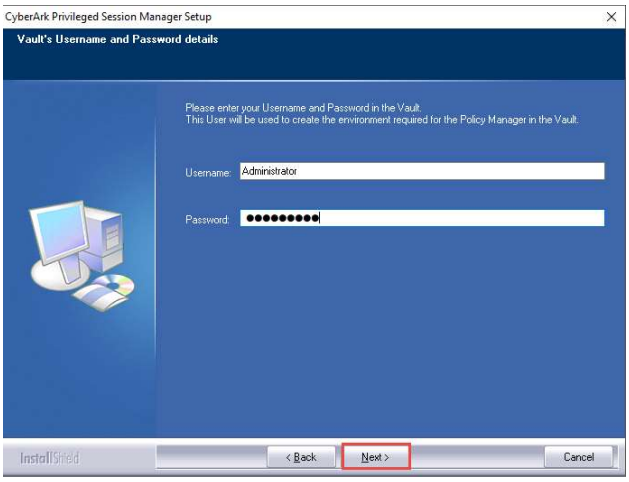
1. Accept the default Recordings Folder and click **Next**, then accept the default Configuration safes name and click Next.



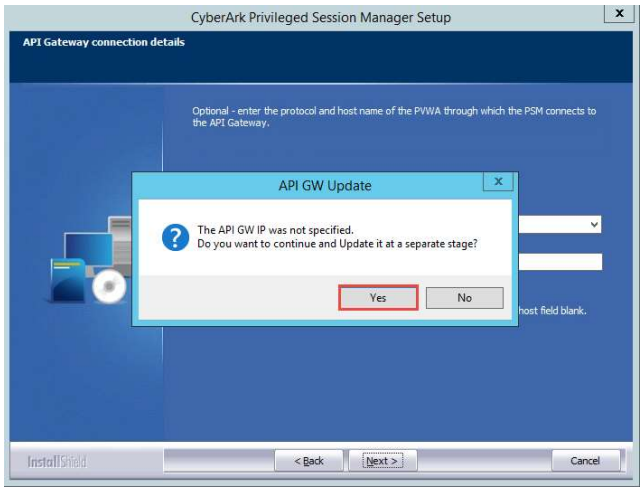


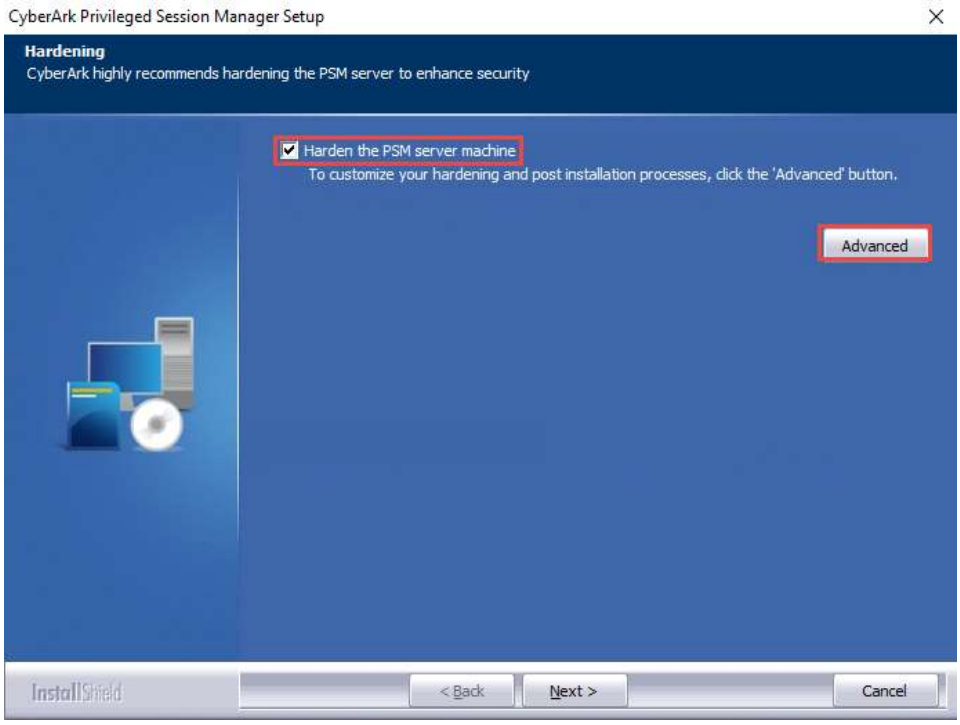
1. Enter the host name (i.e., vault.acme.corp) or IP Address of the vault (i.e., 10.0.10.1) and click Next, then enter the username Administrator, password Cyberark1 and click Next.



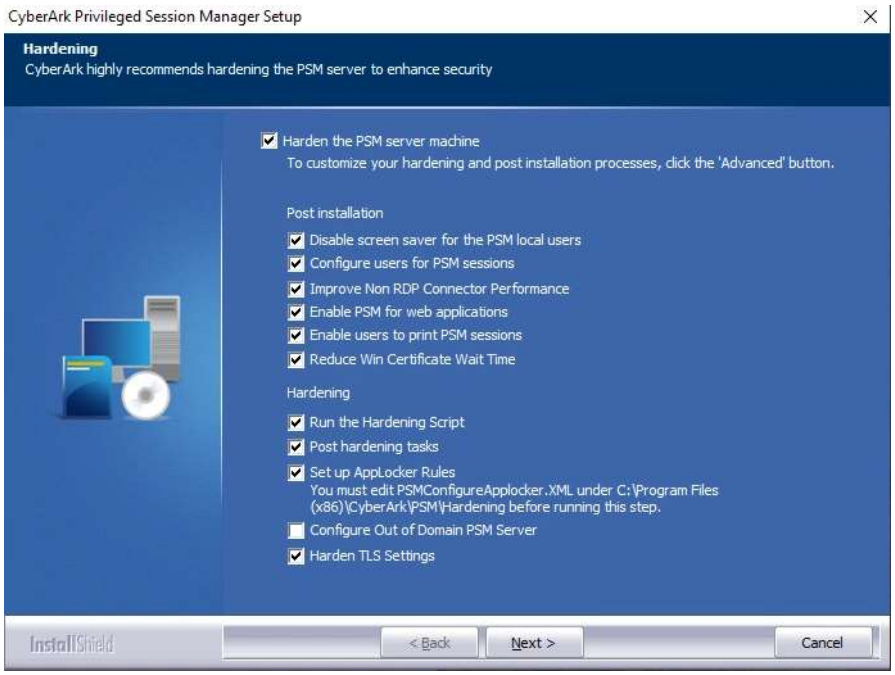


1. At API Gateway connection details option, select Next and Yes to confirm. We will not be configuring the API Gateway in this lab.
2. Do not select the “Enable PKI authentication for PSM” option and select Next.
3. Ensure “Harden the PSM server machine” checkbox is selected and click the Advanced option.



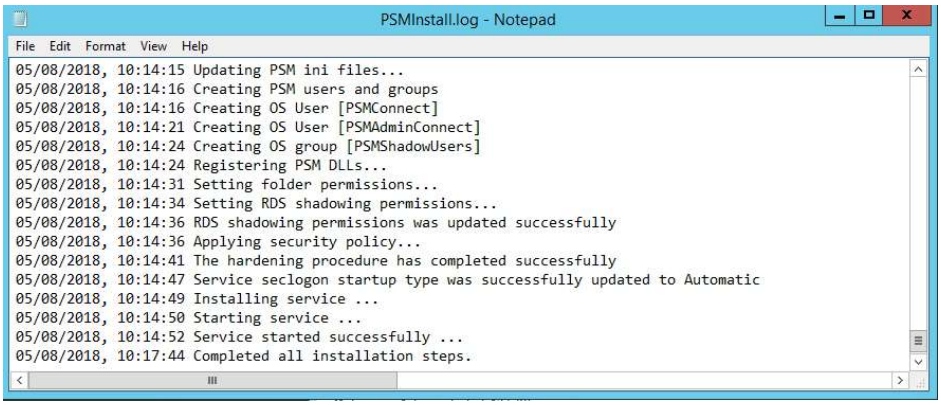


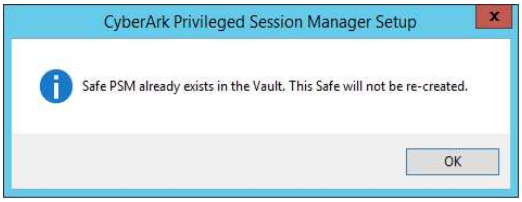
1. Select all options EXCEPT “Configure Out of Domain PSM Server” and click Next.
2. At InstallShield Wizard Complete windows, select “No, I will restart my computer later” and click Finish.
3. Install the PrivateArk Client and choose to restart the server when complete.
    a. Use the Vault IP address (10.0.10.1), for both Server Name, and Address fields, when defining the first Vault.

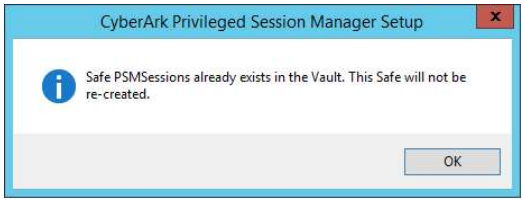


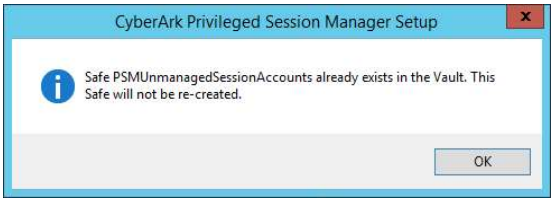
Note: It is important NOT to use a DNS host name when defining the server’s name in the Vault definition on the PSM server, to prepare for the PSM-PrivateArk Client connection component configuration, in a later exercise.

1. Following the installation and server restart, go to C:\Windows\Temp and review the PSM related log files; PSMHardening, PSMInstall, PSMPostInstallation log files.
2. Repeat the following steps on the Comp01D component server.
    a. PSM Installation Prerequisites
    b. PSM Installation
3. Multiple notifications are expected during the installation of additional PSM servers. These are expected and normal. Accept each notification by clicking the OK button.









PSM Hardening for In-Domain Deployments

The PSM hardening stage enhances PSM security by defining a highly secured Windows server.

Objective: Enable the PSM Hardening GPO for the PSM Servers in Active Directory Group Policy Management.

1. Sign in to the DC01 Virtual Machine as Administrator/Cyberark1.
2. On the Desktop, open the Group Policy Management Console.
3. Expand acme.corp > Servers > CyberArk and select the PSM Organizational Unit.
4. Right click the PSM Organizational Unit and select “Link an Existing GPO…”
5. Select “PSM Hardening” GPO and click OK.
6. In the “Linked Group Policy Object” tab, right click the “PSM Hardening” and select “Enforced”.
7. Select OK to confirm.
8. Close Group Policy Management Console and sign out of DC01 server.
9. Sign in to COMP01C as Admin02@ACME.Corp (mailto:Admin02@ACME.Corp). Open PowerShell as Administrator. Run the command “*gpupdate /force*”.
10. Repeat step 9 above on COMP01D.

PSM Testing and Validation

1. From Comp01A or Comp01B, sign in to the PVWA as vaultadmin01.
2. Navigate to Policies and change policy rule “Require privileged session monitoring and isolation” to Active.

1. Attempt connecting to the customer’s target devices using the relevant PSM Connection Components for all accounts (PSM-SSH, PSM-RDP and PSM-WinSCP).
2. Test each PSM server independently.
   a. The default PSM server specified in every platform is the very first PSM server installed, PSMSERVER.
   b. Retest every connection component after updating each target platform with the 2nd PSM Server ID, PSM-COMP01D.
3. Troubleshoot issues as needed.

Challenge: You should be able to connect to all accounts using available connection components with one exception, dba01 using PSM-SQL*Plus. Expected result is a PSM-SQLPlus recorded session. Actual result will be a PSMSR133E error.

What is the root cause of error PSMSR133E?

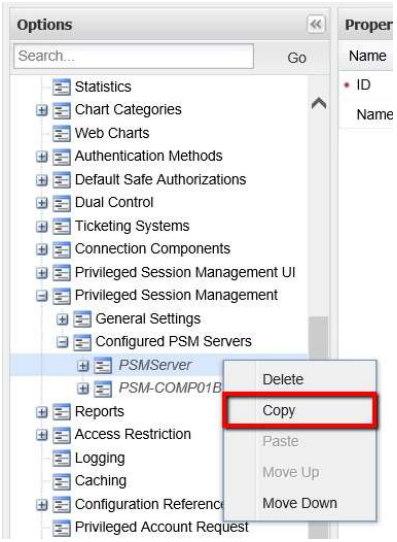
How might you resolve the issue when attempting to establish a PSM-SQL*Plus connection?

Load Balanced PSM Servers

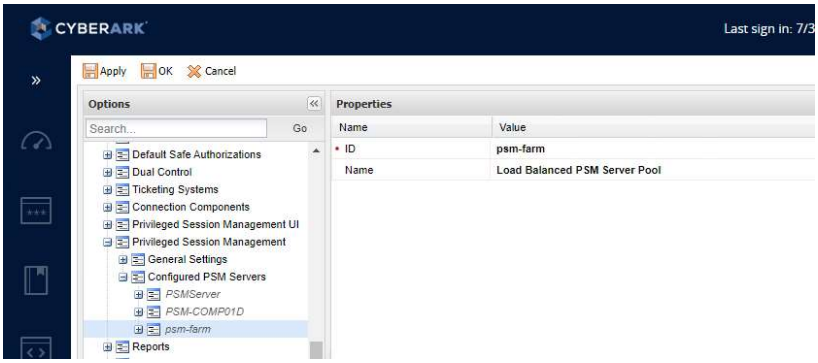
Configure PSM Load Balancing

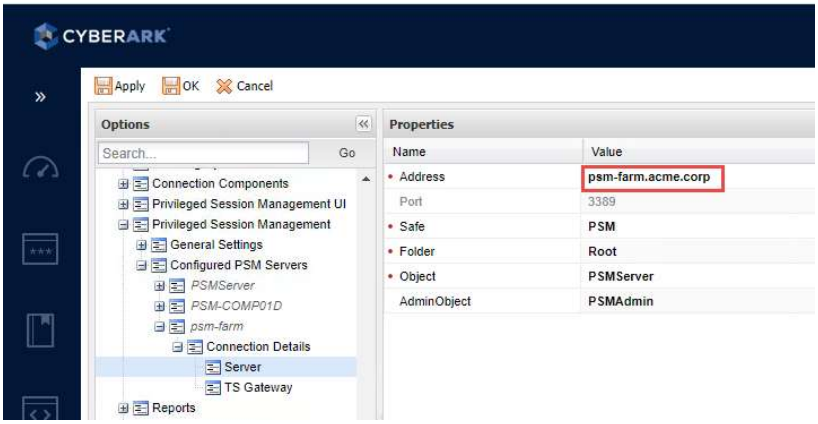
Objective: The Load Balancer in your lab environment is a Round Robin DNS. The Network Administrator has created a virtual pool of IP addresses and assigned a Virtual IP for the Load Balancer represented by, **psmfarm.acme.corp**. The following procedure guides you through the necessary changes to the PVWA to support PSM Load Balancing.

1. Login to the PVWA as vaultadmin01 and go to Administration > Configuration Options > Options > Privileged Session Management > Configured PSM Servers.
2. Right click on and copy the PSMServer folder.

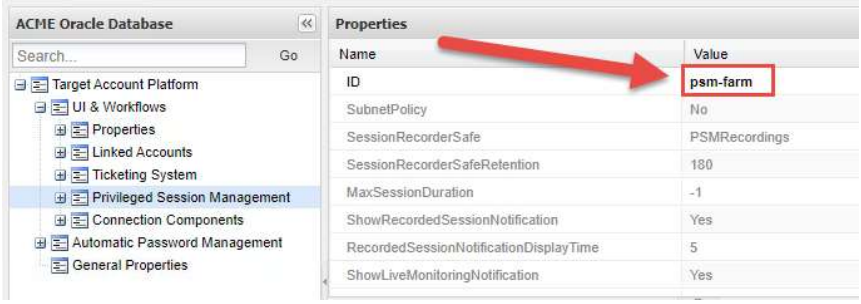


1. Right click on folder Configured PSM Servers. Select Paste PSMServer.
2. Go to the newly added *PSMServer* and change the ID to psm-farm and the name to Load Balanced PSM Server Pool.
3. Expand PSM-Farm. Select Connection Details > Server. Update the Address parameter to that of your PSM Farm virtual hostname, 'psm-farm.acme.corp'. Click on Apply and OK to save the changes.
4. Expand > Configured PSM Servers > PSMServer > Connection Details > Server and change the Address attribute to the FQDN of the PSM server (comp01c.acme.corp) so that it matches the name defined in the COMP01C server certificate that you will apply in the next section.
5. Click Apply to save the changes.
6. Repeat step 6 above, for Configured PSM Servers > PSM-COMP01D using comp01d.acme.corp.
7. Go to Manage Platforms and edit all active target platforms. Update PSM ID to reference psm-farm.





Note: This is a good time to update the status of all unused platforms to *"Inactive"* to optimize the performance of the CPM.



Update RDS Certificate

The following procedure will guide you through the steps to assign a certificate to the Remote Desktop Services deployment in support of the PSM Farm virtual hostname. A certificate has been provided by the Certificate Administrator for both PSM Servers; Comp01c and Comp01d.

1. Sign in to PSM Server Comp01c as Admin02.
2. Open Server Manager and select Remote Desktop Services in the left navigation pane.
3. In Deployment Overview select *Tasks* > *Edit Deployment Properties*. In the Configure the deployment window, select *Certificates* > *Select existing certificate…* > *Choose a different certificate* and browse to C:\CYBR_Files.
4. Select the file with the .pfx extension and click Open. In the Password: field enter *Cyberark1*, select the box to *"Allow the certificate to be added to the Trusted Root Certification Authorities…"* and select OK to close the Deployment Properties window.
5. Repeat steps 1-4 on PSM Server Comp01d.

Note: You must be signed in to one of the component servers, i.e., Comp01A/B with a domain account for PSM Connection Components to be successful. If signed into the server as the local Administrator, the current user will not have access to the Certificate Revocation List Distribution Point.

1. Attempt to connect to different target devices using the PSM-Farm virtual PSM server and observe there are no certificate errors using the psm-farm.acme.corp host name defined in the psm-farm server connection details.

PSM for SSH Installation

Objective: In this exercise you will install and configure a Linux server to run **CyberArk PSM for SSH** (PSMP) server **v12.2.** This version is compatible with the Digital Vault v12.6. See the Privileged Session Manager for SSH (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Installing-the-Privileged-Session-Manager-SSH-Proxy.htm#PrivilegedSessionManagerforSSH) section of *docs.cyberark.com* (https://docs.cyberark.com/Product-Doc/OnlineHelp/Portal/Docs.html) for a full explanation of all the required steps.

Note: Ensure that all Virtual Machines (VM's) are started in your Skytap lab before proceeding (with the exception of the DR VM).

<u>PSM for SSH (PSMP) Preparation</u>

Note: Installing applications in Windows is different than installing apps on a Linux Server. A Windows Installer program prompts for information, such as the Vault IP address, the directory path to install the software, e.g., the Administrator username and password, and accepting the EULA. On a Linux system these questions must be provided to the installer prior to launching setup in the form of text files.

1. Login into your PSMP server console as root/Cyberark1. Alternatively, you can connect to the PSMP server (10.0.1.16) using Putty from either Component Server.
2. Create an administrative user. Run 'useradd proxymng' to create the user account then set a password for the new account with the command 'passwd proxymng' as shown**.** Set the password as Cyberark1 and confirm.
3. Edit the vault.ini file. Change directories to /opt/CARKpsmp/ directory and edit the vault.ini file using the VI editor.

```
[root@centos ~]# useradd proxymng
[root@centos ~]# passwd proxymng
Changing password for user proxymng.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@centos ~]# _
```

cd /opt/CARKpsmp/

vi vault.ini

1. Update the ADDRESS parameter value to the address of your vault server (e.g. 10.0.10.1). Use the arrow keys to move the cursor to the text you want to amend, type the character 'i' on your keyboard to insert text and make the necessary changes. Press Esc to stop editing.

Note: For help with VI editor commands, search the internet for "VI Editor Cheat Sheet"

```
VAULT = "Demo Vault"
ADDRESS=10.0.10.1
PORT=1858

#-----------------------------------
# Additional parameters (optional)
#-----------------------------------
```

vi

1. Enter the command :wq! to save the file and quit vi.
2. Create a credential file for the built-in Administrator. The built-in Administrator user will authenticate to the Vault and create the Vault environment during installation.
   a. Enter the following command to assign read, write and execute permissions to the file CreateCredFile.

chmod 755 CreateCredFile

```
[root@localhost CARKpsmp]# chmod 755 CreateCredFile
[root@localhost CARKpsmp]# ls -la
total 289964
drwxr-xr-x. 5 root root      4096 Dec  8 16:14 .
drwxr-xr-x. 3 root root        22 Oct 27 14:22 ..
-rw-r--r--. 1 root root  42684104 Mar 14  2022 accountuploader
-rw-r--r--. 1 root root 148385604 Mar 14  2022 CARKpsmp-12.02.5.19.x86_64.rpm
-rwxr-xr-x. 1 root root  41208496 Mar 14  2022 CreateCredFile
-rw-r--r--. 1 root root     31110 Mar 14  2022 EULA
-rw-r--r--. 1 root root  26211808 Mar 14  2022 icudt58l.dat
-rw-r--r--. 1 root root     28451 Mar 14  2022 install_cyberark_sshd.sh
drwxr-xr-x. 2 root root        50 Dec  8 16:14 IntegratedMode
drwxr-xr-x. 2 root root        64 Dec  8 16:14 META-INF
drwxr-xr-x. 3 root root        61 Dec  8 16:14 Pre-Requisites
-rw-r--r--. 1 root root      3793 Mar 14  2022 psmpparms.sample
-rw-r--r--. 1 root root       971 Mar 14  2022 RPM-GPG-KEY-CyberArk
-rw-r--r--. 1 root root  38347896 Mar 14  2022 sshd
-rw-r--r--. 1 root root      1935 Mar 14  2022 vault.ini
[root@localhost CARKpsmp]#
```

   a. Run the CreateCredfile utility as shown. Enter Administrator as the Vault Username and Cyberark1 as the Vault Password.
   b. Type “Yes” at Restrict to Entropy File option. Accept the defaults for all other options.

./CreateCredFile user.cred

```
[root@localhost CARKpsmp]# ./CreateCredFile user.cred
Vault Username [mandatory] ==> administrator
Vault Password (will be encrypted in secret file) ==>
Disable wait for DR synchronization before allowing password change (yes/no) [No] ==>
External Authentication Facility (LDAP/Radius/None) [None] ==>
Run the utility in unsecure mode (yes/no) [No] ==>
Restrict to Application Type [optional] ==>
Restrict to Executable Path [optional] ==>
Restrict to OS User name [optional] ==>
Restrict to current machine IP (yes/no) [No] ==>
Restrict to current machine hostname (yes/no) [No] ==>
Restrict to Machine GUID (yes/no) [No] ==>
Restrict to Disk Signatures (yes/no) [No] ==>
Restrict to Entropy File (yes/no) [No] ==> yes
Use HSM protection (yes/no) [No] ==>
Display Restrictions in output file (yes/no) [No] ==> yes
Path of Token dll [optional] ==>
Pin code required by the Token device ==>
Initialize the Token (yes/no) [No] ==>
Command ended successfully
[root@localhost CARKpsmp]# _
```

1. Edit the psmpparms file to define the installation directory and accept the End User License Agreement. Remain in the current directory, /opt/CARKpsmp.

a. Move psmpparms.sample to the /var/tmp directory and rename it to psmpparms using the command in the following example.

mv psmpparms.sample /var/tmp/psmpparms

```
[root@host-1 CARKpsmp]# mv psmpparms.sample /var/tmp/psmpparms
[root@host-1 CARKpsmp]# _
```

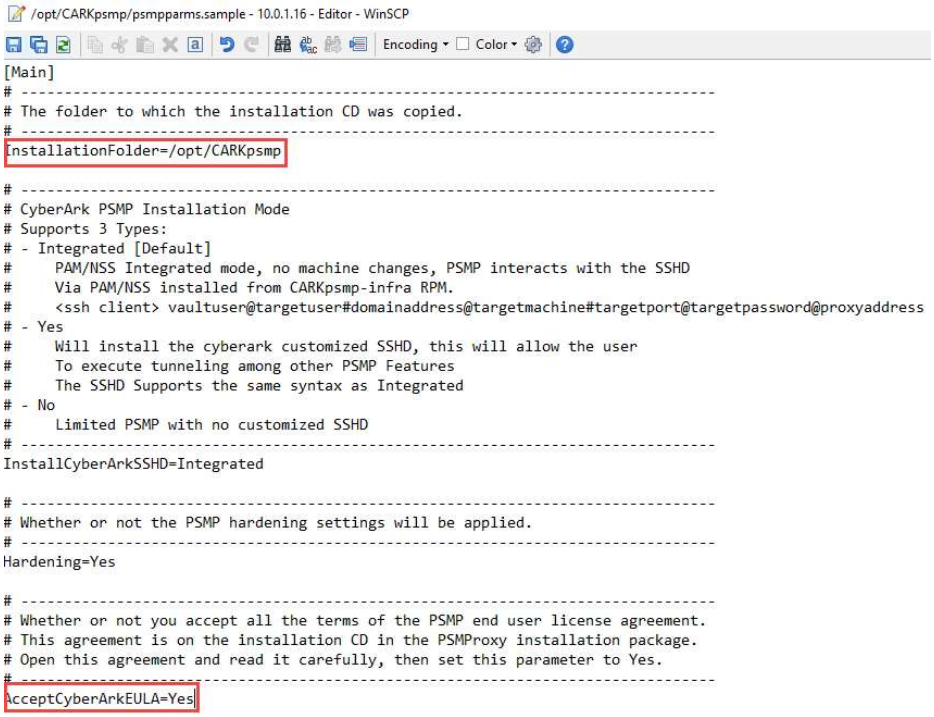
a. Edit the psmpparms file by entering the following command.

vi /var/tmp/psmpparms

a. Edit the following lines as shown.

InstallationFolder=/opt/CARKpsmp

AcceptCyberArkEULA=Yes



1. Use the arrow keys to move the cursor to the text you want to amend, type *R (case-sensitive) to make the changes and press Esc to stop editing. Enter the command :wq! to save the file and quit vi.

Objective: Install the PSM for SSH Infrastructure package, an important pre-requisite to running the PSM for SSH installation.

Note: The version number in the example command below may not be identical. At the command line type the first characters of the filename (case sensitive) and press tab to auto-complete.

1. Launch the PSMP Infrastructure package by running the following commands as shown.

cd /opt/CARKpsmp/IntegratedMode

rpm -ivh CARKpsmp-infra-12.02.5.19.x86_64.rpm

Objective: Install the PSM for SSH installation RPM package.

Note: The version number in the example command below may not be identical. At the command line type the first characters of the filename (case sensitive) and press tab to auto-complete.

1. Change directory back to /opt/CARKpsmp/ and launch the PSMP installation by running the following command.

rpm -ivh CARKpsmp-12.02.5.19.x86_64.rpm

```
[root@host-1 CARKpsmp]# rpm -ivh CARKpsmp-12.01.0.4.x86_64.rpm
warning: CARKpsmp-12.01.0.4.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID 08beaa44: NOKEY
Preparing...                          ################################# [100%]
Installation process is starting...
CARKpsmp-infra package version was verified
Updating / installing...
   1:CARKpsmp-12.01.0-4               ################################# [100%]
Starting PSM SSH Proxy...
PSM SSH Proxy was started successfully.
Starting PSMP ADBridge...
PSMP ADBridge was started successfully.
Service [sshd] is about to be restarted...
Service [sshd] was restarted successfully.
Unloading SELinux policy...
Loading SELinux policy...
Machine hardening was completed successfully.
Installation process was completed successfully.
```

1. When complete, run the following command to ensure that the services are running.

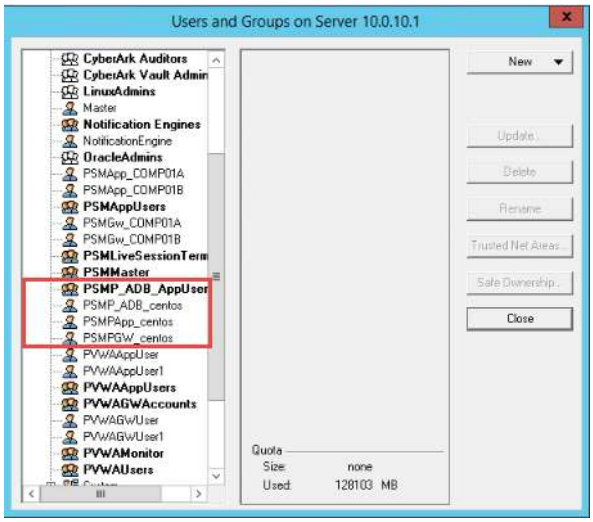
service psmpsrv status

1. Review the log using the cat command as shown.

cat /var/tmp/psmp_install.log

```
Wed Mar 2 11:33:47 EST 2016 | Updating [sshd]...
Wed Mar 2 11:33:47 EST 2016 | Configuring the [sshd_config] file...
Wed Mar 2 11:33:47 EST 2016 | Configuring [sshd_config] file has finished.
Wed Mar 2 11:33:47 EST 2016 | Configuring the [sshd] service initialization script...
Wed Mar 2 11:33:47 EST 2016 | Configuring the [sshd] service initialization script has finished.
Wed Mar 2 11:33:47 EST 2016 | Replacing the [sshd] executable...
Wed Mar 2 11:33:47 EST 2016 | Starting the [sshd] executable...
Wed Mar 2 11:33:48 EST 2016 | The [sshd] executable was started successfully.
Wed Mar 2 11:33:48 EST 2016 | Replacing the [sshd] executable has finished.
Wed Mar 2 11:33:48 EST 2016 | Updating [sshd] has finished.
Wed Mar 2 11:33:48 EST 2016 | Script execution has finished.
Wed Mar 2 11:33:48 EST 2016 | Installation process was completed successfully.
```

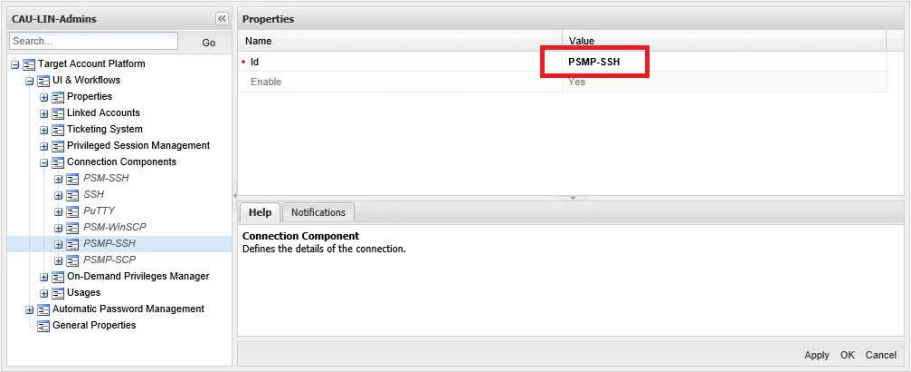
1. Check that the PSMPApp_<*hostname*> users and groups were added to the Vault.



Note: If a Platform managing the *root01* account was duplicated prior to installing PSMP you will need to manually create the link to the *Connection Component*.

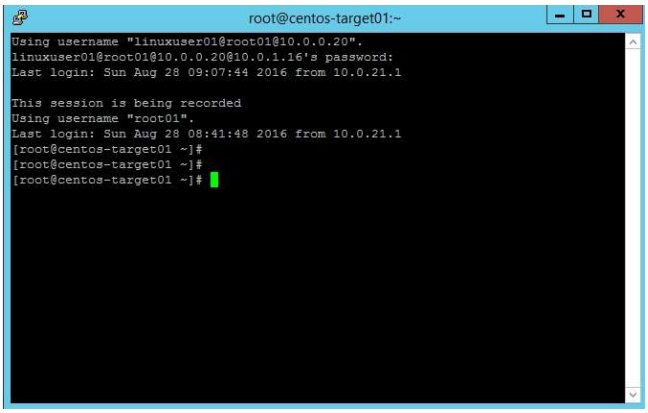
1. Sign in to the PVWA (VaultAdmin01/ldap) from COMP01A/B and add the PSMP-SSH and PSMP-SCP Connection Components to target platform “ACME Unix via SSH Accounts” by right clicking on folder “Connection Components” and choosing “Add Connection Component”.
2. Ensure that the PSM for SSH server updates the policy change in step 14, by restarting the services. Run “service psmpsrv restart” on the PSM for SSH server.

3. From **Comp01A/B** server open PuTTY from the desktop shortcut and enter the following connection string in *Host Name*to verify that you can you log in with linuxadmin01 to the Linux Server CentOS-Target(centos.acme.corp) using root01 via the PSMP:
    a. **linuxadmin01@root01@centos.acme.corp @10.0.1.16** (mailto:linuxadmin01@root01@centos.acme.corp%20@10.0.1.16)**.**



Note: Ensure that the Users Directory Map authentication requirement has been reset to LDAP, then delete any CyberArk Users from the PrivateArk Client.

a. Enter the password “Cyberark1”
b. You may need to issue the “service psmpsrv restart” command on the PSMP server, after editing your platform, to refresh the platform changes**.**



1. Terminate the session.
2. Confirm the recording of your session in the PVWA.
    a. Login to the PVWA as Auditor01 using LDAP authentication. Navigate to Monitoring, and play the session recording for linuxadmin01 using client PSMP-SSH.

Troubleshooting

1. If the installation fails, you can view errors in the following logs:
    a. /var/tmp/psmp_install.log – This log file describes the activities that occurred during the installation process.
    b. /var/opt/CARKpsmp/temp/EnvManager.log – This log file describes the activities that occurred when the Vault environment for PSMP was created.
2. View the logs with the less command to view the logs and browse the pages using the space button.
3. Run the rpm with the -e switch to remove the existing PSMP package and install again.

```
[root@centos PSM-SSHProxy-Installation]#
[root@centos PSM-SSHProxy-Installation]# less /var/tmp/psmp_install.log _
```

rpm –e CARKpsmp

1. If the installation completes successfully, but you cannot connect successfully via the PSMP, check the following logfile:

cat /var/opt/CARKpsmp/logs/PSMPConsole.log

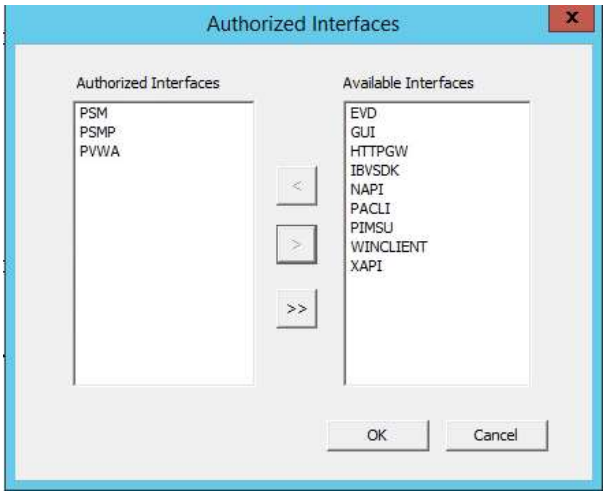
Securing CyberArk

Objective: In this section you will be asked to perform several tasks to make your existing CyberArk implementation secure. Perform these operations on either Comp01A or Comp01B servers. The following procedure will restrict an LDAP User from authenticating via any other interface except the PVWA and PSM.

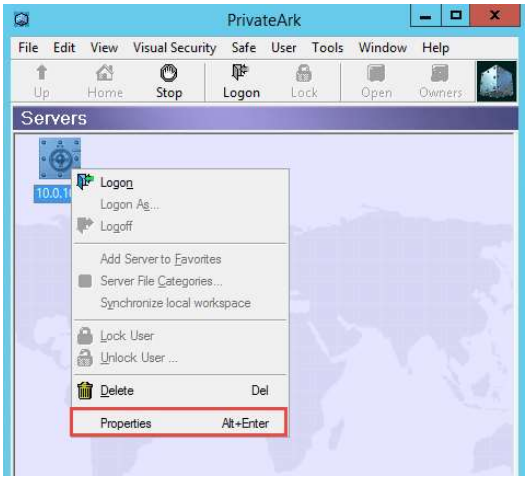
Lock Down a User's Interface

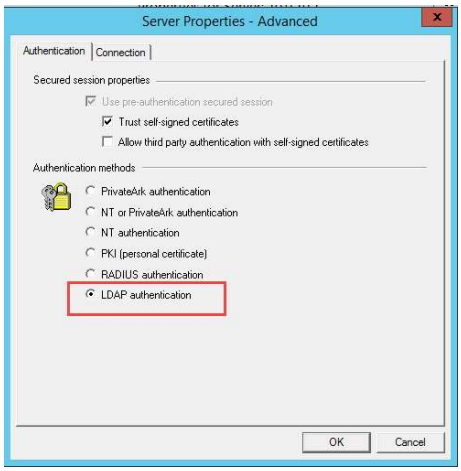
Note: Ensure that all Virtual Machines(VM's) are started in your Skytap lab before proceeding (with the exception of the DR VM).

1. Log in to the PrivateArk Client as administrator.
2. Open Tools, Administrative Tools, Directory Mapping.
3. Select Map Name Users_acme.corp > Update > User Template > General > Authorized Interfaces.
4. Using the arrows in the center, select and move all entries listed under the "Authorized Interfaces" column except **PSM, PSMP** and PVWA, to Available Interfaces.



1. Select Ok, Ok again and OK a final time, then close the Directory Mapping utility and logoff the PrivateArk Client.
2. Now logged off, select the defined Vault in the PrivateArk Client. Right click and select Properties > Advanced > Authentication > Authentication Methods > LDAP authentication.





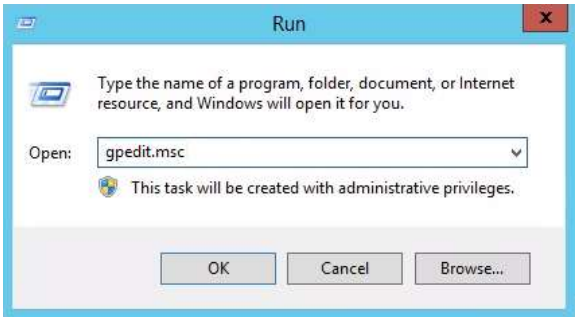
1. Select OK and Ok again, then double click the Vault Server icon to login to the Vault.
    a. Attempt to logon as Winadmin02, Linuxadmin02 or any other LDAP user that has never signed in to the PVWA so they are filtered by the Users Directory Mapping.
    b. The WINCLIENT provides authorization to login to the PrivateArk Client, and so the expected result is the attempt should fail with an ITATS004E Authentication failure popup.
    c. Check the ITALOG.LOG on the Vault server for “ITATS942E Client WINCLIENT is not allowed for user…”.
2. Attempt to sign in to the PVWA with the same LDAP user, and attempt to launch a PSM connection component. Expected result = success!

Use RDP over SSL

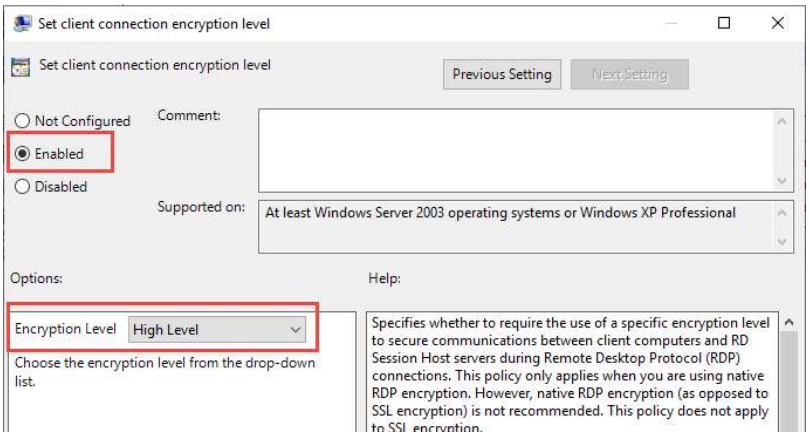
NOTE: In this section you will configure the PSM server to require RDP connections over SSL.

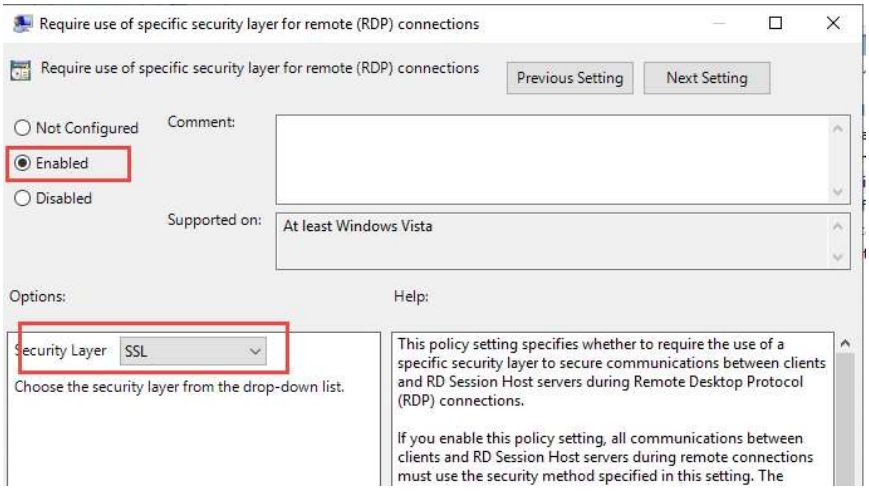
Connections to the **PSM** require a certificate on the **PSM** machine. By default, Windows generates a self-signed certificate. In a production implementation a trusted certificate issued by a Certificate Authority should be obtained.

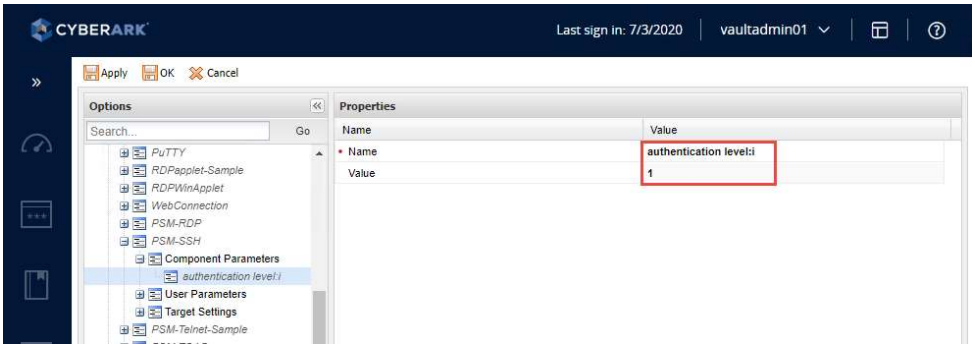
1. Sign in to comp01C as Admin02 and run GPEDIT.MSC.
2. Navigate to Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security.
3. Open the Security settings for: Set client connection encryption level. Click on Enabled and set the encryption level to High Level then click OK.
4. Open the setting for: Require use of specific security layer for remote (RDP) connections. Click on Enabled and set the Security Layer to SSL and click OK.
5. Exit GPEDIT.MSC.
6. Repeat steps 1-5 above on the 2nd PSM server in the Load Balanced pool of PSM servers, Comp01d.
7. In the PVWA, navigate to ADMINISTRATION > Configuration Options > Options > Connection Components > PSM-SSH > Component Parameters.
    a. Add a new parameter named authentication level:i and set the Value to 1.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
gpedit.msc
This task will be created with administrative privileges.
OK
Cancel
Browse...

Local Group Policy Editor
File Action View Help
Biometrics
BitLocker Drive Encryption
Credential User Interface
Desktop Gadgets
Desktop Window Manager
Device and Driver Compatibility
Digital Locker
Edge UI
Event Forwarding
Event Log Service
Event Viewer
Security
Set client connection encryption level
Edit policy setting
Requirements:
At least Windows Server 2003 operating systems or Windows XP Professional
Description:
Setting
State
Server authentication certificate template
Set client connection encryption level
Always prompt for password upon connection
Require secure RPC communication
Require use of specific security layer for remote (RDP) conn...
Do not allow local administrators to customize permissions
Require user authentication for remote connections by usin...
Not configured

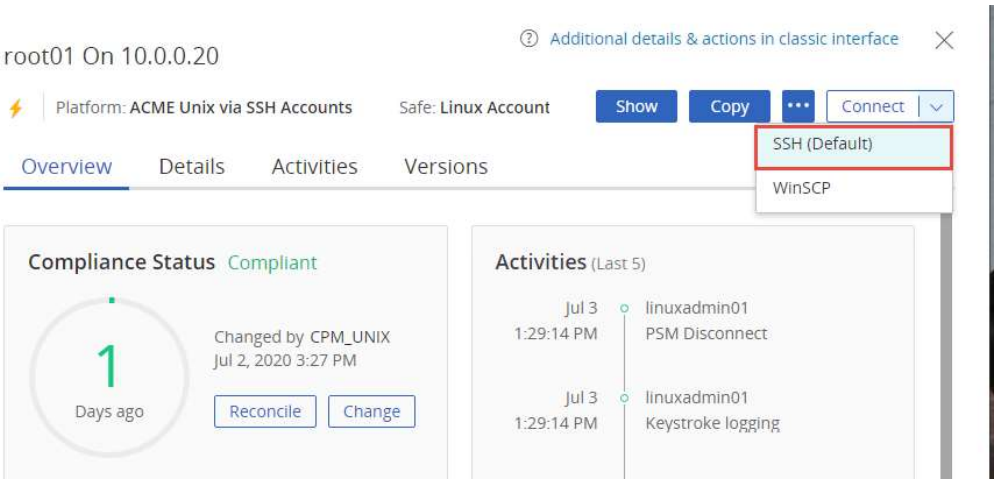

Set client connection encryption level
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Server 2003 operating systems or Windows XP Professional
Options:
Help:
Encryption Level
High Level
Choose the encryption level from the drop-down list.
Specifies whether to require the use of a specific encryption level to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. This policy only applies when you are using native RDP encryption. However, native RDP encryption (as opposed to SSL encryption) is not recommended. This policy does not apply


Require use of specific security layer for remote (RDP) connections
Previous Setting
Next Setting
Not Configured
Enabled
Disabled
Comment:
Supported on:
At least Windows Vista
Options:
Help:
Security Layer
SSL
Choose the security layer from the drop-down list.
This policy setting specifies whether to require the use of a specific security layer to secure communications between clients and RD Session Host servers during Remote Desktop Protocol (RDP) connections.
If you enable this policy setting, all communications between clients and RD Session Host servers during remote connections must use the security method specified in this setting. The


CYBERARK
Last sign in: 7/3/2020
vaultadmin01
Apply
OK
Cancel
Options
Search...
Go
PuTTY
RDPapplet-Sample
RDPWinApplet
WebConnection
PSM-RDP
PSM-SSH
Component Parameters
authentication level:i
User Parameters
Target Settings
PSM-Telnet-Sample
Properties
Name
Value
Name
authentication level:i
Value
1

Note: Repeat this procedure for each connection component the customer intends to use, (excluding PSMP Connection Components) to enable RDP over SSL connections to the **PSM** machine.

1. Restart the PSM service on COMP01C and COMP01D servers to refresh the configuration changes or wait the default 20 minutes refresh cycle.
2. Establish a PSM-SSH connection using account root01.



Note: If the RDS Certificate was updated during the “Load Balanced PSM Servers” section you will not receive a certificate error. If an error occurs, revisit “Update RDS Certificate” on page 94.

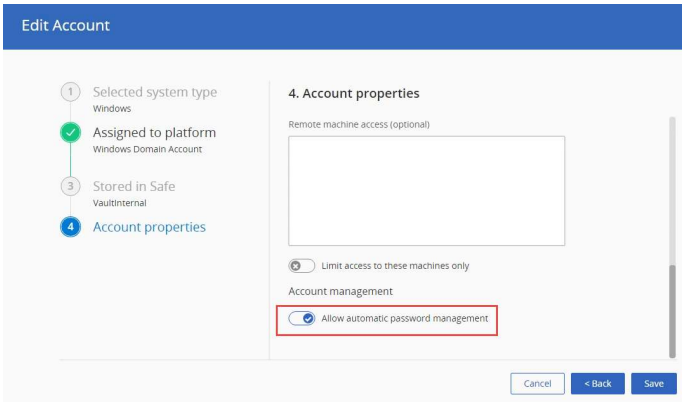
Manage LDAP BindAccount

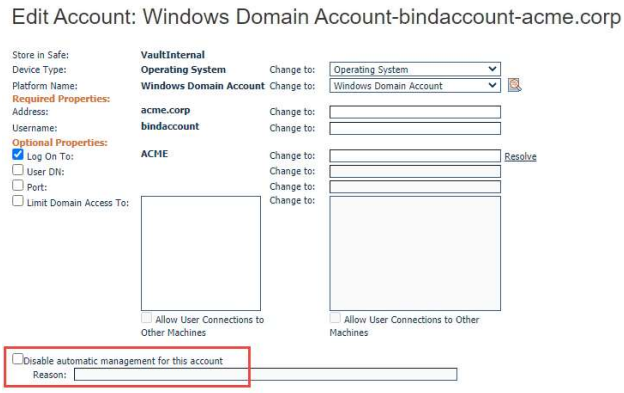
Objective: Configure the system to allow the CPM to automatically manage the LDAP BindAccount.

We recommend configuring BindAccount password changes to take place “off hours”, to minimize or eliminate the risk of a service outage during password changes. This can be accomplished by configuring the “From hour, To hour” platform settings appropriately.

1. Logon to the PVWA as Vaultadmin01.
2. Edit the VaultInternal safe and assign CPM: CPM_WIN and Save.
3. Duplicate the Windows Domain Account platform. Name the new platform “ACME Windows Domain SERVICE Accounts”
4. Edit the new “ACME Windows Domain SERVICE Account” platform.
   a. Go to Automatic Password Management > Password Change.
      - Update FromHour parameter to a value of 1 and ToHour parameter to a value of 7
      - Update ExecutionDays = Mon,Tue,Wed
      - Update PerformPeriodicChange = Yes
   b. Go to Automatic Password Management > Password Verification.
      - Update FromHour parameter to a value of 1 and ToHour parameter to a value of 7
      - Update VFExecutionDays = Mon,Tue,Wed
      - Update VFPerformPeriodicVerification = Yes
   c. Go to Automatic Password Management > Password Reconciliation.
      - Update FromHour parameter to a value of 1 and ToHour parameter to a value of 7
      - Update RCExecutionDays = Mon,Tue,Wed
      - Update RCAutomaticReconcileWhenUnsynched = Yes
5. Go to Accounts and search for BindAccount
6. Edit BindAccount.

a. Assign the new platform created in step 3
b. Username field must not include the address i.e., should be 'BindAccount' not 'BindAccount@acme.corp'
c. Update the Address field to the domain name only i.e, "acme.corp"
d. Select the optional property 'Logon To:' and select resolve, to populate the NetBIOS domain name
e. Enable "Allow automatic password management" in v10ui or deselect the option "Disable automatic management for this account" in v9ui.

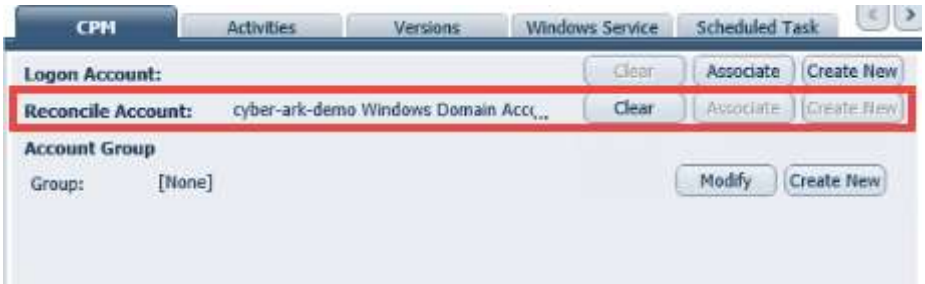




a. Save the changes

1. In Account Details, associate a Reconcile Account by selecting Associate and choosing the Admin01 domain account

Note: A reconcile account can also be associated at the platform level. All accounts assigned to the platform with reconcile account configured will automatically be associated.



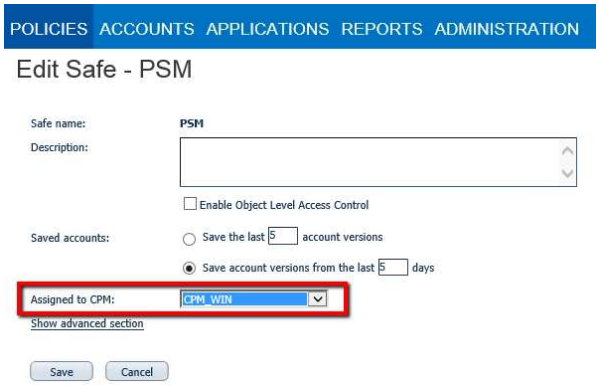
1. Select the Change button to change the password of BindAccount@acme.corp

Manage PSMConnect/PSMAdminConnect using the CPM

Objective: Configure CyberArk to automatically manage accounts *PSMConnect* and *PSMAdminConnect* with the **CPM.**

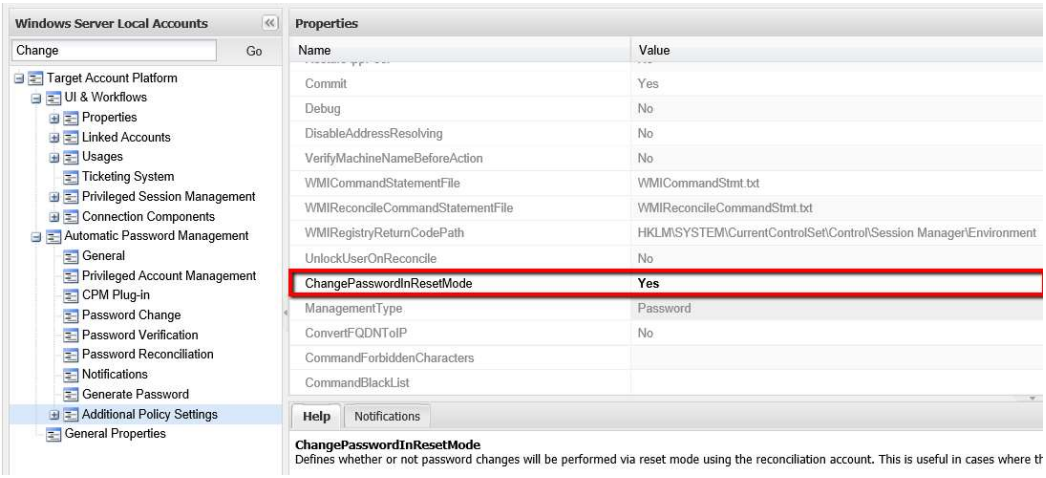
Grant permissions to a CPM on the PSM safe.

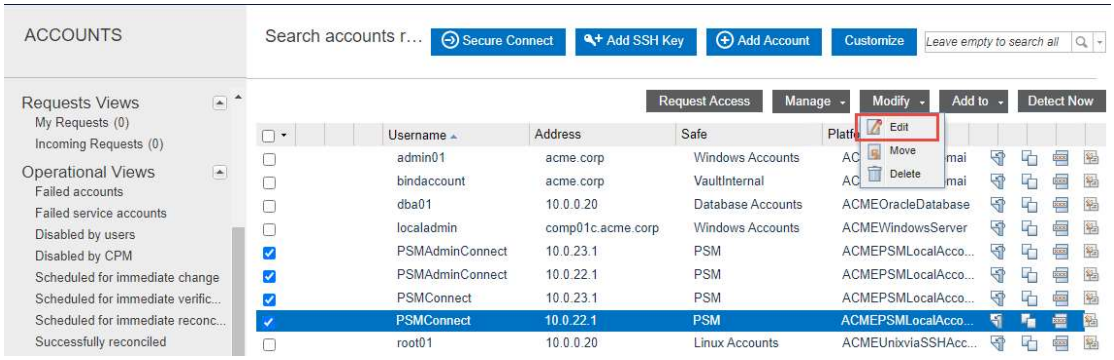
1. Login to the PVWA as CyberArk as Administrator and go to POLICIES > Access Control (Safes) and choose the PSM safe. Click on Edit.
2. Assign to CPM: CPM_WIN.
3. Select Save, then select the PSM safe again and choose Members.
4. Choose Add Member. Query the Vault for the 'Vault Admins' group, Assign all roles. Assigning the built-in 'Vault Admins' group will now allow the VaultAdmin01 user to see the PSM accounts in the PSM safe.
    a. Sign out of the PVWA as Administrator. Sign in as VaultAdmin01.

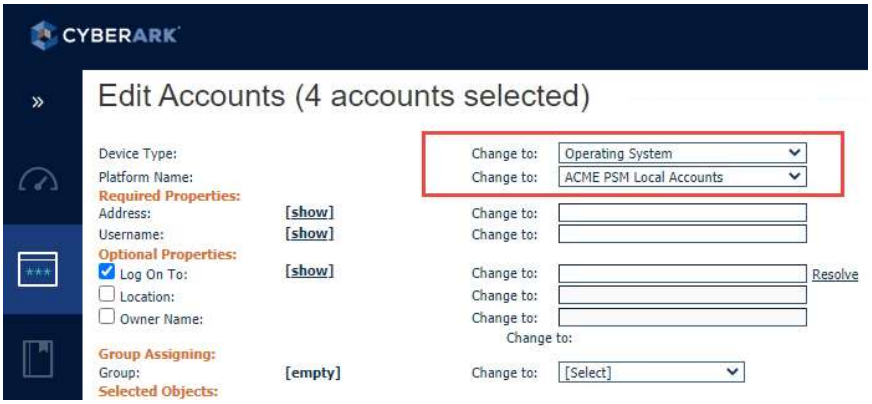


Objective: Duplicate platform **Windows Local Server Accounts** and assign the PSM accounts. Configure the platform to reconcile as the default method of rotating the password.

1. Go to platform management and create a duplicate of Windows Server Local Accounts platform. Suggested name is “ACME PSM Local Accounts”.
2. Edit platform “ACME PSM Local Accounts”.
   a. Go to Automatic Password Management > Password Change.
      - Update FromHour parameter to a value of 1 and ToHour parameter to a value of 7
      - Update ExecutionDays = Mon,Tue,Wed
      - Update PerformPeriodicChange = Yes
   b. Go to Automatic Password Management > Password Verification.
      - Update FromHour parameter to a value of 1 and ToHour parameter to a value of 7
      - Update VFExecutionDays = Mon,Tue,Wed
      - Update VFPerformPeriodicVerification = Yes
   c. Go to Automatic Password Management > Password Reconciliation.
      - Update FromHour parameter to a value of 1 and ToHour parameter to a value of 7
      - Update RCExecutionDays = Mon,Tue,Wed
      - Update RCAutomaticReconcileWhenUnsynched = Yes
3. Right click on Automatic Password Management and select “Add Additional Policy Settings”.
4. Select “Additional Policy Settings” and update ChangePasswordInResetMode to Yes. Click on OK to save.
5. Go to ACCOUNTS in the classic UI. Search on and select all PSMConnect and both PSMAdminConnect users.
   a. Select the Modify button and click on Edit.
6. Change Device Type to Operating System and Platform Name to “ACME PSM Local Accounts” and select Save.







Associate a Reconcile Account

Note: A Reconcile Account can be associated at the platform level or at the account level. If associated at the platform all accounts assigned to the platform will be automatically associated with the Reconcile Account. Another option is to associate a Reconcile Account for each **PSMConnect** and **PSMAdminConnect** user individually by selecting Associate and choosing the **Admin01 domain account** in Account Details.

1. Using the Accounts View search for and select the Admin01 account.
    a. Copy the Account name and Safe name property values. Save these values in Notepad for future use.
2. Edit platform “ACME PSM Local Accounts”.
    a. Go to Automatic Password Management > Password Reconciliation.
    b. Update ReconcileAccountSafe parameter value with the Safe name recorded in step 1 above.
    c. Update ReconcileAccountName parameter value with the Account name recorded in step 1 above.

Tip: Leave no trailing or leading spaces when editing a platform. Always assume case sensitivity.

a. Click Apply and OK to save your changes.

1. Select each PSMConnect and PSMAdminConnect accounts in the Accounts View in classic interface.
    a. Note that a reconciliation account is now associated but cannot be cleared.
    b. Perform a password change operation. After a few minutes, note the “Last modified” parameter value.

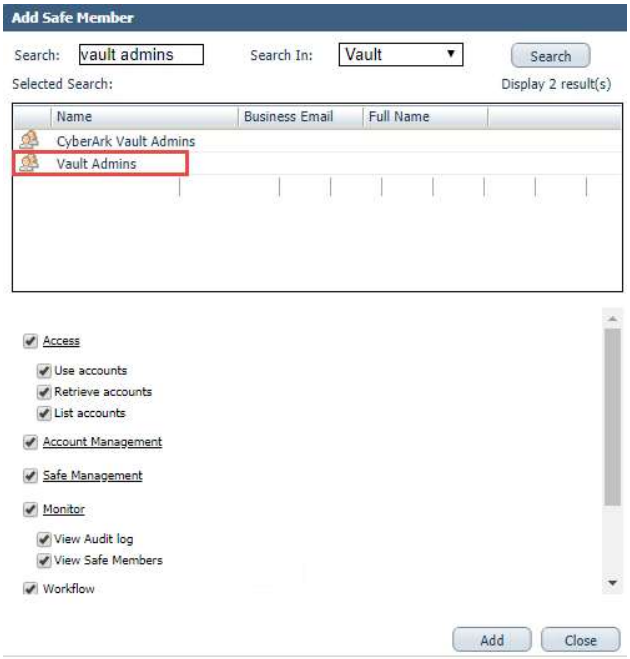
-

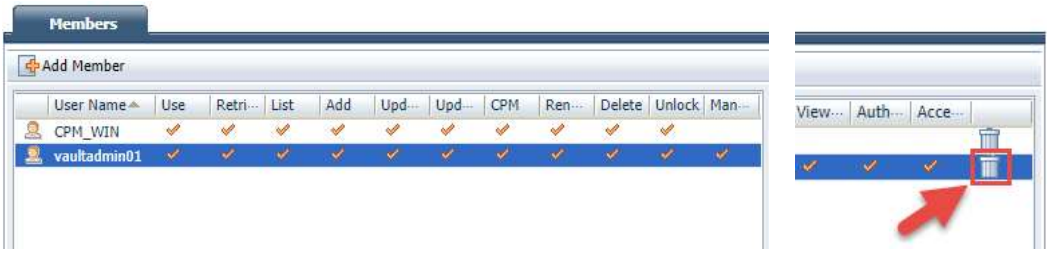
Manage CyberArk Administrator Account using the CPM

Objective: Configure the CPM to manage the password for the built-in CyberArk Administrator user.

NOTE: After this step Vault administrators will need to retrieve the password of the *Administrator* account from the Vault or when using a PSM Connection Component.

1. Login to the PVWA as vaultadmin01 and change the CyberArk Vault platform to Active.
2. Create a new safe.
   a. Safe name = CyberArk Administrators
   b. Assigned CPM = CPM_WIN
   c. Add Safe Member = Vault Admins from Vault. Grant all roles (Access, Account Management, Safe Management, Monitor, Workflow, Advanced).
3. Delete the Vaultadmin01 user. Scroll to the right, and click on the trash can.





1. Create a new account in the PVWA for Administrator with the following properties.

Store in Safe	**CyberArk Administrators**
System(Device) Type	**Application**
Platform	**CyberArk Vault**
Username	**Administrator**
Address	**10.0.10.1**

Password	**Cyberark1**

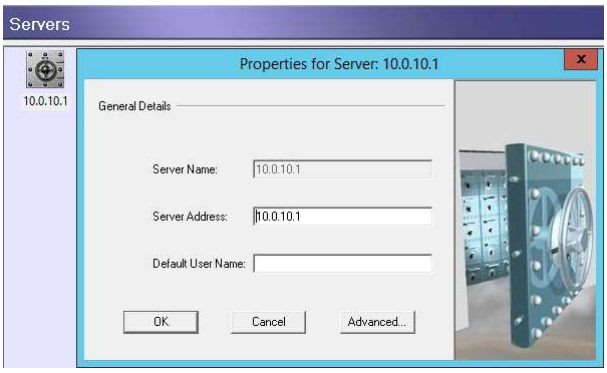
1. Execute a password change operation for Administrator.

Connect with PSM-PrivateArk Client

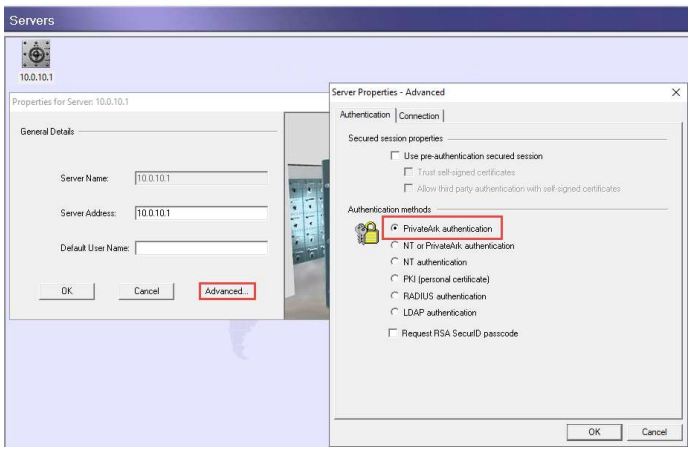
Objective: Configure the PSM to support the PSM-PrivateArk Client Connection Component.

The PrivateArk Client must be installed on the PSM server, as instructed during the PSM Installation section of this guide. The PrivateArk Client must also be configured in *Global Configuration* mode, which enables you to define Vault definitions that will be available to users of the PSM-PrivateArk Client Connection Component.

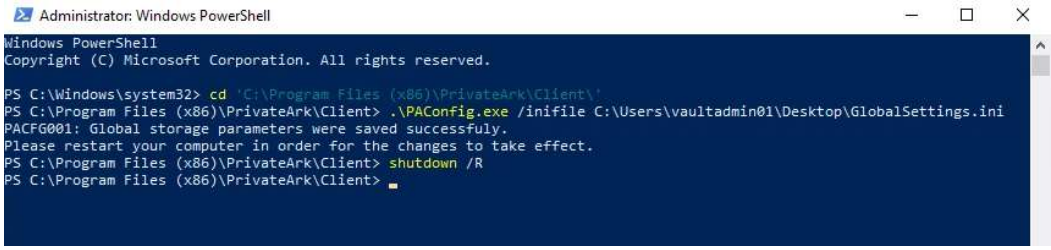
1. Sign in to the PSM server Comp01C as Admin02 and run the PrivateArk Client from the desktop. Do not login to the Vault.
2. Ensure that at least one vault server is defined, as shown in the graphic. If not, select the File, New, Server menu option and define a new vault using 10.0.10.1 for the Name, and Address fields.



1. Ensure that Authentication method = PrivateArk authentication
2. Go to Tools > Administrative Tools > Export Configuration Data.
3. Browse to your Desktop folder and select “Export Global Configuration Data” and click OK. Close the PrivateArk Client.
4. Rename the file to GlobalSettings.ini.
5. Right click on GlobalSettings.ini file and choose Properties > Security tab. Select “Edit…, Add…” and assign default (RX) permissions for the local Comp01C\PSMShadowUsers group.
6. Use the PAConfig.exe utility to change the configuration to Global Configuration. Open Windows Powershell (Admin) in folder “C:\Program Files (x86)\PrivateArk\Client” and run the following command:



PAConfig.exe /inifile c:\Users\Admin02\Desktop\GlobalSettings.ini

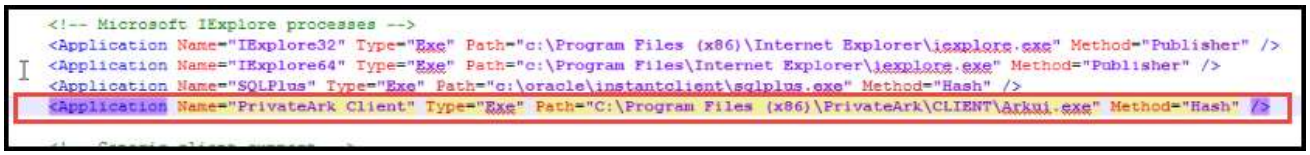


1. Restart the server.
2. Sign in to the PSM server Comp01C as Admin02 and add the Private Ark client executable as an authorized application in the Applocker configuration.
   a. Using File Explorer navigate to c:\Program Files (x86)\CyberArk\PSM\Hardening.

Note: PSM Hardening hides local drives to users. In the address bar, type “c:\” to display the local drive.

a. Edit the file PSMConfigureApplocker.xml using Notepad++.
b. Find the “Generic Client support” section at the bottom. Copy the “Generic client sample” line. Paste this line anywhere without comments (<!-- , -->).
c. Update the new line as show below.

<Application Name=”PrivateArk Client” Type=”Exe” Path="C:\Program Files (x86)\PrivateArk\Client\Arkui.exe” Method=”Hash” />



1. Save the file.

Objective: Apply the Applocker rules by executing the PSMConfigureApplocker.ps1 script.

1. Execute the following 3 commands.

Get-ExecutionPolicy *(Result should be “Restricted”)*

Set-ExecutionPolicy Bypass -Scope Process

.\psmconfigureapplocker.ps1

Note: For more information on Applocker, refer to “**Run AppLocker Rules** (https://docs.cyberark.com/Product-Doc/OnlineHelp/PAS/Latest/en/Content/PAS%20INST/Install_PSM_harden.htm?

Highlight=applocker#RunAppLockerrules)" online at Docs.cyberark.com.

Repeat "Connect with PSM-PrivateArk Client" steps 1-12 on PSM Server COMP01D.

1. Sign in to the PVWA from Comp01A or Comp01B.
    a. Enable RDP over SSL (see "Use RDP over SSL" on page 103) for the PSM-PrivateArkClient connection component.
    b. Test both members of the load balanced pool of PSM servers
    c. Update the CyberArk Vault platform to take advantage of the load balanced PSM configuration.
2. Attempt to connect to the Vault using Administrator and the PSM-PrivateArkClient connection component.

Connect using PSM-PVWA-Chrome

Objective: In this section you will configure the PSM to support connections with CyberArk administrative accounts to the Vault using the PVWA.

Note: In order for the PSM to support Web Applications, the PSM hardening scripts must be configured and executed appropriately.

In this exercise, you will enable Google Chrome on the PSM Server, and use the new PSM-PVWA-v10 Connection Component.

1. Configure Applocker to enable Google Chrome.
    a. In the "*C:\Program Files (x86)\CyberArk\PSM\Hardening*" subfolder, edit the PSMConfigureApplocker.xml using Notepad++.
    b. Find the "Google Chrome process" section near the bottom of the file and remove the comments from the section. Be certainto delete both comment lines as shown or you will break the xml file structure and experience errors when launching the PSMConfigureAppLocker.ps1 script.
        - <!- - If relevant, uncomment this part to allow Google Chrome webform based connection clients
        - End of Google Chrome process comment - - >
    c. Replace Method="Hash" with Method="Publisher", as shown.
    d. Save the file.
    e. Open PowerShell as Administrator in the folder specified in step 1 above and run the following commands.

```
<!-- Google Chrome process -->
<Application Name="GoogleChrome" Type="Exe" Path="C:\Program Files (x86)\Google\Chrome\Application\chrome.exe" Method="Publisher" />
```

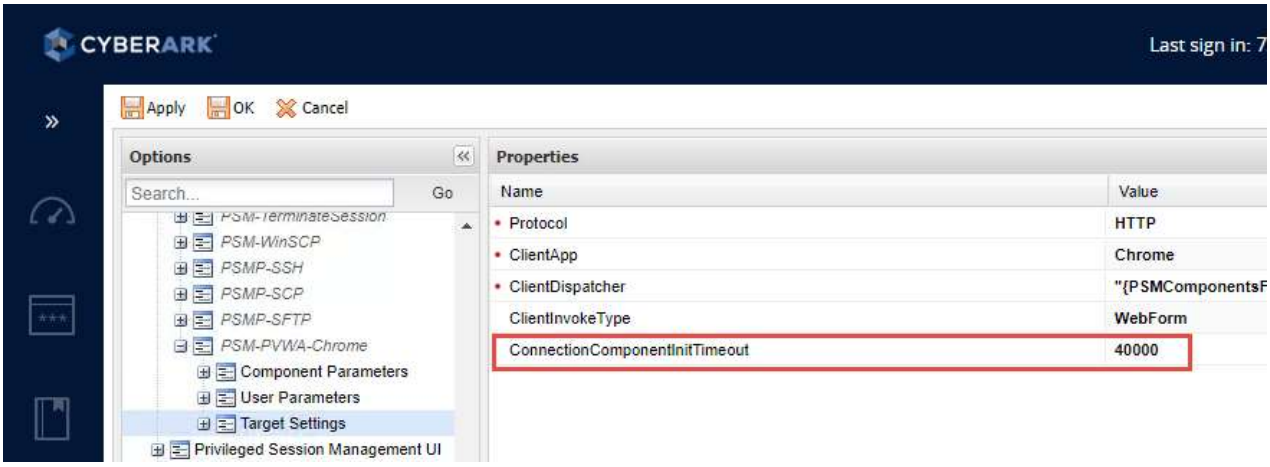
Get-ExecutionPolicy (Result should be "Restricted")

Set-ExecutionPolicy Bypass -Scope Process

.\psmconfigureapplocker.ps1

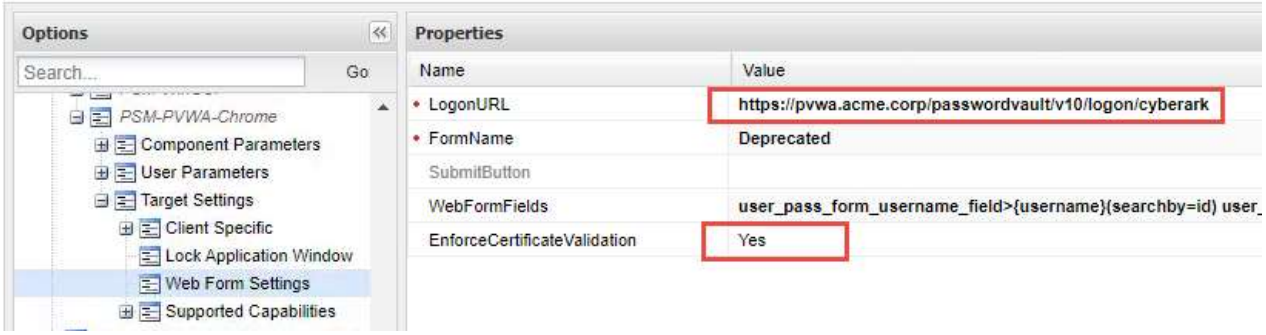
1. Sign in to the PVWA as Vaultadmin01 and navigate to Administration > Configuration Options > Options > Connection Components.
2. Copy **PSM-PVWA-v10** and paste it under Connection Components. Rename the copied component PSM-PVWA-Chrome.
3. Select the **PSM-PVWA-Chrome**connection component.
    a. Edit the Display Name parameter to **PSM-PVWA-Chrome**.
    b. Navigate to Target Settings. Update ConnectionComponentInitTimeout value to 40000.

Note: This value is effective for this Skytap lab environment. Analysis is necessary to determine the value appropriate for a production configuration.

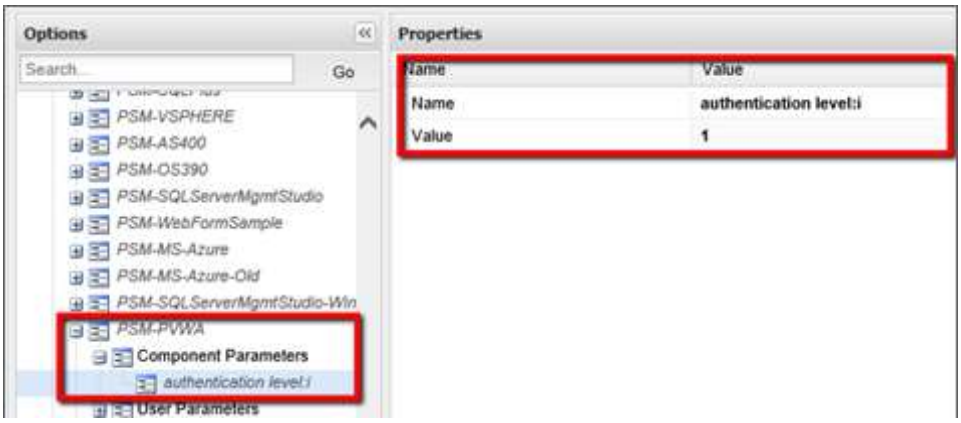


a. Navigate to Target Settings->Web Form Settings and configure:
   - LogonURL, replace "{address}" to match the fully qualified hostname of your Load Balanced PVWA server pool including the authentication method as follows: **https://pvwa.acme.corp/passwordvault/v10/logon/cyberark** (https://pvwa.acme.corp/passwordvault/v10/logon/cyberark)

Note: "EnforceCertificateValidation" = Yes by default. In this lab we have replaced the self-signed web certificate with a trusted web certificate. If signed in to the component server as an ACME.Corp domain user, no certificate errors will result.



a. Enable RDP over SSL for the **PSM-PVWA-Chrome** connection component by adding authentication level:i with a value of 1 as shown.



1. Click Apply and OK to save the changes.
2. Edit the CyberArk Vault platform. Rename **PSM-PVWA-v10**connection component to PSM-PVWA-Chrome. Click Apply to save your changes but remain editing the platform.

a. Select **"Connection Components".** Add the value PSM-PVWA-Chrome to the PSMConnectionDefault parameter. This will make it show up first in the list of Connection Components for accounts assigned to this platform.

Delete PSM-PVWA Connection Component and save the platform.

1. Restart the "Cyber-Ark Privileged Session Manager" Server service on both PSM servers to refresh their cache of policies.
2. Signed in to the PVWA as **Vaultadmin01, select the** PSM-PVWA-Chrome connection component associated with account Administrator@10.0.10.1.

Note: The PSM-PrivateArk client window may launch in full screen mode, but the PVWA will not display properly. Resize the window to view the PVWA.

1. Validate recording. Sign out of the PVWA and sign in as **Auditor01** using LDAP authentication and verify that you can view the recordings of your PrivateArk Client and PVWA sessions.

CyberArk Vault Backup

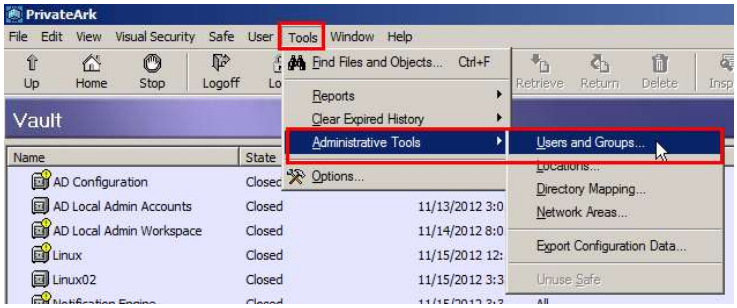
Enable the Backup and DR Users

Objective: Configure component CyberArk Replicate to backup the vault to a remote server.

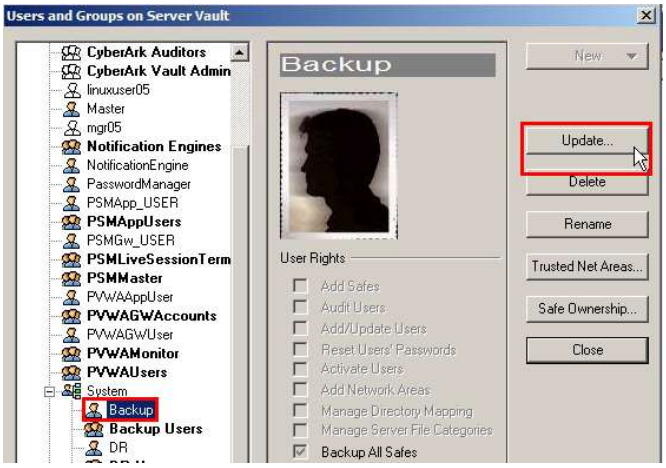
Note: Ensure that all Virtual Machines(VM's) are started in your Skytap lab before proceeding (except for the DR VM).

For this section of the exercise, you will first login to the **PrivateArk Client** on **Comp01A Server**.

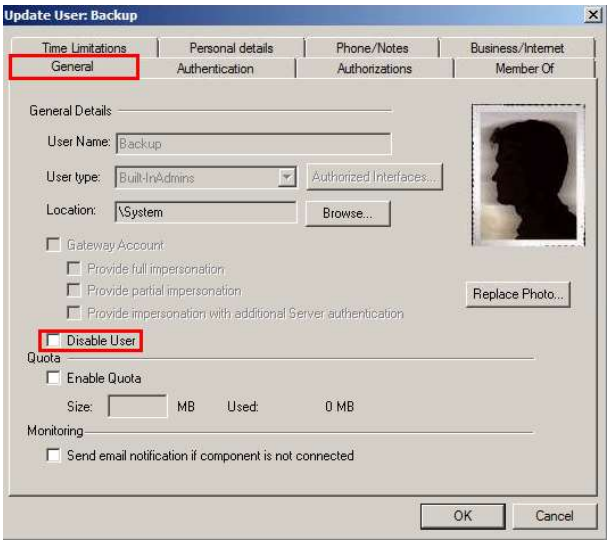
1. Use the **PrivateArk** client to log into the Vault as administrator (use the PSM-PrivateArk Client connection component).
2. Go to Tools > Administrative Tools > Users and Groups.



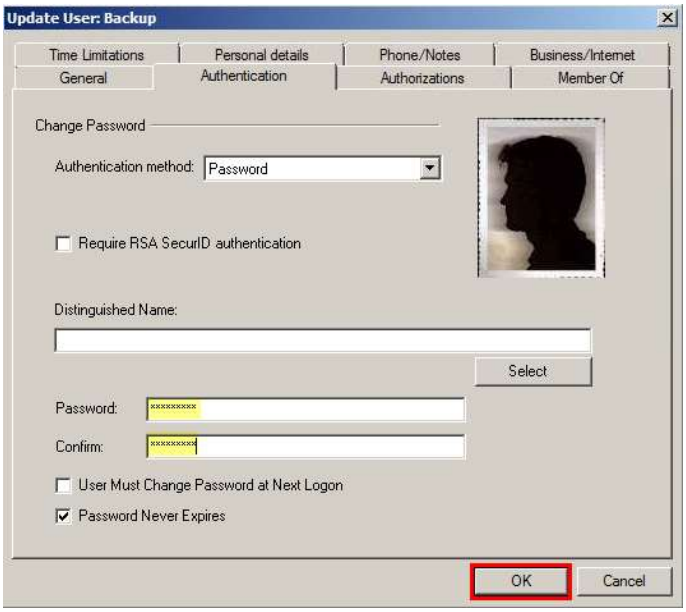
1. Highlight the Backup user (located under System) and press Update.



1. On the General tab deselect the Disable User checkbox.

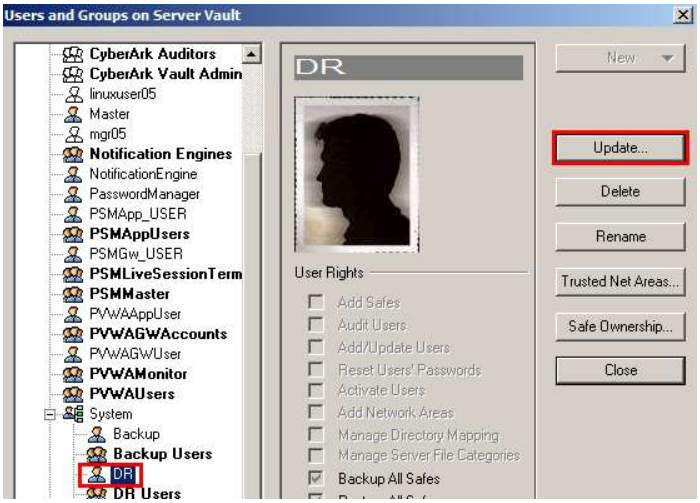


1. On the Authentication tab enter Cyberark1 in the Password and Confirm fields.
2. Press OK.

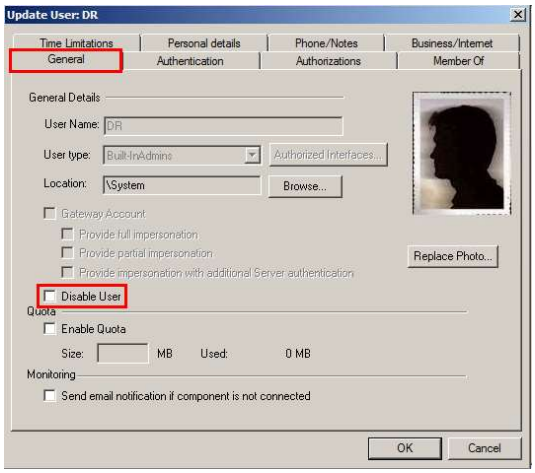


Note: The DR user will be used in the coming Disaster Recovery exercise. As such we will enable it now.

1. Highlight the DR user (located under System) and press Update.



1. On the General tab uncheck the Disable User checkbox.



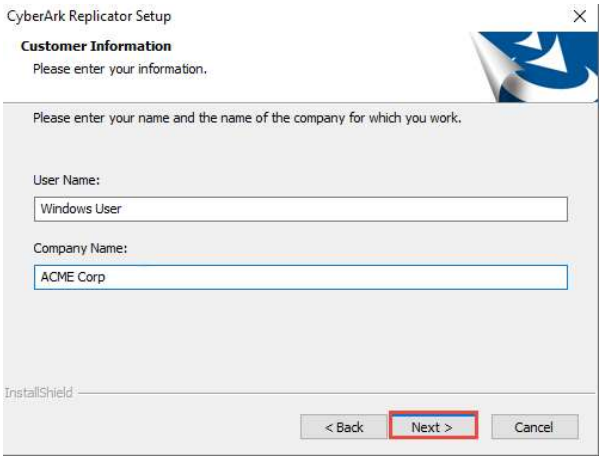
1. On the Authentication tab enter Cyberark1 in the Password and Confirm fields. Click OK then Logoff the PrivateArk Client.

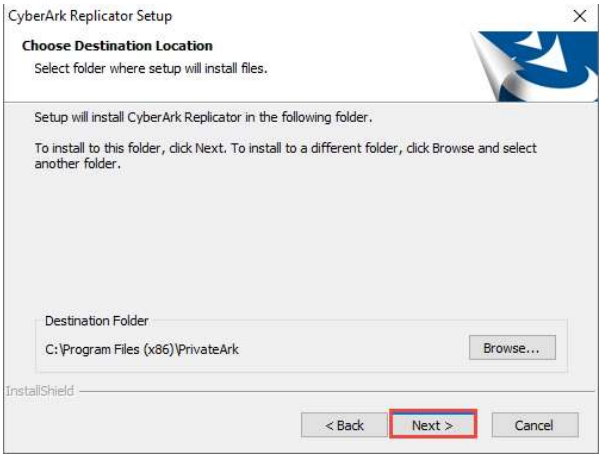
-

Install the PrivateArk Replicator Component

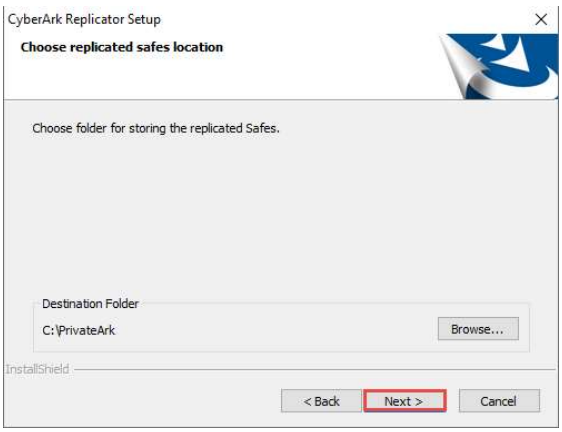
1. Sign in to the **Comp01A** Server, open Windows File Explorer and navigate to the shared resource folder, “Z:\. If the Z: drive is not mapped, map Z: to \\dc01\shared.
2. Navigate to “Z:\CyberArk PAM Solution\v12.6\”. Copy the file ‘Replicate-Rls- v12.6.zip’ to “C:\CYBR_Files” and extract all files.
3. Navigate to extracted folder “‘C:\CYBR_Files\ Replicate-Rls-v12.6”, and right click and “Run As Administrator” setup.exe.
4. Accept all the default parameters to complete the installation. On the Welcome screen enter Next and click Yes to accept the license agreement.

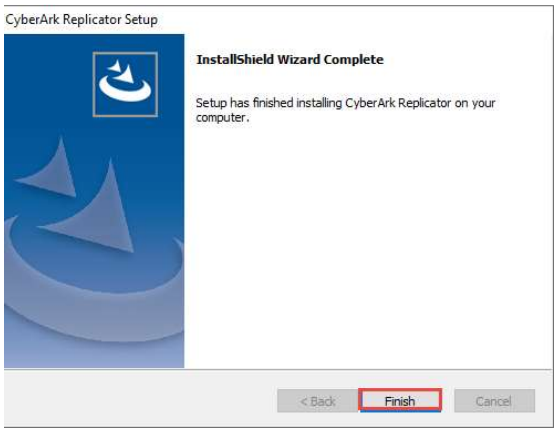
1. Enter *ACME Corp* for the user and company names and click Next, and Next again to accept the default destination location.



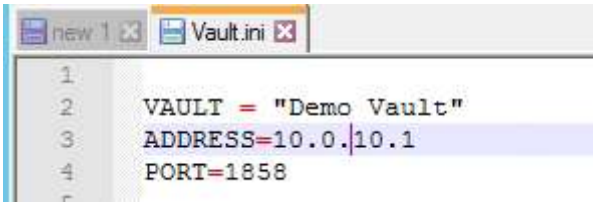


1. Press Next to accept the default Safes location and click Finish to complete the installation.





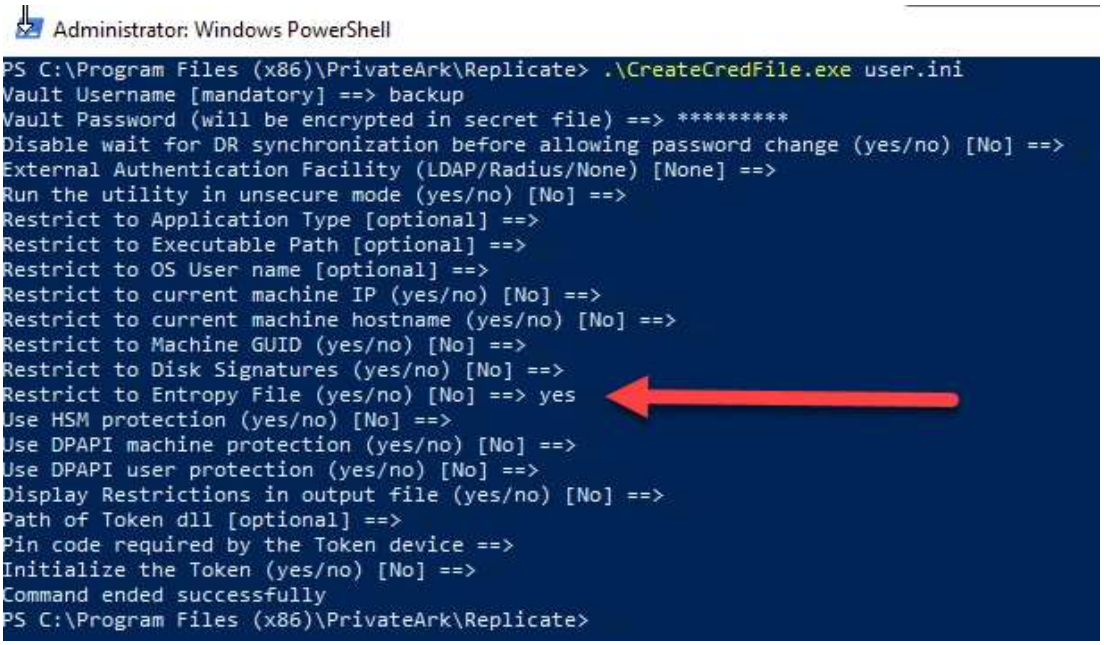
1. In Windows File Explorer, navigate to C:\Program Files (x86)\PrivateArk\Replicate.
2. Edit the Vault.ini file and enter the IP address of your Vault server in the address parameter.



1. Save and close the file.

Objective: Create a credential file that the Replicator Component will use to authenticate to the vault server.

1. Open “Windows PowerShell” in the Replicate root installation directory, “C:\Program Files (x86)\PrivateArk\Replicate”.
2. Use the CreateCredfile.exe utility to create the user.ini for the backup user with the following options.
   a. Vault Username: backup
   b. Vault Password: Cyberark1
   c. Type “Yes” at Restrict to Entropy File option. Accept the defaults for all other options.



Create a Windows Scheduled Task

Objective: Create a Windows Scheduled Task to launch PAReplicate and backup the vault data on a schedule.

1. Open the “Task Scheduler” application from the Windows Start Menu > Administrative Tools menu. Select Task Scheduler Library, right click and select Create a Basic Task.
   a. In the Name field type ‘CyberArk Vault Full Backup’ and click Next.
   b. Task Trigger select Daily and click Next.
   c. Accept the default start date and time and click Next.
   d. Action: Select ‘Start a program’ and select Next.
   e. Start a Program: Program/script: field enter the following including double quotes.

“C:\Program Files (x86)\PrivateArk\Replicate\PAReplicate.exe”

a. Enter the following without double quotes in the ‘Arguments (optional):’ field.

vault.ini /logonfromfile user.ini /FullBackup

a. Enter the following without double quotes in the ‘Start in (optional):’ field

C:\Program Files (x86)\PrivateArk\Replicate

1. Click Next and Finish at the Summary.
2. Double click the ‘CyberArk Vault Full Backup’ from the Task Scheduler Library.
3. In Security options, Change the User or Group to ‘System’ and click Ok.
4. Select the ‘CyberArk Vault Full Backup’ from the Task Scheduler Library, right click on it and select ‘Run’.

Note: You can check the status of the job by scrolling to the right and refreshing column 'Last Run Result'

You can also run the command from a command line as follows, as an initial test.

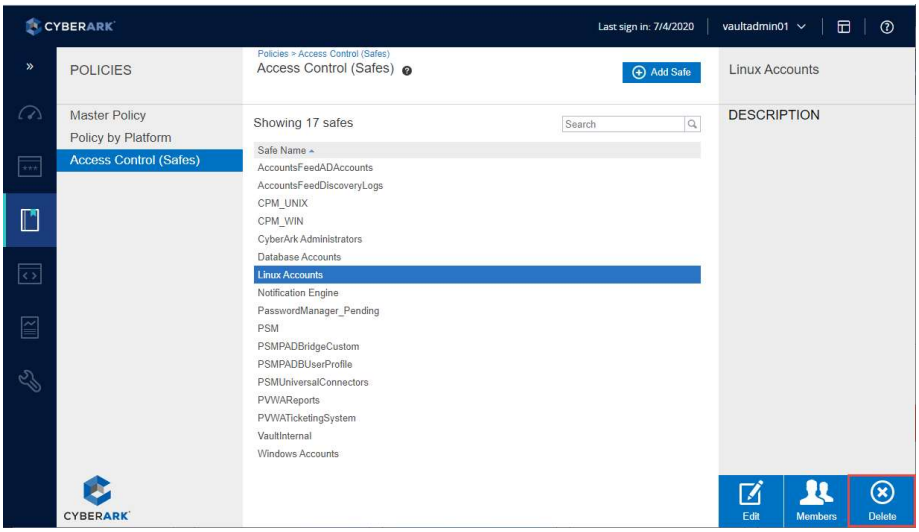
1. ```
   c:\Program Files (x86)\PrivateArk\Replicate>PAReplicate.exe vault.ini /logonfromfile user.ini /FullBackup
   ```
2. Review the PAReplicate.log file located in the \Replicate root directory.

Note: The first time running PAReplicate with the /FullBackup argument may take an extended amount of time in a Production environment depending on the number and size of accounts and PSM recordings.
Subsequent Full Backups will only backup changed files, equivalent to an incremental backup.

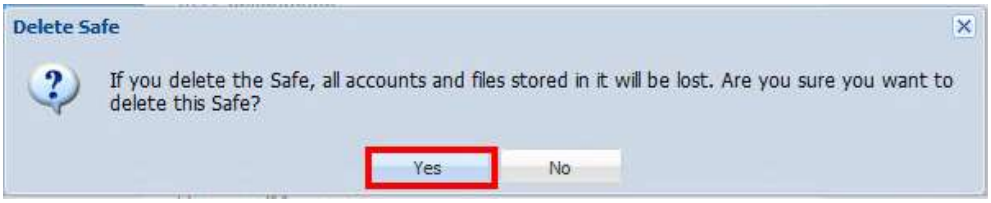
-

Testing the Backup/Restore Process

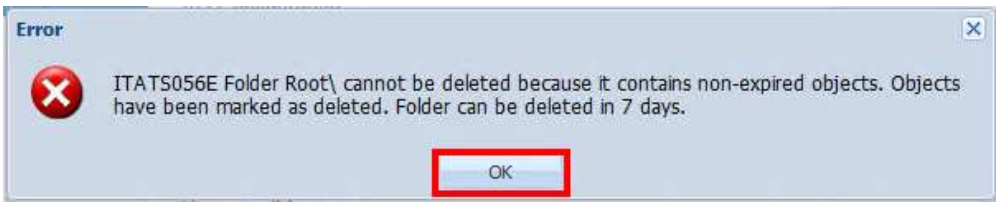
1. Login to the **PVWA** as Vaultadmin01.
2. Go to POLICIES > Access Control (Safes).
3. Select your Linux accounts safe and Delete it.



1. Press Yes to confirm that you would like to delete the Safe and its contents.



1. You will receive a message that the Root folder cannot be deleted for 7 days. However, the contents of the Safe will be removed.

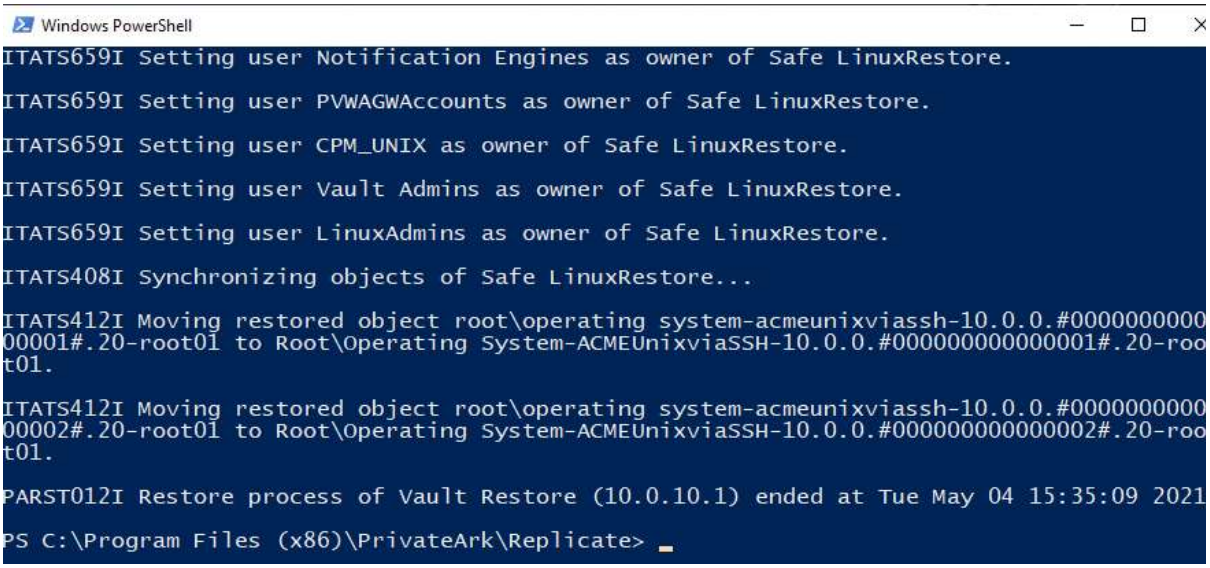

   ```

1. To confirm that the contents of the Safe have been deleted, go to the Accounts page.
2. Enter root01 in the search box and press the Search button and confirm that the root account that you created earlier in this exercise using address centos.acme.corp, will not appear.
3. Open a PowerShell Window in 'C:\Program Files (x86)\PrivateArk\Replicate' and run the following:

PARestore.exe vault.ini dr /RestoreSafe "Linux Accounts" /TargetSafe LinuxRestore

Note: If the command doesn't run, check the syntax and make sure you have entered all the spaces correctly.

1. Enter the DR user's password (Cyberark1).
2. You should receive a message "PARST012I Restore process of Vault Restore (10.0.10.1) ended…"



1. Return to the PVWA as Vaultadmin01 and search for root01 again.
2. You should now see the root01 account residing in the Safe LinuxRestore.

Disaster Recovery

Objective: In this section we will install and test the Disaster Recovery module. Prior to installing the CyberArk Disaster Recovery software, the DR server must have the **Private Ark Server** installed.

Note: The **PrivateArk Server v12.6** and **PrivateArk Client** software has already been installed on your DR server.

IMPORTANT: Ensure that the DR VM is running in your Skytap lab before proceeding.

Note: If you have completed the CyberArk Vault Backup exercise, the DR user has already been enabled. If you did not enable the DR user, do it now.

Note: The DR Vault must be configured to support LDAP Authentication. The import of the CA Root Certificate and the Hosts file configuration has been updated for you.

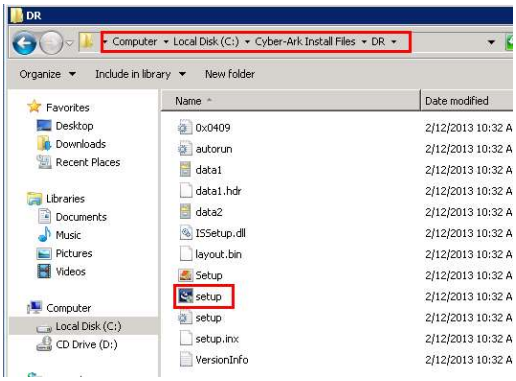
Install the Disaster Recovery Module

1. Sign into the Disaster Recovery Vault server (DR) as *Administrator*.
2. Open the Server Central Administration app from the Desktop icon labeled 'PrivateArk Server' to confirm the version of the DR Digital Vault is identical to the version installed on the Primary Digital Vault Server.

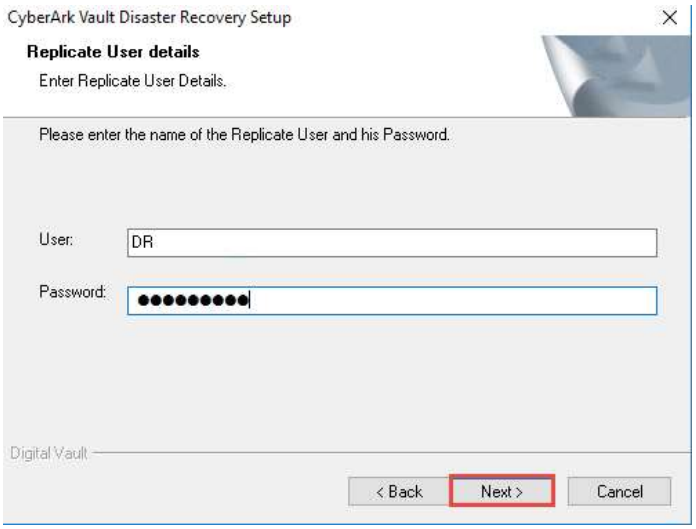
a. Look for the message "**ITADB313I** Server (12.6.0.21) is up"
b. Close the Server Central Administration application.

3. Open the PrivateArk client and login to the DRVault (10.0.14.1) as administrator/Cyberark1. Confirm that the only Safes in the Vault should be the three built-in Safes as shown in the graphic below.

1. Logoff and close the PrivateArk Client application.
2. Open the Windows Services applet and stop the PrivateArk Server service and all dependencies.
3. Open File Explorer and navigate to "C:*CYBR_Files\Vault Installation Files/Disaster Recovery*".
4. Right click setup.exe and "Run as administrator".



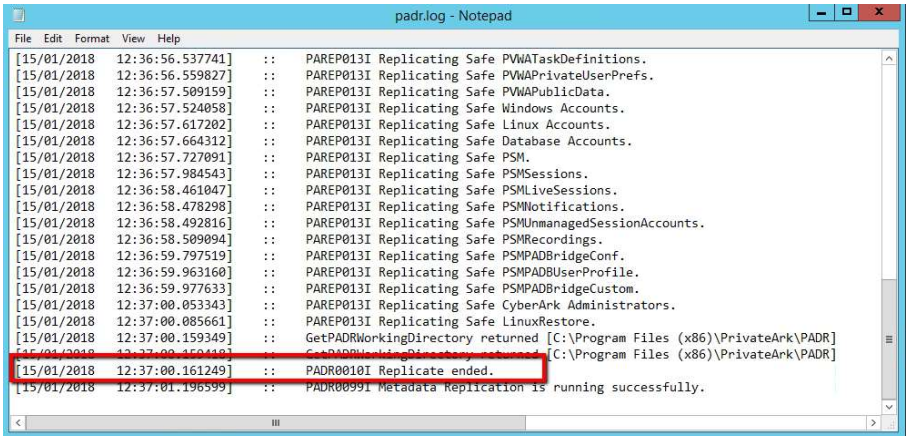
1. Press Next on the welcome screen and Yes to accept the license agreement.
2. Enter "ACME Corp" in the Company field.
3. Click Next to accept the default destination folder.
4. Enter DR as the user and *Cyberark1* as the password and click Next.



1. Enter your Primary Vault IP Address (10.0.10.1) and click Next,
2. Allow the server to restart by pressing Finish.

Validate Replication

1. After the server restarts, sign in to the **DR Server** as Administrator/Cyberark1.
2. Confirm that the production Vaultreplicated successfully.
    a. Open the C:\Program Files (x86)\PrivateArk\PADR\Logs\PADR.log file, you should see entries with informational codes PAREP013I Replicating Safe and at the end, PADR0010I Replicate ended.



1. Open \Conf\PADR.INI file and note that FailoverMode is equal to No.

Execute Automatic Failover Test

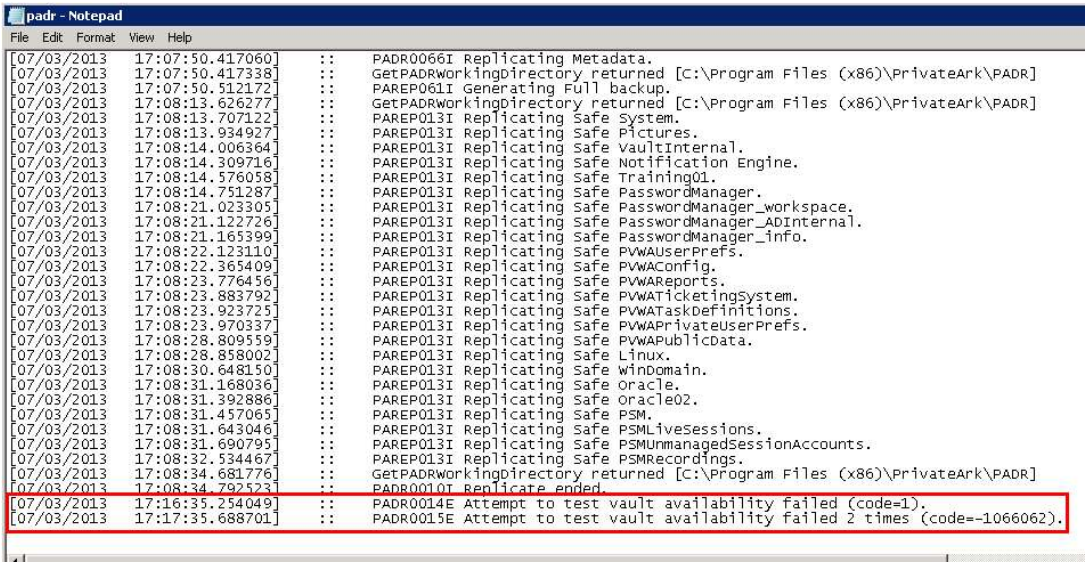
Preparation: In the following procedures you will be guided through the process of failover and failback, replicating Vault data to and from the DR Vault. This requires an additional DR user that you must create on the Primary Vault so that it is available on the DR Vault when needed.

Note: The following procedure requires additional licensing to support a second DR user.

1. Sign in to the PVWA on Comp01A/B. Find the built-in Administrator for the Vault and launch the PSM-PrivateArk Client Connection Component.
2. Select menu item Tools > Administrative Tools > Users and Groups then select the System folder.
3. Select New > User and configure the following.
    a. Tab ‘General Details’
        - User Name: DR_Failback
        - User type: DR_Users
    b. Tab ‘Authentication’
        - set the password to ‘Cyberark1’ and confirm.
        - Deselect ‘User Must Change Password at Next Logon and select Password Never Expires.
    c. Tab ‘Authorizations’
        - select Backup All Safes and Restore All Safes.
    d. Tab ‘Member Of’
        - In the Groups column on the right, select ‘DR Users’ and move to the ‘Member Of:’ column on the left.
4. Click OK to save. Close the ‘Users and Groups’ window and Logoff the PrivateArk Client.
5. Sign in to the DR Vault server console and restart the CyberArk Vault Disaster Recovery Service using the Windows Services Applet. This will ensure that the new DR_Failback user has been replicated to the DR Vault.
    a. Check the PADR.LOG file to ensure that replication is working correctly.

Objective: Execute Failover procedures.

1. Sign in to the console of your **Primary** Vault server, VAULT01A.
2. Open the Windows Services applet and stop the PrivateArk Server service and all dependencies.
3. On the console of the *DR Server*, open the PADR log file. You should see messages stating that the DR Vault cannot reach the production Vault.

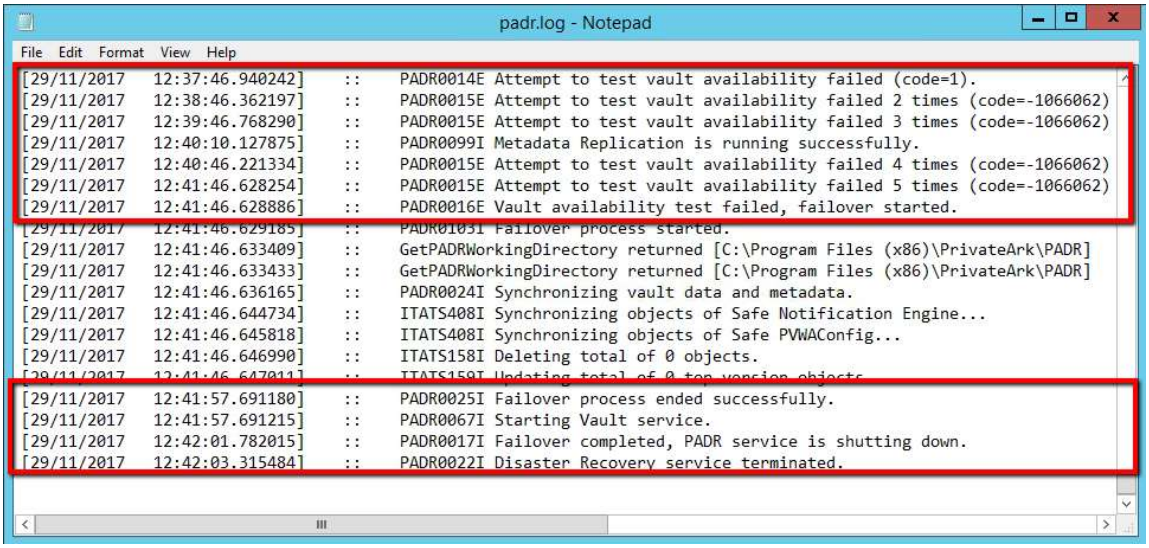


```
padr - Notepad
File  Edit  Format  View  Help
[07/03/2013   17:07:50.417060]   ::   PADR0066I Replicating Metadata.
[07/03/2013   17:07:50.417338]   ::   GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[07/03/2013   17:07:50.512172]   ::   PAREP061I Generating Full backup.
[07/03/2013   17:08:13.626277]   ::   GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[07/03/2013   17:08:13.707122]   ::   PAREP013I Replicating Safe System.
[07/03/2013   17:08:13.934927]   ::   PAREP013I Replicating Safe Pictures.
[07/03/2013   17:08:14.006364]   ::   PAREP013I Replicating Safe VaultInternal.
[07/03/2013   17:08:14.309716]   ::   PAREP013I Replicating Safe Notification Engine.
[07/03/2013   17:08:14.576058]   ::   PAREP013I Replicating Safe Training01.
[07/03/2013   17:08:14.751287]   ::   PAREP013I Replicating Safe PasswordManager.
[07/03/2013   17:08:21.023305]   ::   PAREP013I Replicating Safe PasswordManager_workspace.
[07/03/2013   17:08:21.122726]   ::   PAREP013I Replicating Safe PasswordManager_ADInternal.
[07/03/2013   17:08:21.165399]   ::   PAREP013I Replicating Safe PasswordManager_info.
[07/03/2013   17:08:22.123110]   ::   PAREP013I Replicating Safe PVWAUserPrefs.
[07/03/2013   17:08:22.365409]   ::   PAREP013I Replicating Safe PVWAConfig.
[07/03/2013   17:08:23.776456]   ::   PAREP013I Replicating Safe PVWAReports.
[07/03/2013   17:08:23.883792]   ::   PAREP013I Replicating Safe PVWATicketingSystem.
[07/03/2013   17:08:23.923725]   ::   PAREP013I Replicating Safe PVWATaskDefinitions.
[07/03/2013   17:08:23.970337]   ::   PAREP013I Replicating Safe PVWAPrivateUserPrefs.
[07/03/2013   17:08:28.809559]   ::   PAREP013I Replicating Safe PVWAPublicData.
[07/03/2013   17:08:28.858002]   ::   PAREP013I Replicating Safe Linux.
[07/03/2013   17:08:30.648150]   ::   PAREP013I Replicating Safe WinDomain.
[07/03/2013   17:08:31.168036]   ::   PAREP013I Replicating Safe Oracle.
[07/03/2013   17:08:31.392886]   ::   PAREP013I Replicating Safe Oracle02.
[07/03/2013   17:08:31.457065]   ::   PAREP013I Replicating Safe PSM.
[07/03/2013   17:08:31.643046]   ::   PAREP013I Replicating Safe PSMLiveSessions.
[07/03/2013   17:08:31.690795]   ::   PAREP013I Replicating Safe PSMUnmanagedSessionAccounts.
[07/03/2013   17:08:32.534467]   ::   PAREP013I Replicating Safe PSMRecordings.
[07/03/2013   17:08:34.681776]   ::   GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[07/03/2013   17:08:34.792523]   ::   PADR0010I Replicate ended.
[07/03/2013   17:16:35.254049]   ::   PADR0014E Attempt to test vault availability failed (code=1).
[07/03/2013   17:17:35.688701]   ::   PADR0015E Attempt to test vault availability failed 2 times (code=-1066062).
```

1. Alternatively, follow the tail of the padr.log using Windows Powershell.
2. Open Windows PowerShell from the taskbar.
3. Change directories to “C:\Program Files (x86)\PrivateArk\PADR”
4. Type the following command

Get-Content .\logs\padr.log –wait

1. After 5 failures by default, the DR Vault will go into failover mode. Total duration = 5 minutes. Check the PADR.log and review the sequence of events.



```
padr.log - Notepad
File  Edit  Format  View  Help
[29/11/2017   12:37:46.940242]   ::   PADR0014E Attempt to test vault availability failed (code=1).
[29/11/2017   12:38:46.362197]   ::   PADR0015E Attempt to test vault availability failed 2 times (code=-1066062)
[29/11/2017   12:39:46.768290]   ::   PADR0015E Attempt to test vault availability failed 3 times (code=-1066062)
[29/11/2017   12:40:10.127875]   ::   PADR0099I Metadata Replication is running successfully.
[29/11/2017   12:40:46.221334]   ::   PADR0015E Attempt to test vault availability failed 4 times (code=-1066062)
[29/11/2017   12:41:46.628254]   ::   PADR0015E Attempt to test vault availability failed 5 times (code=-1066062)
[29/11/2017   12:41:46.628886]   ::   PADR0016E Vault availability test failed, failover started.
[29/11/2017   12:41:46.629185]   ::   PADR0103I Failover process started.
[29/11/2017   12:41:46.633409]   ::   GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017   12:41:46.633433]   ::   GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017   12:41:46.636165]   ::   PADR0024I Synchronizing vault data and metadata.
[29/11/2017   12:41:46.644734]   ::   ITATS408I Synchronizing objects of Safe Notification Engine...
[29/11/2017   12:41:46.645818]   ::   ITATS408I Synchronizing objects of Safe PVWAConfig...
[29/11/2017   12:41:46.646990]   ::   ITATS158I Deleting total of 0 objects.
[29/11/2017   12:41:46.647011]   ::   ITATS159I Updating total of 0 top version objects.
[29/11/2017   12:41:57.691180]   ::   PADR0025I Failover process ended successfully.
[29/11/2017   12:41:57.691215]   ::   PADR0067I Starting Vault service.
[29/11/2017   12:42:01.782015]   ::   PADR0017I Failover completed, PADR service is shutting down.
[29/11/2017   12:42:03.315484]   ::   PADR0022I Disaster Recovery service terminated.
```

1. On the DR Vault server, open the PrivateArk client.
2. Modify the properties of the DRVault (10.0.14.1) shortcut to require LDAP Authentication. Login as VaultAdmin01.

Note: The DR Vault has a CA Root certificate and Hosts file configured to support LDAP/S.

Note: The built-in *Administrator* user is now being managed by the CPM and the password has been changed and replicated to the DR Vault. In the event of an actual disaster, the built-in *Administrators* password may not be accessible and so it is important to configure the DR Vault to support LDAP Authentication for administrative and normal user access.

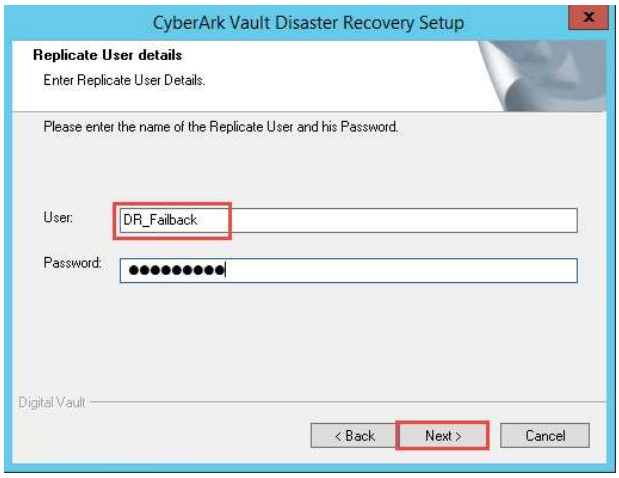
Note: The Safes and data should match those in the Primary Vault.

1. Logoff the PrivateArk Client.

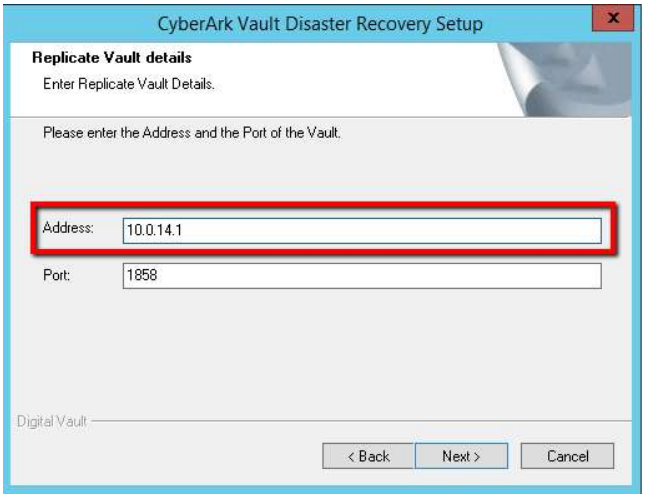
Execute Failback Procedure Using Manual Failover

Objective: Replicate data back from the **DR Vault** to the **Primary Vault**, perform a **Manual Failover** to the **Primary Vault** and set the DR server back to DR mode.

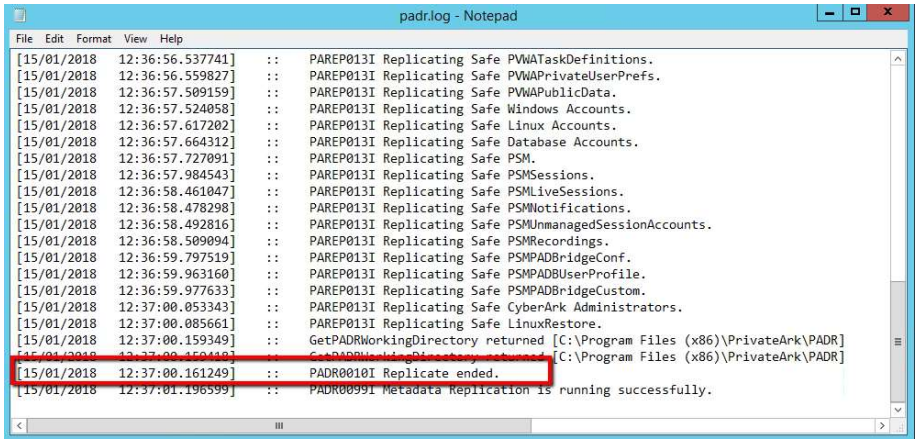
1. Sign in to the **Primary Vault Server** and repeat the steps for Installing the DR module, this time configuring the DR module to replicate data from the **DR Vault**.
   a. Enter DR_Failback as the DR user with password ‘Cyberark1’.



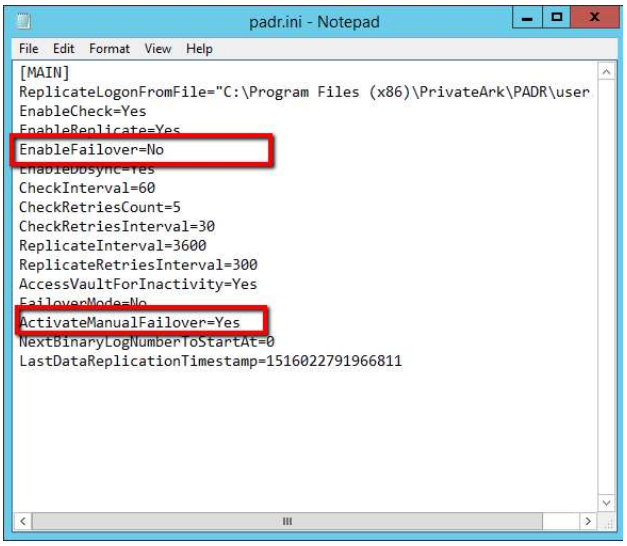
a. Enter the DR Vaults IP Address.



1. After the server restart, review the PADR.LOG on VAULT01A to verify that the Primary Vault has replicated all changes, if any from the DR Vault.



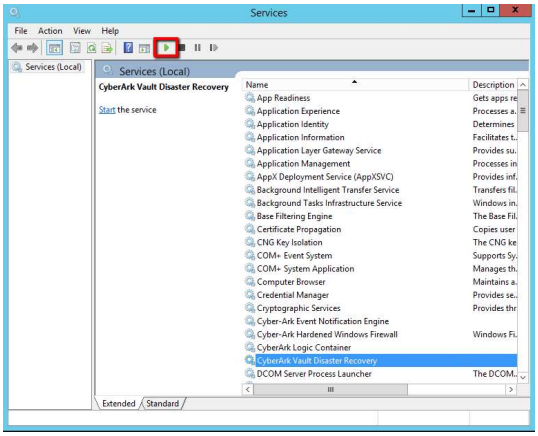
1. On the **Primary Vault Server**edit the PADR.ini file.
   a. Set EnableFailover=No
   b. Add the following line: ActivateManualFailover=Yes
   c. Save the file and exit.



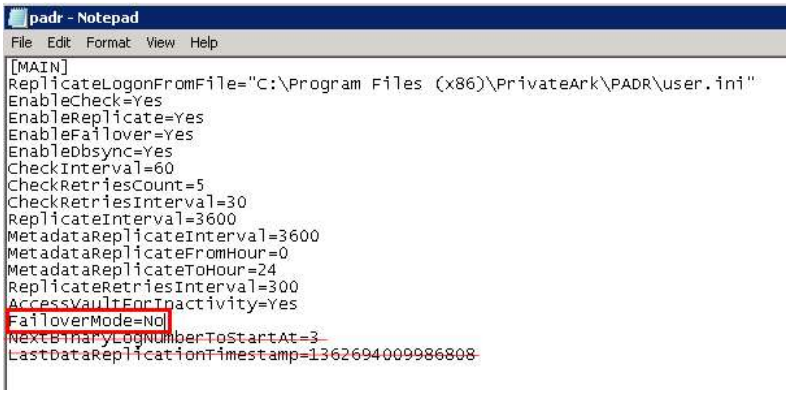
1. Restart the ‘CyberArk Vault Disaster Recovery’ Service on the Primary Server. The service should start and stop immediately (because of the “ActivateManualFailover” parameter), then the ‘PrivateArk Server’

service should start. Verify that the PrivateArk Server service has started successfully on the Primary Vault server.

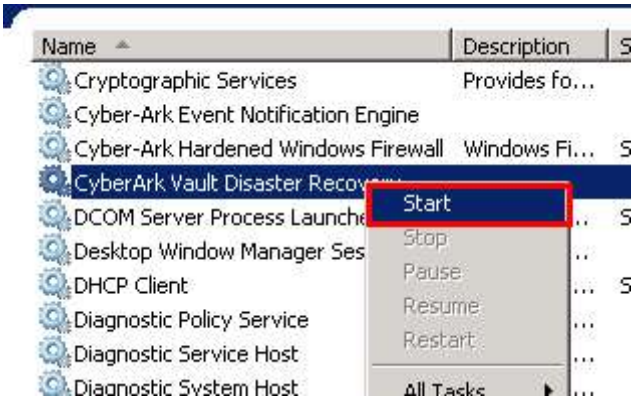
a. Wait a few minutes. If the PrivateArk Server service does not start automatically, start the service manually.



1. On the **DR Vault server**edit the PADR.ini file.
   a. Change *Failover mode* from Yes to No.
   b. Delete the last two lines (log number and timestamp of the last successful replication) in the file. This will trigger a full replication.
   c. Save and exit the file.



1. Using the Windows Services applet, stop the PrivateArk Server service and Start the CyberArk Vault Disaster Recovery service.



1. Check the PADR log file and confirm that the replication process started and that the replication (from the Primary Server to the DR Server) has ended successfully.

```
Windows PowerShell
[15/12/2022  15:24:01.429070]  ::  PAREP013I Replicating Safe PasswordManager_ADInternal.
[15/12/2022  15:24:01.444358]  ::  PAREP013I Replicating Safe PasswordManager_Info.
[15/12/2022  15:24:01.469090]  ::  PAREP013I Replicating Safe PasswordManager_Accounts.
[15/12/2022  15:24:01.479649]  ::  PAREP013I Replicating Safe PasswordManagerShared.
[15/12/2022  15:24:01.495979]  ::  PAREP013I Replicating Safe PasswordManagerTemp.
[15/12/2022  15:24:01.512211]  ::  PAREP013I Replicating Safe PasswordManager_Pending.
[15/12/2022  15:24:01.525775]  ::  PAREP013I Replicating Safe AccountsFeedADAccounts.
[15/12/2022  15:24:01.538873]  ::  PAREP013I Replicating Safe AccountsFeedDiscoveryLogs.
[15/12/2022  15:24:01.554097]  ::  PAREP013I Replicating Safe CPM_UNIX.
[15/12/2022  15:24:01.579096]  ::  PAREP013I Replicating Safe CPM_UNIX_workspace.
[15/12/2022  15:24:01.616886]  ::  PAREP013I Replicating Safe CPM_UNIX_ADInternal.
[15/12/2022  15:24:01.651759]  ::  PAREP013I Replicating Safe CPM_UNIX_Info.
[15/12/2022  15:24:01.671694]  ::  PAREP013I Replicating Safe CPM_UNIX_Accounts.
[15/12/2022  15:24:01.689011]  ::  PAREP013I Replicating Safe Linux Accounts.
[15/12/2022  15:24:01.724427]  ::  PAREP013I Replicating Safe Windows Accounts.
[15/12/2022  15:24:01.754599]  ::  PAREP013I Replicating Safe Oracle Accounts.
[15/12/2022  15:24:01.787154]  ::  PAREP013I Replicating Safe PSM.
[15/12/2022  15:24:01.815007]  ::  PAREP013I Replicating Safe PSMSessions.
[15/12/2022  15:24:01.833865]  ::  PAREP013I Replicating Safe PSMLiveSessions.
[15/12/2022  15:24:01.859265]  ::  PAREP013I Replicating Safe PSMUniversalConnectors.
[15/12/2022  15:24:01.879107]  ::  PAREP013I Replicating Safe PSMNotifications.
[15/12/2022  15:24:01.907575]  ::  PAREP013I Replicating Safe PSMUnmanagedSessionAccounts.
[15/12/2022  15:24:01.937829]  ::  PAREP013I Replicating Safe PSMRecordings.
[15/12/2022  15:24:01.956462]  ::  PAREP013I Replicating Safe PSMPConf.
[15/12/2022  15:24:01.987254]  ::  PAREP013I Replicating Safe PSMPLiveSessions.
[15/12/2022  15:24:02.019403]  ::  PAREP013I Replicating Safe PSMPADBridgeConf.
[15/12/2022  15:24:02.050740]  ::  PAREP013I Replicating Safe PSMPADBUserProfile.
[15/12/2022  15:24:02.070150]  ::  PAREP013I Replicating Safe PSMPADBridgeCustom.
[15/12/2022  15:24:02.085165]  ::  PAREP013I Replicating Safe CyberArk Administrators.
[15/12/2022  15:24:02.117887]  ::  GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR
[15/12/2022  15:24:02.117931]  ::  GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR
[15/12/2022  15:24:02.133895]  ::  PADR0010I Replicate ended.
[15/12/2022  15:24:03.143043]  ::  PADR0099I Metadata Replication is running successfully.
```

(Optional) Exercises

Adding Firewall Rules to the Vault Manually

1. Log on to the vault operating system as Administrator.
2. Open up the dbparm.ini file, add the following lines at the bottom, then save the file.

```
[Firewall]
AllowNonStandardFWAddresses=[10.0.20.1],Yes,443:inbound/tcp
```

3. Open up the Privateark Server Icon and restart the **PrivateArk Server** service from there using the Traffic Light buttons. Watch the displayed log to make sure you see the following message.

```
07/08/2019   09:07:25   ITADB313I Server 10.9.0 (10.9.0.18) is up
07/08/2019   09:07:26   ITAQS031I Object cache is loaded.
```

4. Open a command prompt window and type in the following line to open the Windows Firewall

wf.msc

1. The firewall utility should show rules like these underneath the Inbound Rules section.

dbmain.exe_3	CYBERARK_RULE_NETWOR...	All	Yes	Allow	No	C:\Progr...	Any	Any	TCP	1858
dbmain.exe_3	CYBERARK_RULE_NETWOR...	All	Yes	Allow	No	Any	Any	Any	ICMPv4	Any
dbmain.exe_5	CYBERARK_RULE_NON_STD...	All	Yes	Allow	No	Any	Any	10.0.20.1	ICMPv4	Any
dbmain.exe_6	CYBERARK_RULE_NON_STD...	All	Yes	Allow	No	Any	Any	10.0.20.1	TCP	443
PARagent.exe_1	CYBERARK_RULE_RAGENT_...	All	Yes	Allow	No	C:\Progr...	Any	10.0.20.1, 10.0.21.1	TCP	9022
PARagent.exe_1	CYBERARK_RULE_RAGENT_...	All	Yes	Allow	No	Any	Any	10.0.20.1, 10.0.21.1	ICMPv4	Any

Logging On With the Master User

There are some cases where you will need to login to the Vault with the Master user. This can be in case of an emergency or to give permissions to a user for safe when there are no active users with the necessary permissions.

1. On the Vault Server edit the *"C:\Program Files (x86)\PrivateArk\Server\Conf\DBParm.ini*".
2. In order to use the Master user the dbparm.ini file must point to the location of the Recovery Private Key. By default this is the CD-ROM drive of the server. Because we do not have a CD-ROM drive (we are using VMs for our lab exercises) you will need to point it to the relevant location.
3. Update the "RecoveryPrvKey" parameter to point to the location of the file called "RecPrv.key" in the Master CD folder.
    a. C:\CYBR_Files\License and Operator Keys\Master CD\RecPrv.key
4. Restart the PrivateArk Server service using the Windows Service utility. Check the ITALOG.LOG file for error and warnings.
5. Open the Private Ark client from the Vault Server machine.
6. In the User name filed type: Master.
7. In the Password field enter the password that you selected during the installation process (Cyberark1).
8. You should now be logged on to the Vault as the Master user.

What system safes do you see now that you did not see with the built in administrator user? Note that you can see all the safes you created using the different users.

[1] The Cyber-Ark Event Notification Engine service is configured to Automatic (Delayed Start). It may take a few minutes to start.