CYBERARK®
The Identity Security Company™

PAM Administration

Backup and Restore

Agenda

By the end of this session, you will be able to:

1. Describe the Backup and Restore solution
2. Test the procedures for **Vault** backup and restore

CYBERARK®

Overview

CYBERARK®

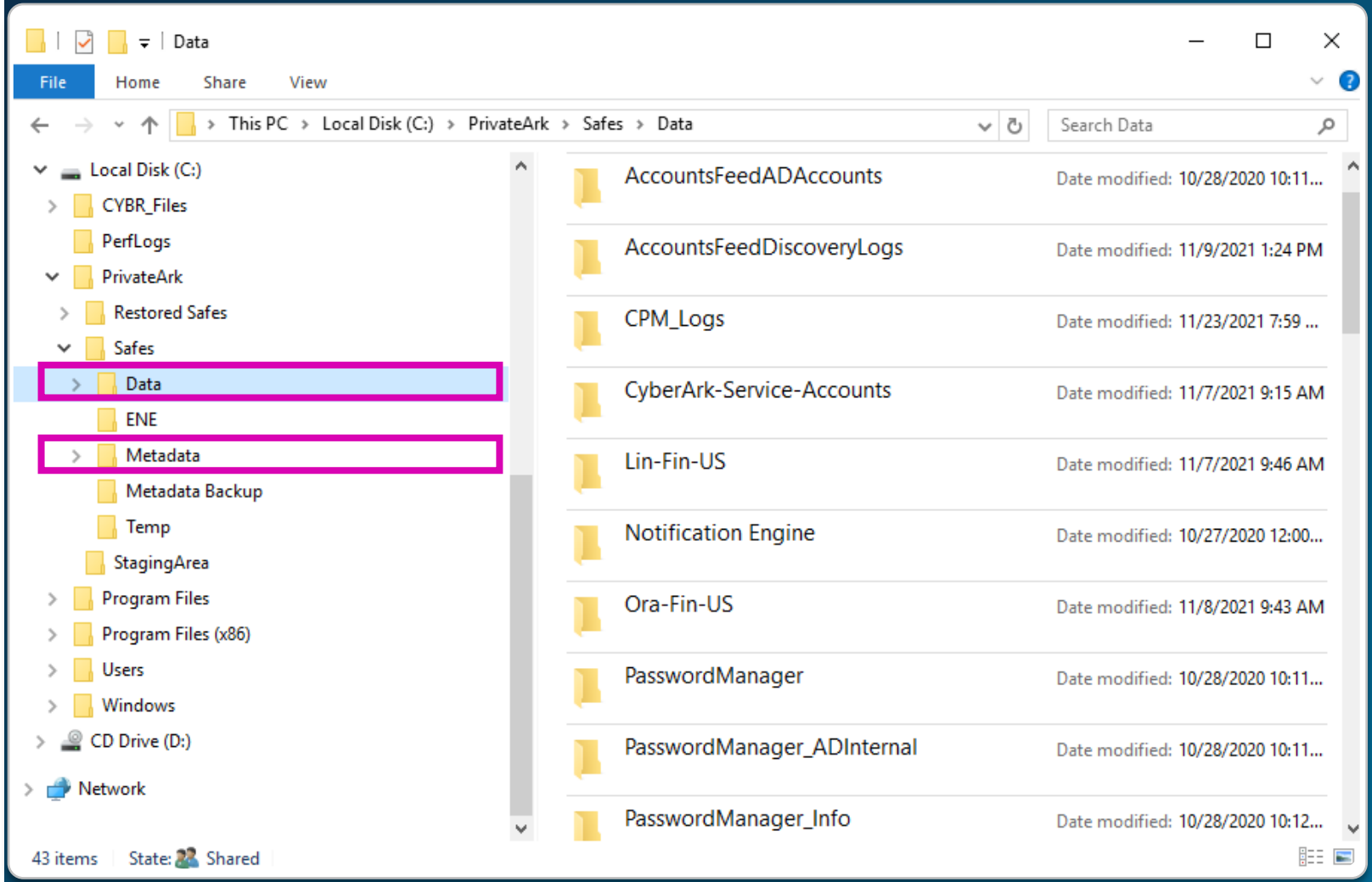
Replicate Use Cases

- Policy requires integration with an Enterprise Backup Solution.
- Policy requires granular point in time data protection.
- Policy requires object-level data protection.

CYBERARK®

Vault Backup Solution

- The Safes in the Vault are stored in the **Data** sub-directory
- Information about users, network areas, Safes, log records, and all activities that occur between them is stored in a database. Database files are stored in the **Metadata** sub-directory
- The Data and Metadata folders are extremely important and it is imperative to back them up regularly
- The CyberArk Vault enables you to backup and restore a single Safe to a Vault, as well as a complete Vault's data and metadata



CYBERARK®

Backup Considerations

Vault backup can be implemented in two ways:

Direct Backup
(Not Recommended)

- Third-party backup software is installed on the **Vault** and the application has access to the backup folders
- This introduces an external application to the **Vault** and potentially reduces the level of security

Indirect Backup
(Recommended)

- **The PrivateArk Replicate Utility** is installed on another server on the network, typically a server hosting another **CyberArk PAM** component
- The **Replicate Utility** *pulls* **Vault** data as encrypted files to the server
- Enterprise backup software can then backup these files

In this session we will focus on backing up using the **PrivateArk Replicate Utility**

CYBERARK®

CYBERARK®
The Identity Security Company™

Replicate Utility

- Installation
- Perform replication
- Perform restore
- Setup scheduled replications

Installation and Setup

CYBERARK®

Before Installing

Before installing the Replicator utility, make sure that the backup server has the following features and capabilities:

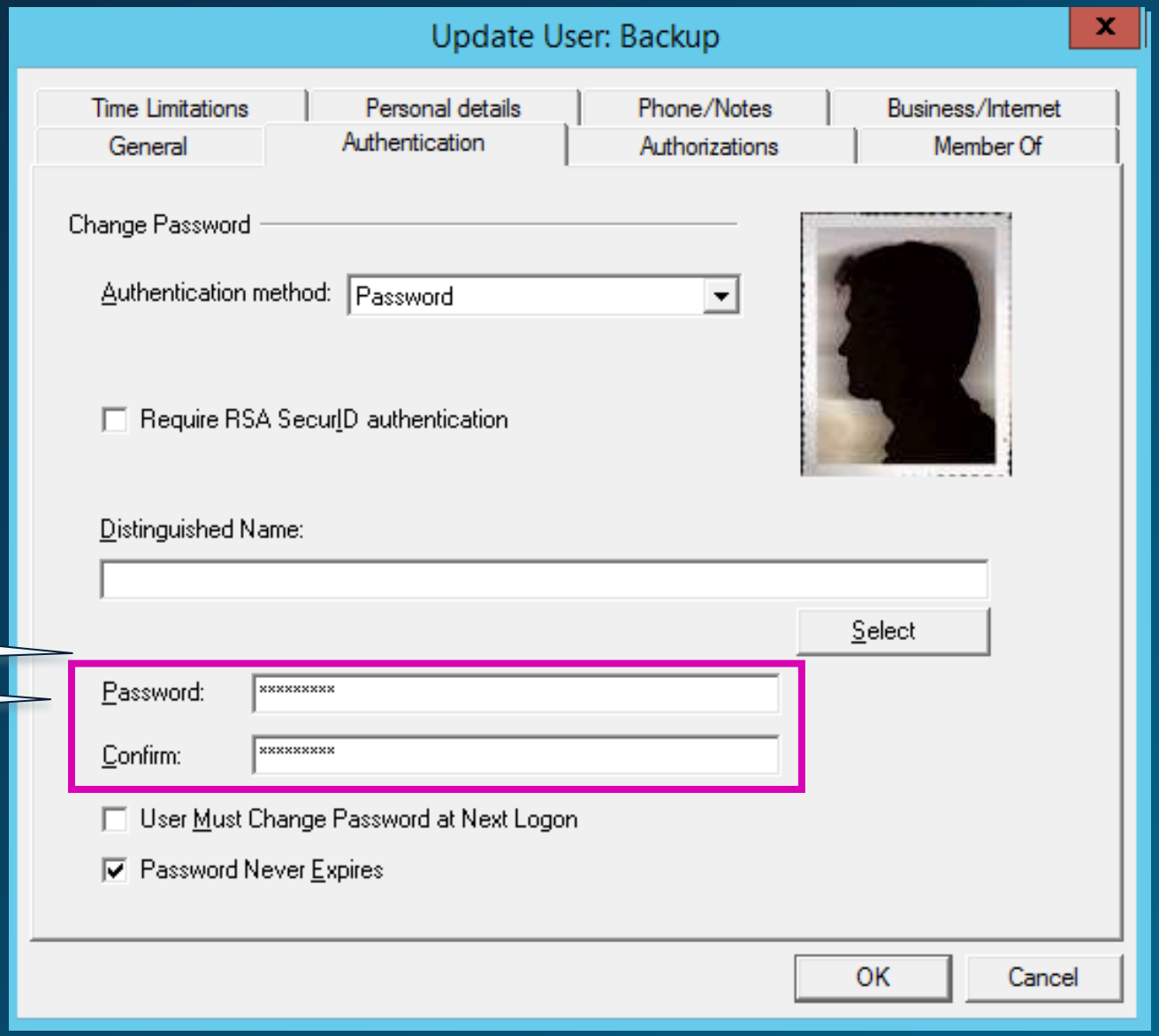
- At least the same disk space as the Vault database on an NTFS volume
- Accessibility by your enterprise backup system
- Physical security that only permits authorized users to access it

CYBERARK®

Before Installing

You will also need to:

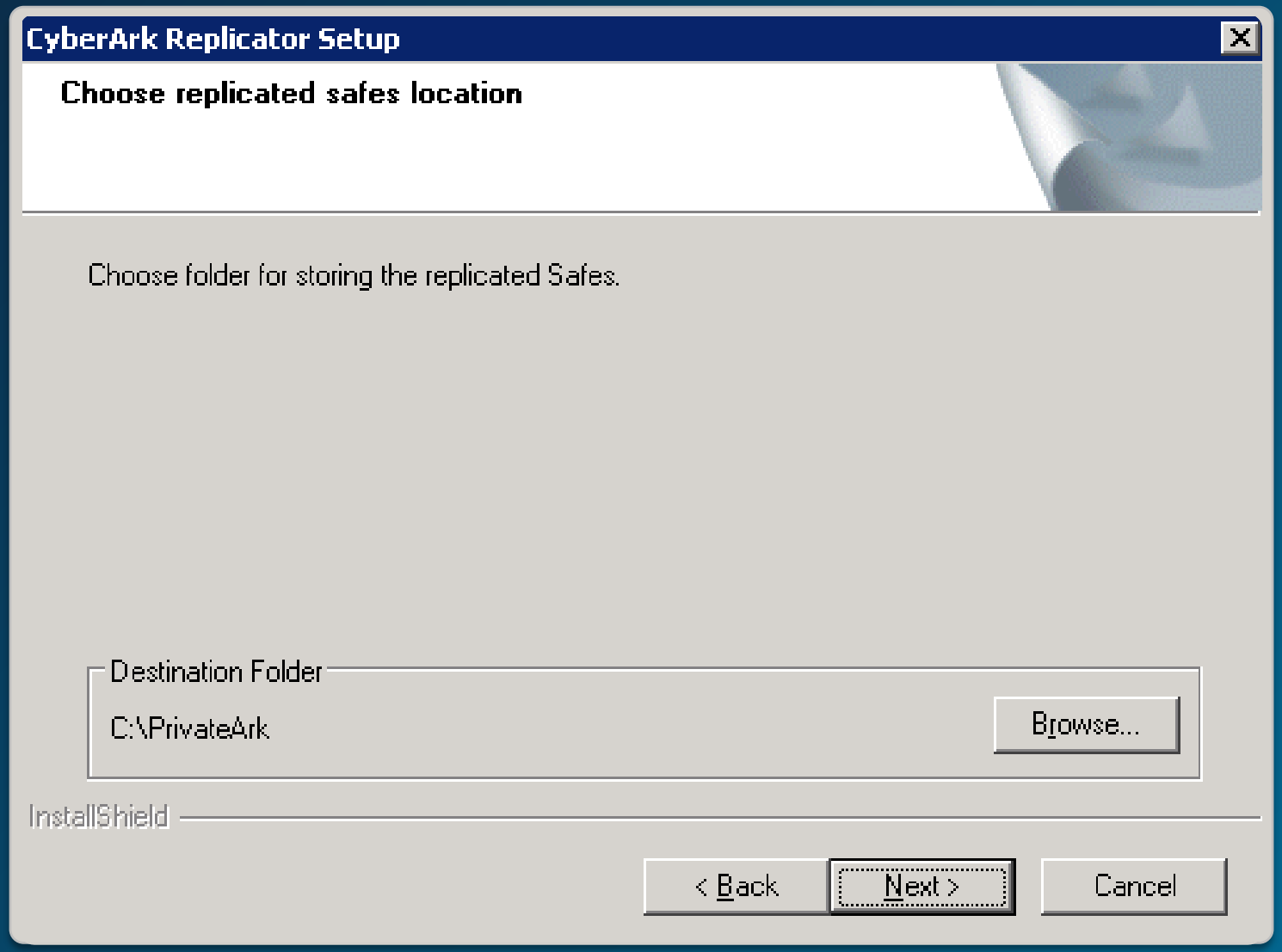
Set the password on the Primary **Vault**



CYBERARK®

Install the Utility

Install the **Replicator** module and specify a path to a backup folder for the replicated data



CYBERARK®

Configure Vault.ini

Edit the ***Vault.ini*** to give the **Replicator** utility the network address of the Vault server

Vault.ini

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

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

#TIMEOUT=30                        - Seconds to wait for a Vault to respond
#AUTHTYPE=PA_AUTH                  - Authentication method (PA_AUTH,NT_AUTH
#NTAUTHAGENTNAME=              - NT Authentication Agent Name
#NTAUTHAGENTKEYFILE=               - NT Authentication Key File Name
#VAULTDN=                  - Vault's Distinguished Name (PKI Authentication

#Proxy server connection settings  - cannot be used together with BEHINDFIR
#--------------------------------
#PROXYTYPE=HTTP                    - Possible values - HTTP, HTTPS, SOCKS4,
#PROXYADDRESS=192.333.44.55        - Proxy server IP address (mandatory whe
#PROXYPORT=8081                    - Proxy server IP Port
#PROXYUSER=xxx                     - User for Proxy server if NTLM authenti
#PROXYPASSWORD=yyy                 - Password for Proxy server if NTLM auth
#PROXYAUTHDOMAIN=NT_DOMAIN_NAME    - Domain for Proxy server if NTLM authen

#BEHINDFIREWALL=NO                 - Accessing the Cyber-Ark vault via a Fi

#USEONLYHTTP1=NO                   - Use only HTTP 1.0 protocol. Valid eith

#NUMOFRECORDSPERSEND=15            - Number of file records that require an
#NUMOFRECORDSPERCHUNK=15           - Number of file records to transfer tog
#RECONNECTPERIOD=-1                - Seconds to wait before session with Va
#ENHANCEDSSL=NO                    - Enhanced SSL based connection (port 44

#PREAUTHSECUREDSESSION=NO      - Enable pre authentication secured session
#TRUSTSSC=NO                - Trust self-sign certificates in pre authentica
#ALLOWSSCFOR3PARTYAUTH=NO      - Are self-sign certificates allowed for 3rd
```


CYBERARK®

Create Cred File

- The Credential File is used by the utility to authenticate to the **Vault** and should be hardened
- The password for the ***Backup*** user is changed in the **Vault** and the Credential File is updated after every successful login

```
CreateCredFile.exe backup.cred Password /username
backup /password Cyberark1 /ExePath "C:\Program Files
(x86)\PrivateArk\Replicate\PAReplicate.exe"
/IpAddress /Hostname /AppType CABACKUP /EntropyFile
/DpapiMachineProtection /DpapiUserProtection
```


CYBERARK®

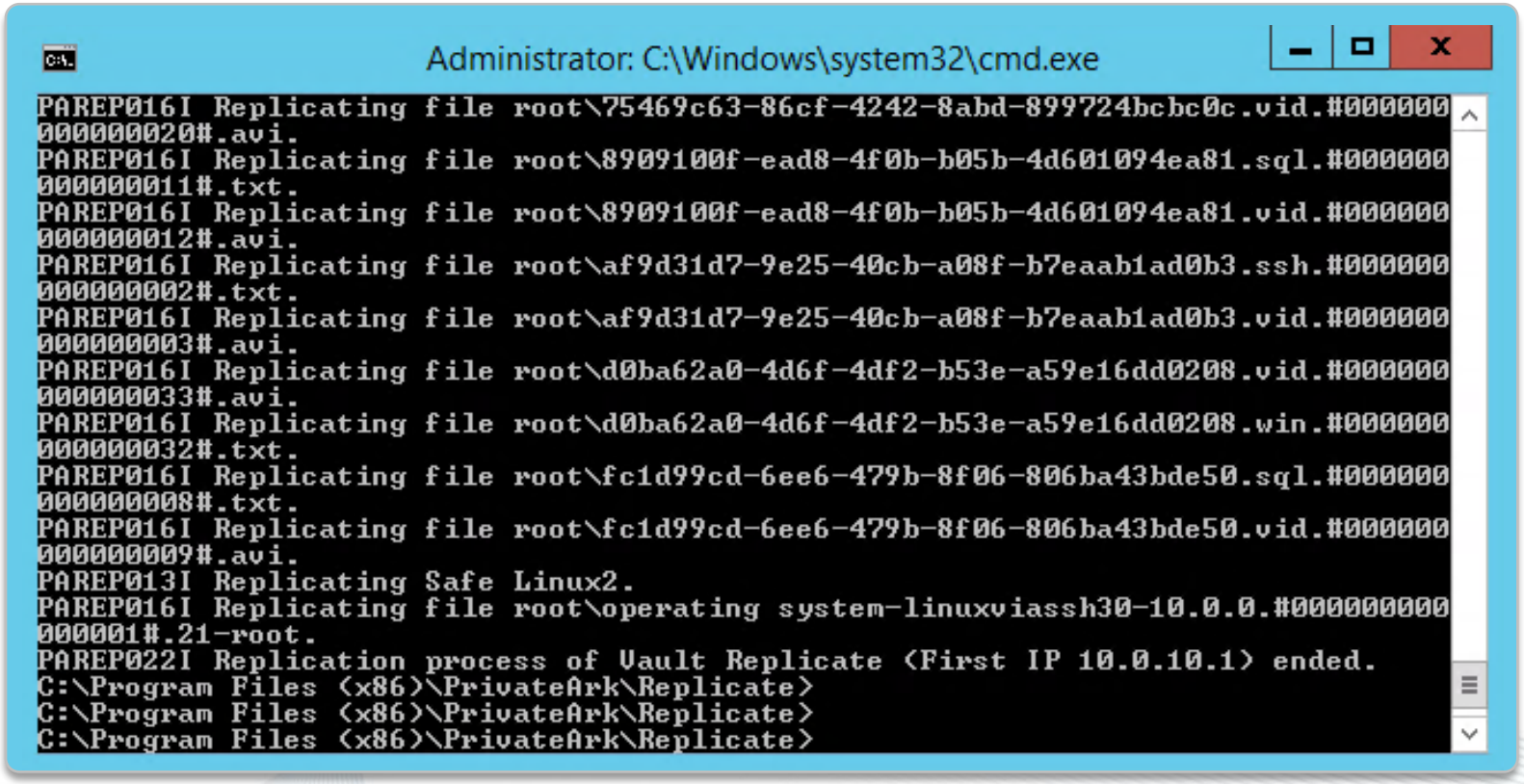
Test Backup and Restore

CYBERARK®

Performing a Backup

```
PAReplicate.exe vault.ini /logonfromfile user.ini /FullBackup
```

- The backup is launched at a command line using the ***PAReplicate.exe*** executable file
- The syntax of the command as shown specifies the ***vault.ini*** file and uses the ***logonfromfile*** and ***fullbackup*** switches



CYBERARK®

Performing a Restore

```
PARestore.exe vault.ini operator /RestoreSafe Linux02 /TargetSafe /LinuxRestore
```

- The **PARestore** command enables you to restore Safes that have previously been backed up
- Only users with the ***Restore All Safes*** authorization in the Vault can restore a Safe

Command Prompt

```
C:\Program Files (x86)\PrivateArk\Replicate>PARestore.exe vault.ini operator /RestoreSafe TEST /TargetSafe TEST-RESTORE
Password: *********
PARST011I Restore process of Vault Restore (10.0.10.1) started at Tue Dec 13 13:22:32 2022
PARST021I Restoring Metadata file backup-dump.sql.gz
PARST009I Restoring file backup-dump.sql.gz.
PARST021I Restoring Metadata file cfg.backup-enecredfile.ini.gz.
PARST009I Restoring file cfg.backup-enecredfile.ini.gz.
PARST021I Restoring Metadata file cfg.backup-replicationuser.pass.gz.
PARST009I Restoring file cfg.backup-replicationuser.pass.gz.
PARST019I 1 out of 1 dump files restored successfully.
PARST020I 0 out of 0 Binary Logs restored successfully.
PARST027I 2 out of 2 Configuration files restored successfully.
PARST009I Restoring file root\acme.#000000000000009#.corp-admin01-59048b6f-8658-48bf-b5bb-7370ec87c095.
PARST009I Restoring file root\operating system-unixssh-target-lin.acme.#000000000000005#.corp-root10.
PARST009I Restoring file root\operating system-unixssh-target-lin.acme.#000000000000014#.corp-linuxadmin01.
PARST009I Restoring file root\operating system-unixssh-target-lin.acme.#000000000000015#.corp-linuxadmin01.
PARST009I Restoring file root\operating system-unixssh-target-lin.acme.#000000000000016#.corp-linuxadmin01.
PARST009I Restoring file root\operating system-unixssh-target-lin.acme.#000000000000017#.corp-linuxadmin01.
PARST009I Restoring file root\operating system-unixssh-target-lin.acme.#000000000000018#.corp-linuxadmin01.
PARST009I Restoring file root\target-lin-root-3328c1c7-29b4-4e13-9fd0-f4970cf3cc99.#000000000000013#.
PARST009I Restoring file root\target-lin-root09-6eb3029d-beff-4cbc-9dc0-c258e6621872.#000000000000012#.
PARST009I Restoring file root\target-lin-root10-4695a844-fe84-4e41-b7a1-4e4ecf60b9be.#000000000000011#.
PARST009I Restoring file root\target-lin.acme.#000000000000010#.corp-root64-2224f592-ef78-42d7-b599-aaa47da248a8.
PARST009I Restoring file root\target-win.acme.#000000000000006#.corp-administrator-fac69564-5878-4120-8b49-50c27168b59d.
PARST009I Restoring file root\target-win.acme.#000000000000007#.corp-localadmin02-da32b881-5c69-4e9d-956f-a9b79d45b892.
PARST009I Restoring file root\target-win.acme.#000000000000008#.corp-localadmin01-cdd4c616-085f-4864-b0e3-1bf4db9ea45a.
PARST008I 14 out of 14 files restored successfully.
ITATS414I Synchronizing owners of Safe TEST-RESTORE.
```

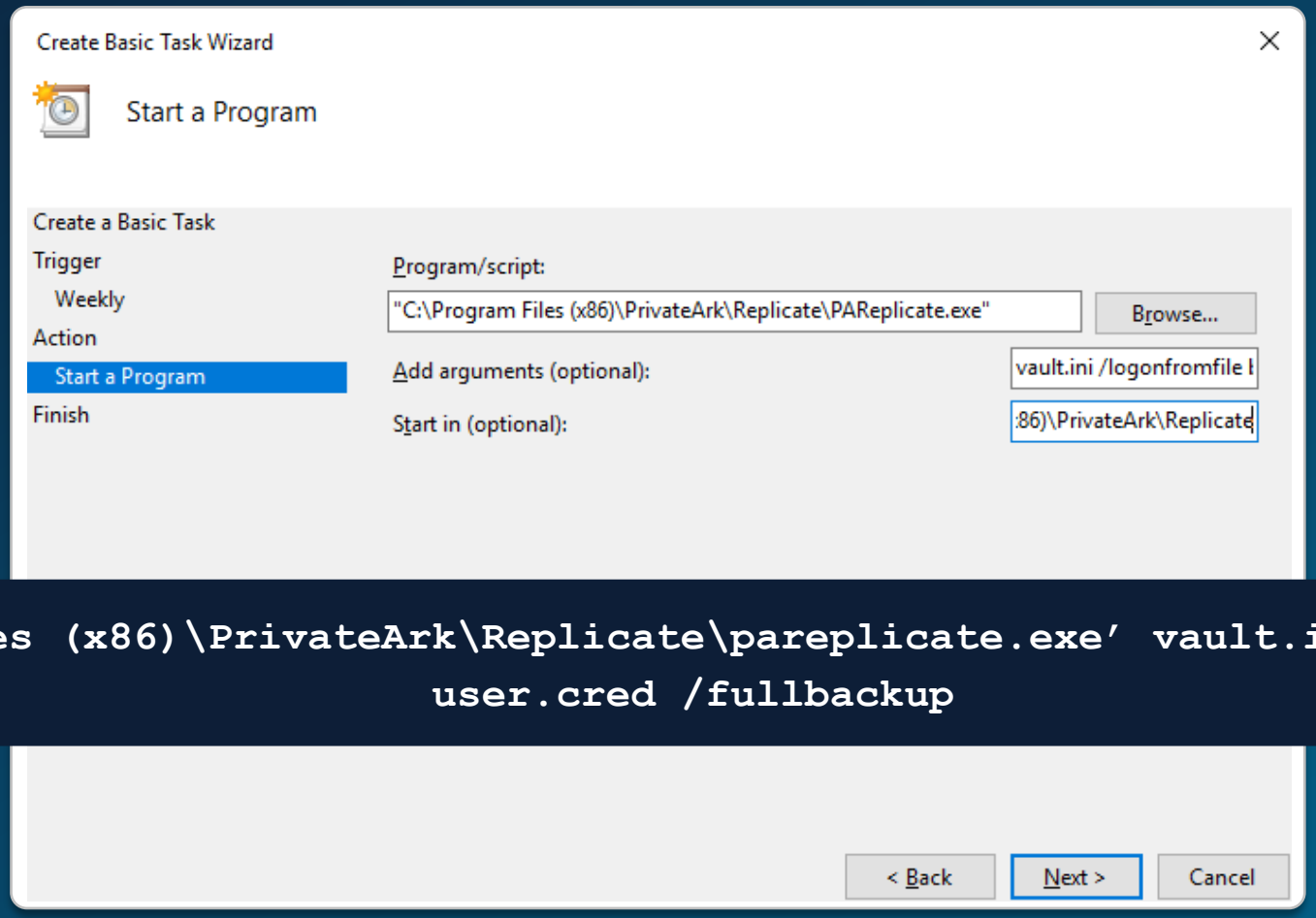

CYBERARK®

Set up Scheduled Backups

CYBERARK®

Setup Scheduled Backup

Scheduled Tasks can be created to launch backups at predetermined intervals.




```
C:\Program Files (x86)\PrivateArk\Replicate\pareplicate.exe' vault.ini /logonfromfile
user.cred /fullbackup
```

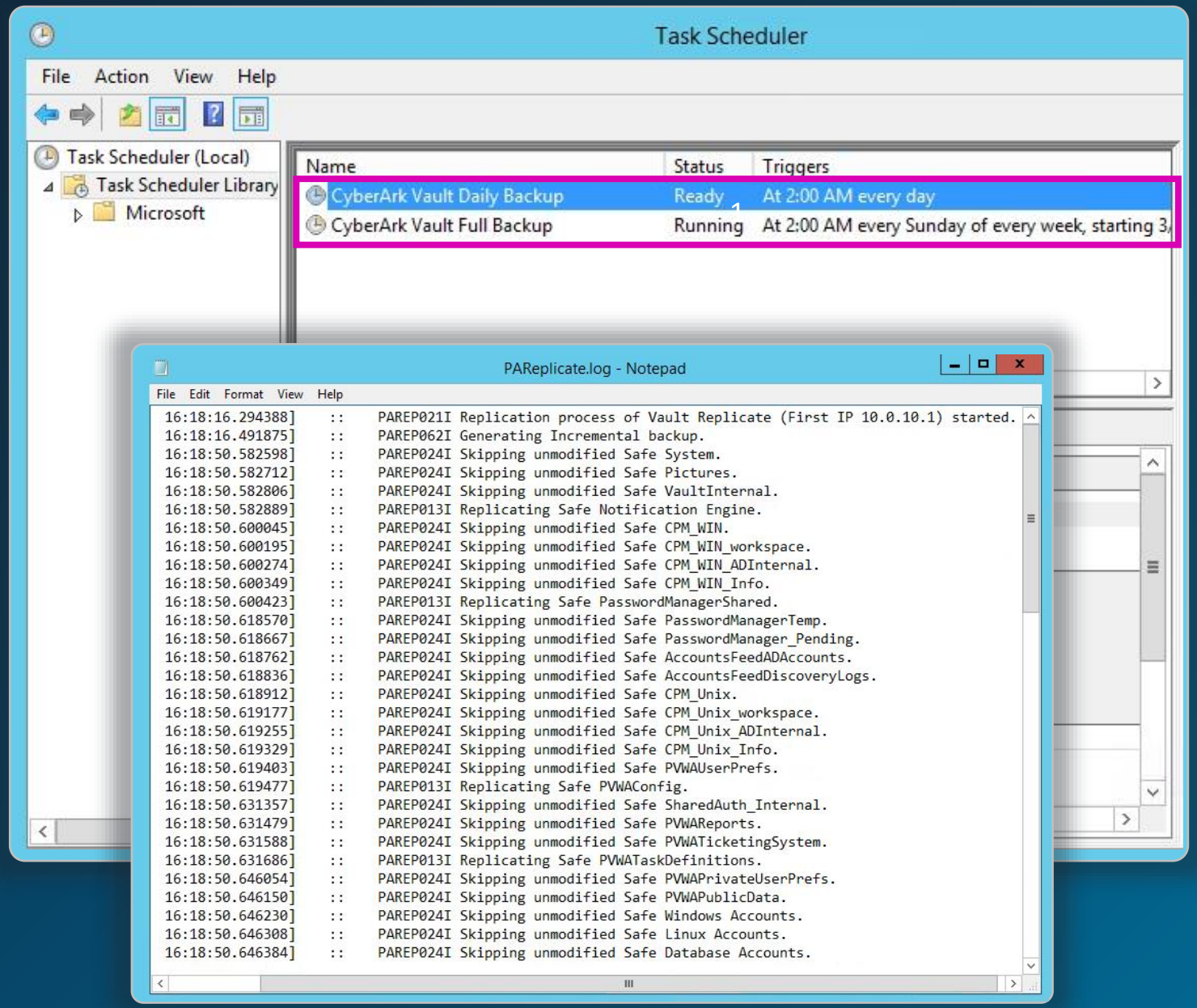

CYBERARK®

Performing Periodic Backups

It is strongly recommended to create **two** Scheduled Tasks:

- One full backup task running every week
- A second one running every day as an incremental backup

Logs can be found in the root of the ***\Replicate*** folder.



CYBERARK®

Summary

CYBERARK®

Summary

In this session we covered:

- Backup and Restore (Replicator utility)
- How to perform backups and restores

CYBERARK®

Exercises

You may now proceed to completing the following exercises:

Backup And Restore

- Configure the CyberArk Replicator Utility
- Run a Backup
- Delete the TEST Safe
- Run a Restore