cpm-logfiles-session21

The Location of the Log Files: C:\Program Files(x86)\CyberArk\PasswordManager\Logs

## List of Log Files Related to CPM

* CACPMScanner.log
  + Account discovery related information is logged here.
* Casos.Activity.log
  + The CPM related activity is logged here, the transactions between the vault and the cpm is logged here
* Casos.Debug.log
* Casos.Error.log
  + vault related errors are updated here
* pm.log
  + the main log file for CPM, everything gets updated here.
* pm\_error.log
  + error related to logs are reported here.
* PMConsole.log
  + Policy related stuff is reported here
* PMTrace.log
  + Gets enabled after we enable debug mode

### Archive Folder

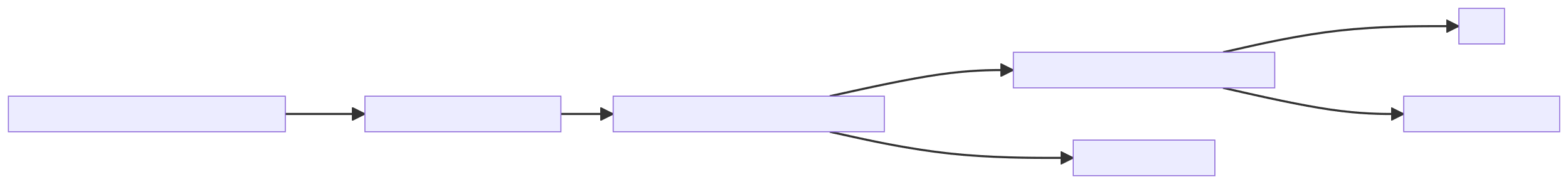
Folder that contains the older archived log files

### Third Party Logs

* Platform level debug log are stored here.
* when a platform is being debugged (we have to do this in PVWA under the particular platform), this platform related messages are logged in the Third Party Logs Folder.

## Troubleshooting Steps if CPM Fails to reconcile/change the Password

### CPM Login Flowchart

1. Attempt to log in with the password from the vault.
2. If the login fails, generate a new password.
3. Attempt to log in again with the new password.
4. If the second login is successful, update the vault with the new password.
5. If the update to the vault is successful, the process ends.
6. If the update to the vault fails, an error is shown.
7. If the second login attempt fails, a separate login error is shown.  
   

### Troubleshooting: CPM Password Change/Reconciliation Failures

* The first step in any troubleshooting process is to ping the target server in question
* Find the CPM that is handling this target server.
* We have to check the CPM port connectivity with the target server, the information is listed below
  + Test-NetConnection : By using Test-NetConnection, you can quickly diagnose network connectivity issues, ensuring that a host is reachable, a specific port is open, or even seeing the path your connection takes to reach its destination.
  1. **Ping a Host**: Test-NetConnection -ComputerName google.com
  2. **Specify a Port**: Test-NetConnection -ComputerName google.com -Port 80
  3. **Information Only**: Test-NetConnection -ComputerName google.com -InformationLevel Detailed
  4. **Trace Route**: Test-NetConnection -ComputerName google.com -TraceRoute
  5. **Check Common Services**: Test-NetConnection -ComputerName server\_name -CommonTCPPort RDP
     1. *The cmdlet also includes predefined parameters for common services like RDP (Remote Desktop), SMB (Windows File Sharing), and more.*

| Device | Protocol | Port |
| --- | --- | --- |
| Windows Domain Accounts | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 139, 445 |
|  | Kerberos | 88 |
|  | DNS | 53 |
| Windows Domain Accounts via LDAP | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 139, 445 |
|  | LDAP/s | 389, 636, 3268, 3269 |
|  | Kerberos | 88 |
|  | DNS | 53 |
| Windows Desktop Accounts | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 135, 445 |
| Windows Local Accounts | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 139, 445 |
| Windows Local Accounts over WMI | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 135, 445, dynamic port range |
| Windows Services | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 135, 445, dynamic port range |
| Windows Scheduled Tasks | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 445, dynamic port range |
| Windows IIS Application Pools | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 135, 445, dynamic port range |
| COM+ Applications | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 135, 445, dynamic port range |
| Windows IIS Directory Security | Windows protocols (SMB, RPC, WMI, DCOM, etc.) | 135, 445, dynamic port range |
| UNIX | SSH | 22 |
|  | Telnet | 23 |
| AS400 | iSeries Access for Windows | 449, 8476 |
| OS/390 | FTP | 21 |
|  | SSH | 22 |
|  | Telnet | 23 |
| ESXi | HTTP | 80 |
|  | HTTPS | 443 |