CYBERARK®

# PAM Administration

## Backup and Restore

CYBERARK®

# Agenda

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

- Describe the Backup and Restore solution
- Test the procedures for **Vault** backup and restore

# Overview

# Replicate Use Cases

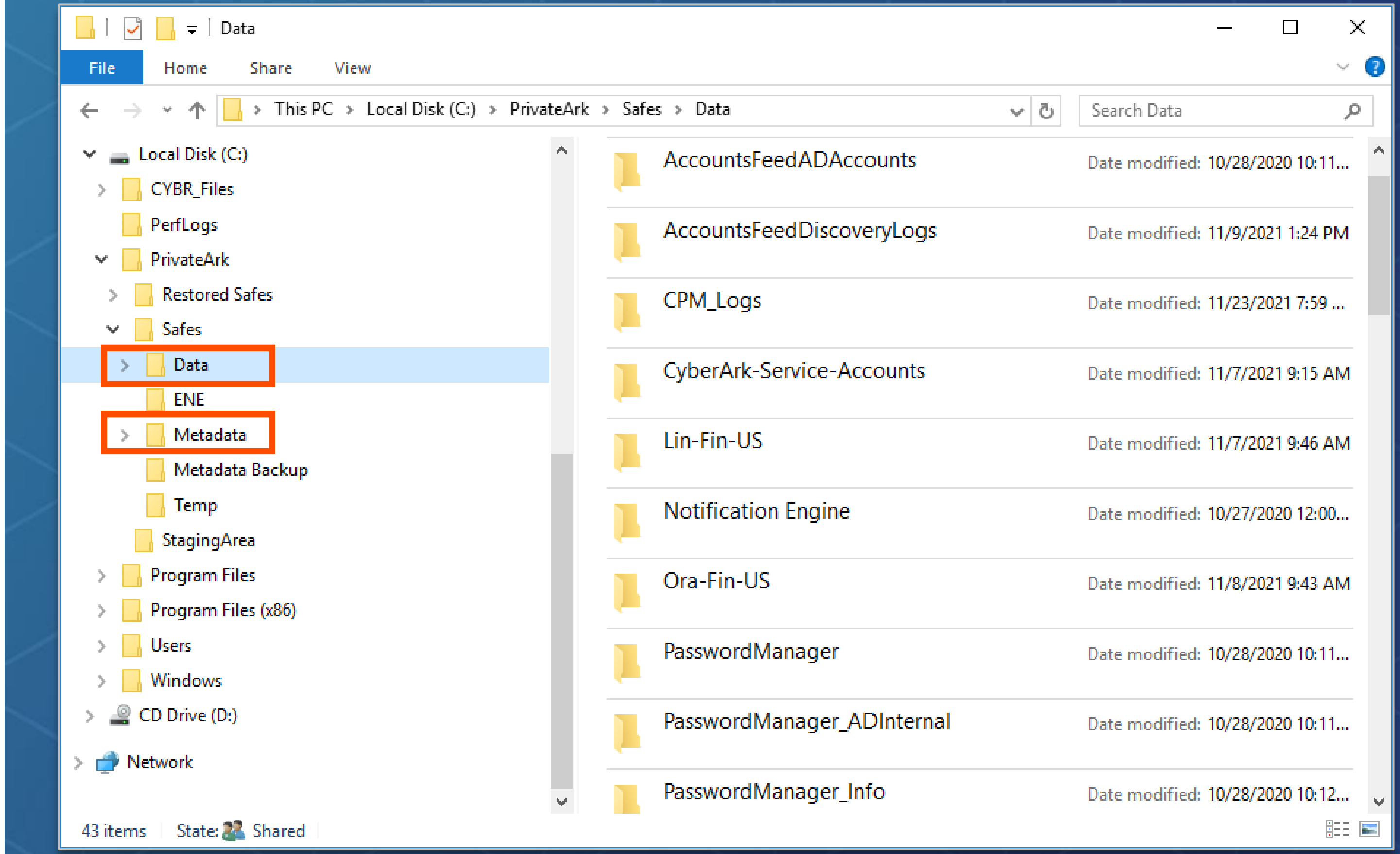
Policy requires integration with an Enterprise Backup Solution.

Policy requires granular point in time data protection.

Policy requires object-level data protection.

# 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



AccountsFeedADAccounts Date modified: 10/28/2020 10:11...
AccountsFeedDiscoveryLogs Date modified: 11/9/2021 1:24 PM
CPM_Logs Date modified: 11/23/2021 7:59 ...
CyberArk-Service-Accounts Date modified: 11/7/2021 9:15 AM
Lin-Fin-US Date modified: 11/7/2021 9:46 AM
Notification Engine Date modified: 10/27/2020 12:00...
Ora-Fin-US Date modified: 11/8/2021 9:43 AM
PasswordManager Date modified: 10/28/2020 10:11...
PasswordManager_ADInternal Date modified: 10/28/2020 10:11...
PasswordManager_Info Date modified: 10/28/2020 10:12...

# 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**

# Replicate Utility

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

# Installation and Setup

# Before Installing

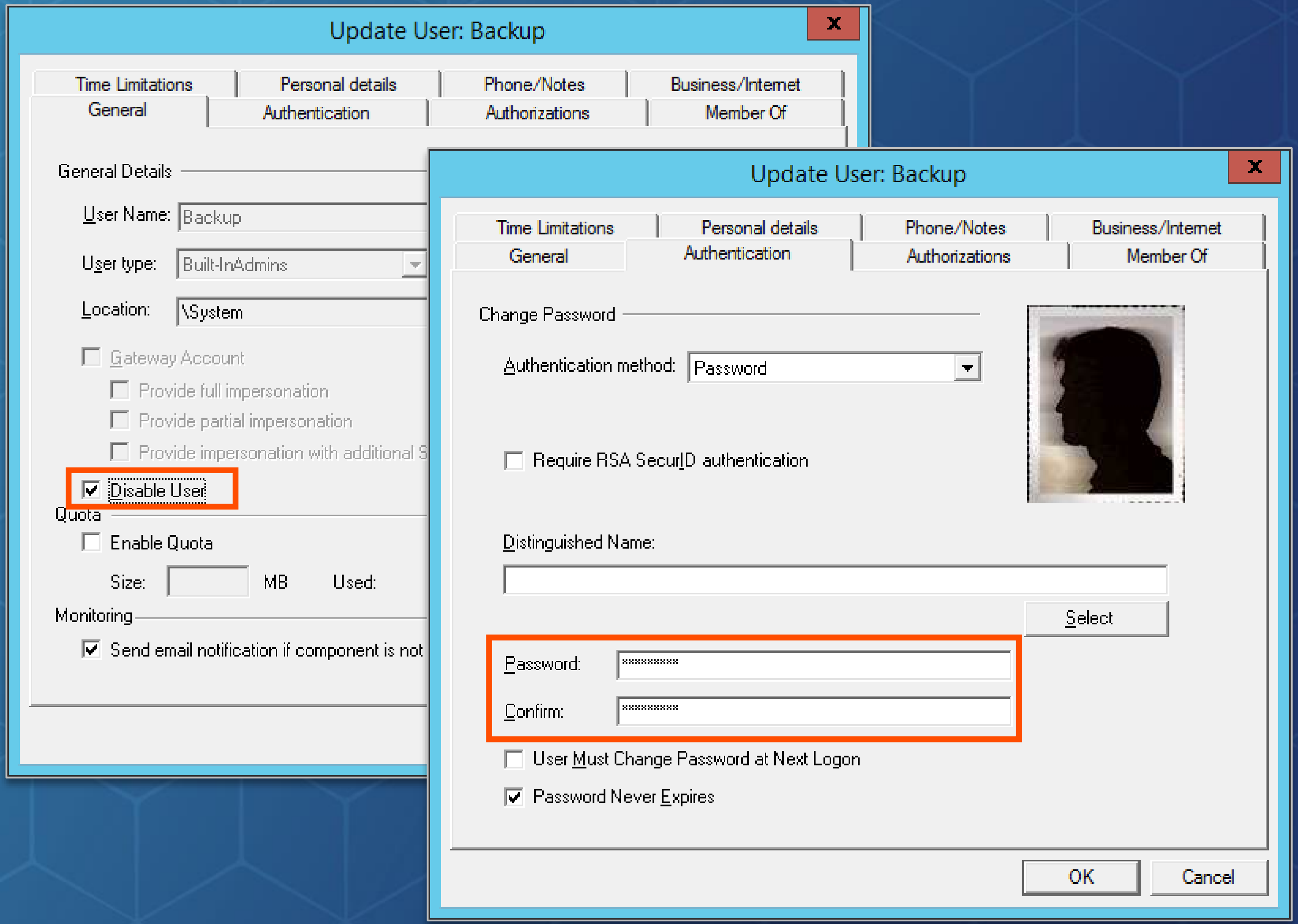
Before installing the **Replicator** utility, make sure that the **backup server** has the following features and capabilities:

- 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

# Before Installing

You will also need to:

- Enable the **Backup** user
- Set the password on the Primary **Vault**



User Name: Backup

User type: Built-InAdmins

Location: \System

☐ Gateway Account

☐ Provide full impersonation

☐ Provide partial impersonation

☐ Provide impersonation with additional S

☑ Disable User

☐ Enable Quota

Size: MB Used:

☑ Send email notification if component is not

Authentication method: Password

☐ Require RSA SecurID authentication

Distinguished Name:

Password: **********

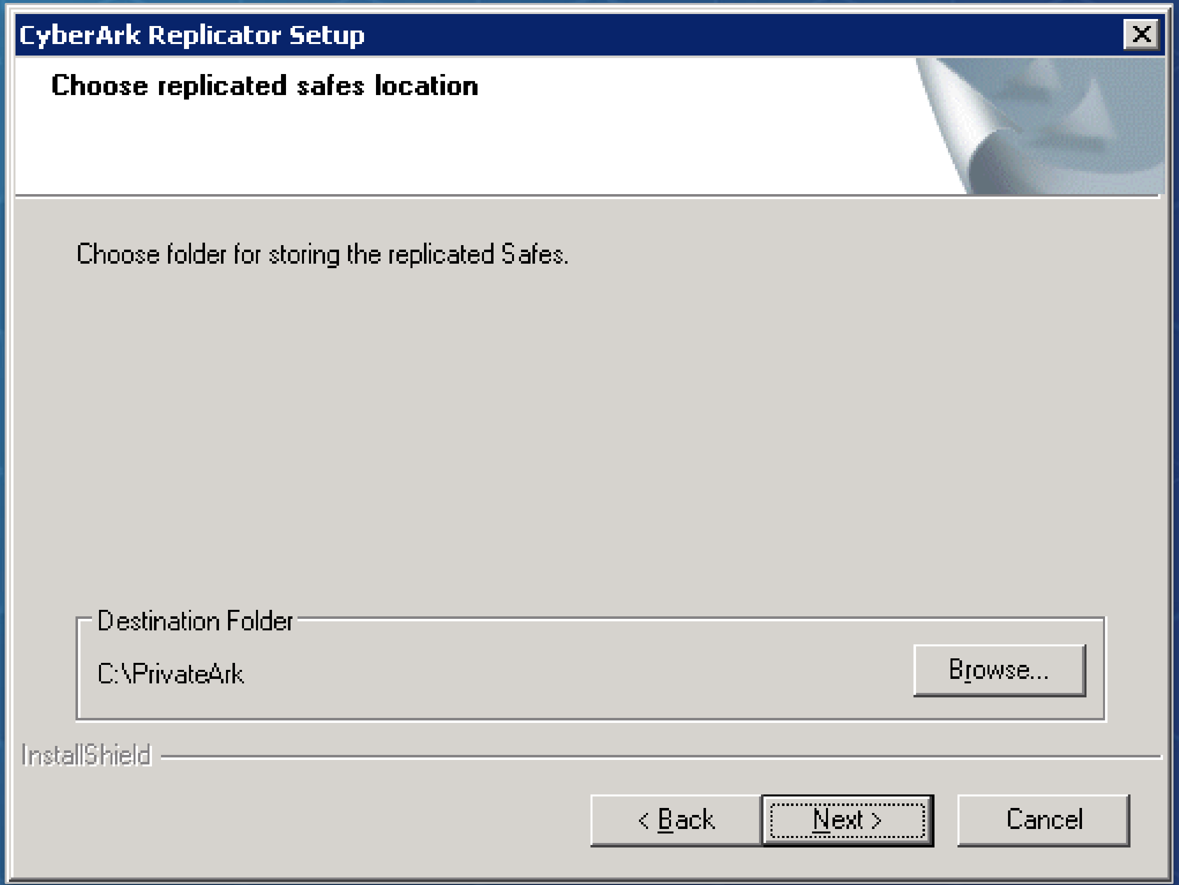
Confirm: **********

☐ User Must Change Password at Next Logon

☑ Password Never Expires

# Install the Utility

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



CyberArk Replicator Setup

Choose replicated safes location

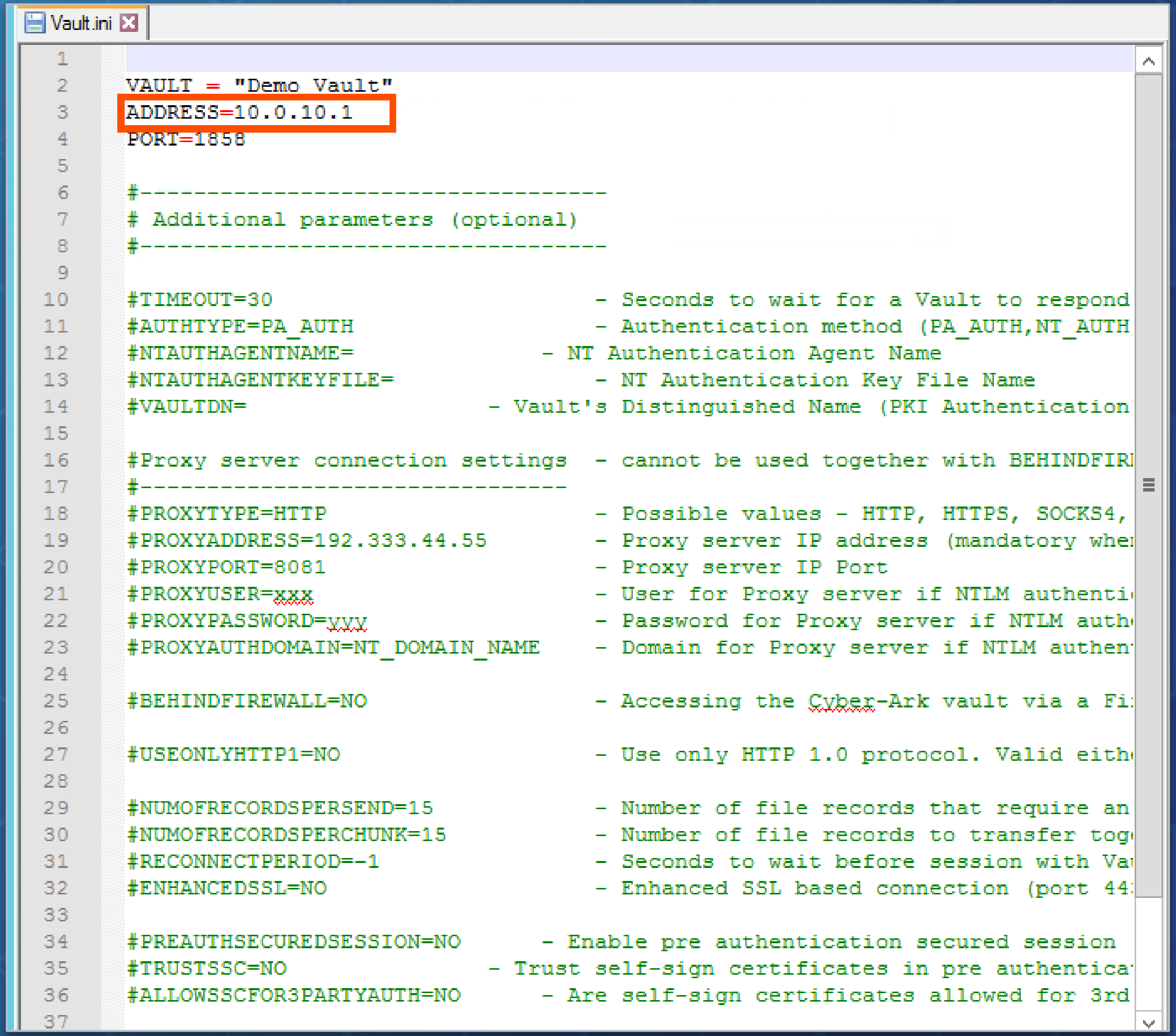
Choose folder for storing the replicated Safes.

Destination Folder

C:\PrivateArk

# Configure vault.ini

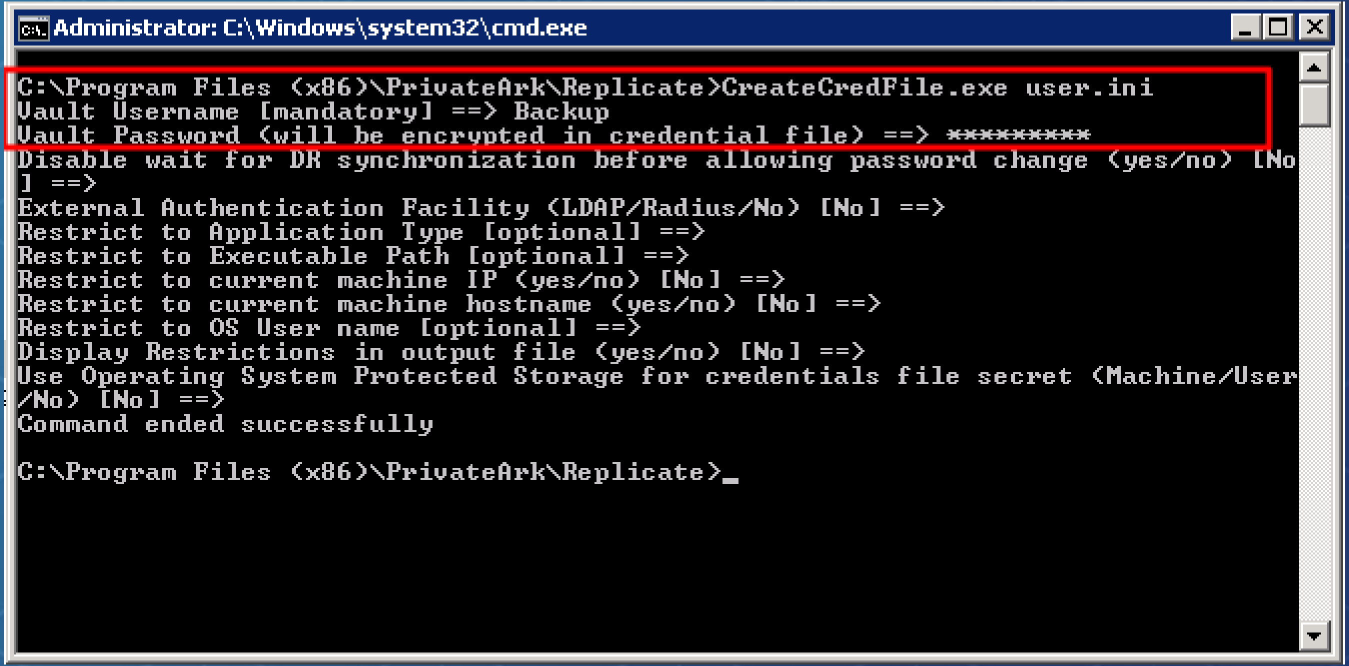
Edit the ***Vault.ini*** to give the **Replicator** utility the network address of the Vault server



```

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

```

# Create cred file

- Create a Credential File for the **Backup** User
- The Credential File is used by the utility to authenticate to the **Vault**
- The password for the Backup user is changed in the **Vault** and the Credential File is updated by the utility at every successful login



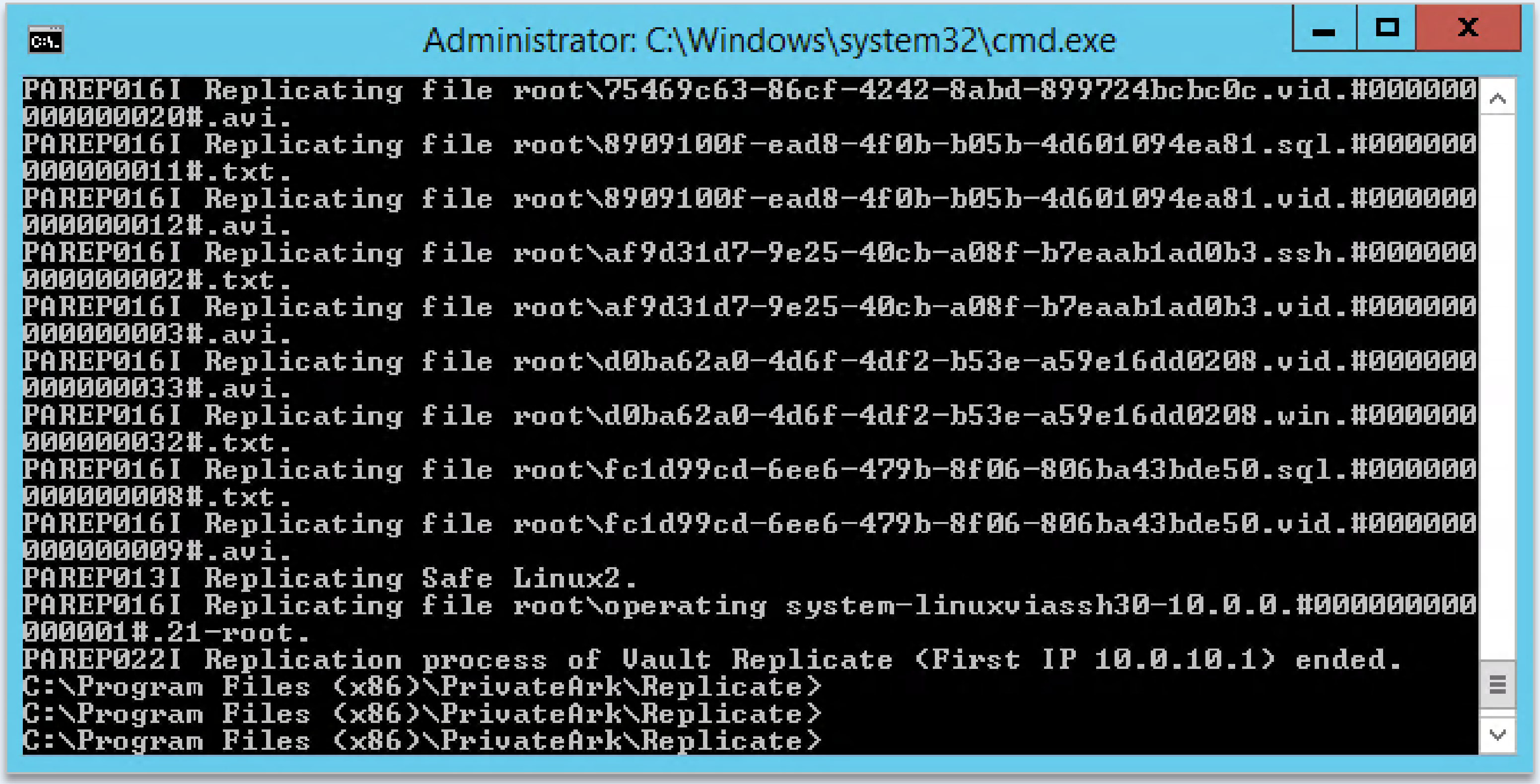
```
C:\Program Files (x86)\PrivateArk\Replicate>CreateCredFile.exe user.ini
Vault Username [mandatory] ==> Backup
Vault Password (will be encrypted in credential file) ==> *********
Disable wait for DR synchronization before allowing password change (yes/no) [No
] ==>
External Authentication Facility (LDAP/Radius/No) [No] ==>
Restrict to Application Type [optional] ==>
Restrict to Executable Path [optional] ==>
Restrict to current machine IP (yes/no) [No] ==>
Restrict to current machine hostname (yes/no) [No] ==>
Restrict to OS User name [optional] ==>
Display Restrictions in output file (yes/no) [No] ==>
Use Operating System Protected Storage for credentials file secret (Machine/User
/No) [No] ==>
Command ended successfully

C:\Program Files (x86)\PrivateArk\Replicate>_
```

# Test Backup and Restore

# 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

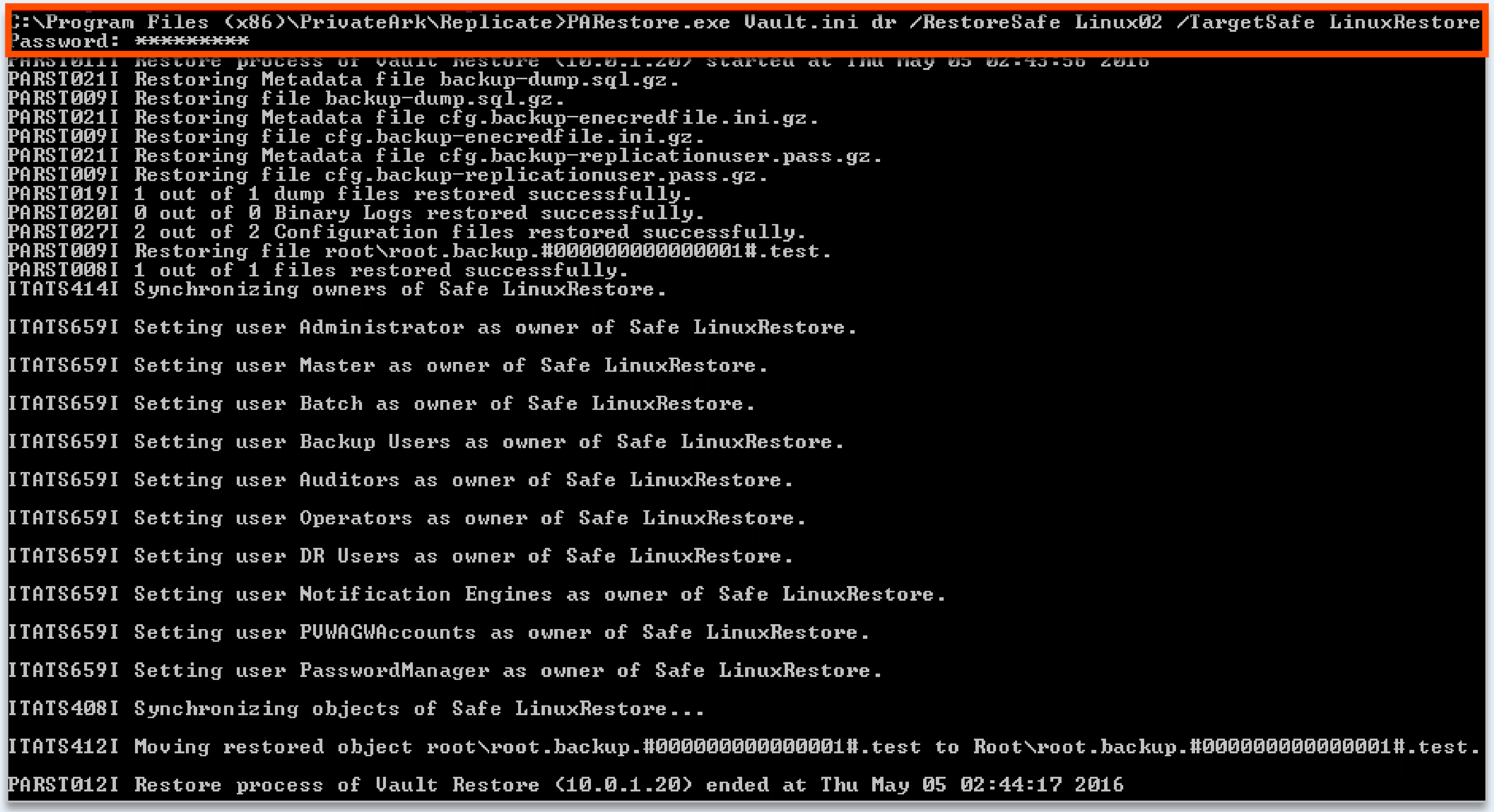


```
PAREP016I Replicating file root\75469c63-86cf-4242-8abd-899724bcbc0c.vid.#000000
000000020#.avi.
PAREP016I Replicating file root\8909100f-ead8-4f0b-b05b-4d601094ea81.sql.#000000
000000011#.txt.
PAREP016I Replicating file root\8909100f-ead8-4f0b-b05b-4d601094ea81.vid.#000000
000000012#.avi.
PAREP016I Replicating file root\af9d31d7-9e25-40cb-a08f-b7eaab1ad0b3.ssh.#000000
000000002#.txt.
PAREP016I Replicating file root\af9d31d7-9e25-40cb-a08f-b7eaab1ad0b3.vid.#000000
000000003#.avi.
PAREP016I Replicating file root\d0ba62a0-4d6f-4df2-b53e-a59e16dd0208.vid.#000000
000000033#.avi.
PAREP016I Replicating file root\d0ba62a0-4d6f-4df2-b53e-a59e16dd0208.win.#000000
000000032#.txt.
PAREP016I Replicating file root\fc1d99cd-6ee6-479b-8f06-806ba43bde50.sql.#000000
000000008#.txt.
PAREP016I Replicating file root\fc1d99cd-6ee6-479b-8f06-806ba43bde50.vid.#000000
000000009#.avi.
PAREP013I Replicating Safe Linux2.
PAREP016I Replicating file root\operating system-linuxviassh30-10.0.0.#000000000
000001#.21-root.
PAREP022I Replication process of Vault Replicate (First IP 10.0.10.1) ended.
C:\Program Files (x86)\PrivateArk\Replicate>
C:\Program Files (x86)\PrivateArk\Replicate>
C:\Program Files (x86)\PrivateArk\Replicate>
```

# Performing a Restore

```
PARestore.exe vault.ini dr /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

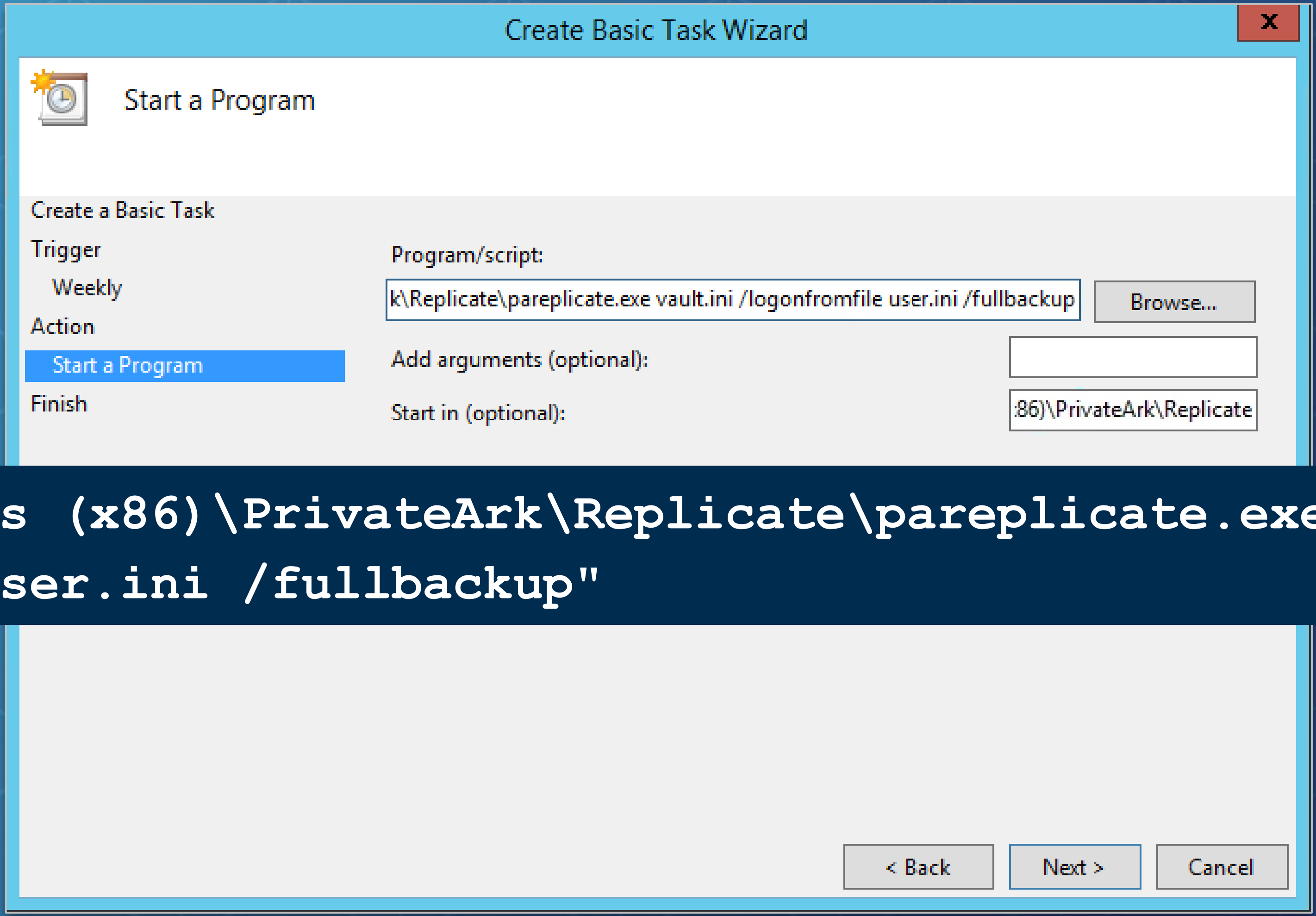


```
C:\Program Files (x86)\PrivateArk\Replicate>PARestore.exe Vault.ini dr /RestoreSafe Linux02 /TargetSafe LinuxRestore
Password: **********
PARST011I Restore process of Vault Restore (10.0.1.20) started at Thu May 05 02:43:56 2016
PARST021I Restoring Metadata file backup-dump.sql.gz.
PARST009I Restoring 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\root.backup.#0000000000000001#.test.
PARST008I 1 out of 1 files restored successfully.
ITATS414I Synchronizing owners of Safe LinuxRestore.

ITATS659I Setting user Administrator as owner of Safe LinuxRestore.

ITATS659I Setting user Master as owner of Safe LinuxRestore.

ITATS659I Setting user Batch as owner of Safe LinuxRestore.

ITATS659I Setting user Backup Users as owner of Safe LinuxRestore.

ITATS659I Setting user Auditors as owner of Safe LinuxRestore.

ITATS659I Setting user Operators as owner of Safe LinuxRestore.

ITATS659I Setting user DR Users as owner of Safe LinuxRestore.

ITATS659I Setting user Notification Engines as owner of Safe LinuxRestore.

ITATS659I Setting user PVWAGWAccounts as owner of Safe LinuxRestore.

ITATS659I Setting user PasswordManager as owner of Safe LinuxRestore.

ITATS408I Synchronizing objects of Safe LinuxRestore...

ITATS412I Moving restored object root\root.backup.#0000000000000001#.test to Root\root.backup.#0000000000000001#.test.

PARST012I Restore process of Vault Restore (10.0.1.20) ended at Thu May 05 02:44:17 2016
```

# Set up Scheduled Backups

# Setup Scheduled Backup

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



Create Basic Task Wizard

Start a Program

Create a Basic Task
Trigger
Weekly
Action
Start a Program
Finish

Program/script: k\Replicate\pareplicate.exe vault.ini /logonfromfile user.ini /fullbackup

Add arguments (optional):

Start in (optional): :86)\PrivateArk\Replicate

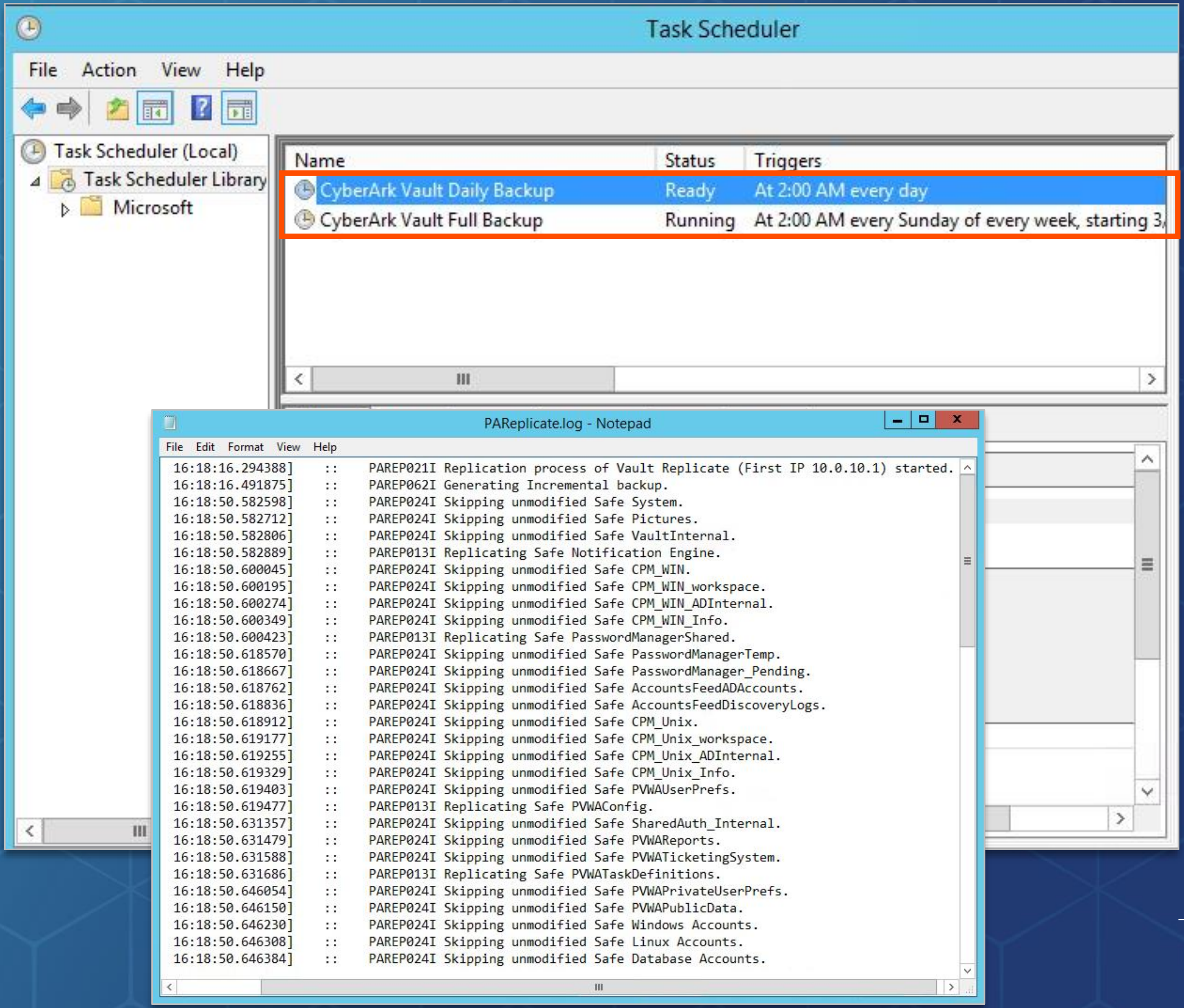
```
"C:\Program Files (x86)\PrivateArk\Replicate\pareplicate.exe vault.ini
/logonfromfile user.ini /fullbackup"
```

# 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.



| Name | Status | Triggers |
|---|---|---|
| CyberArk Vault Daily Backup | Ready | At 2:00 AM every day |
| CyberArk Vault Full Backup | Running | At 2:00 AM every Sunday of every week, starting 3, |

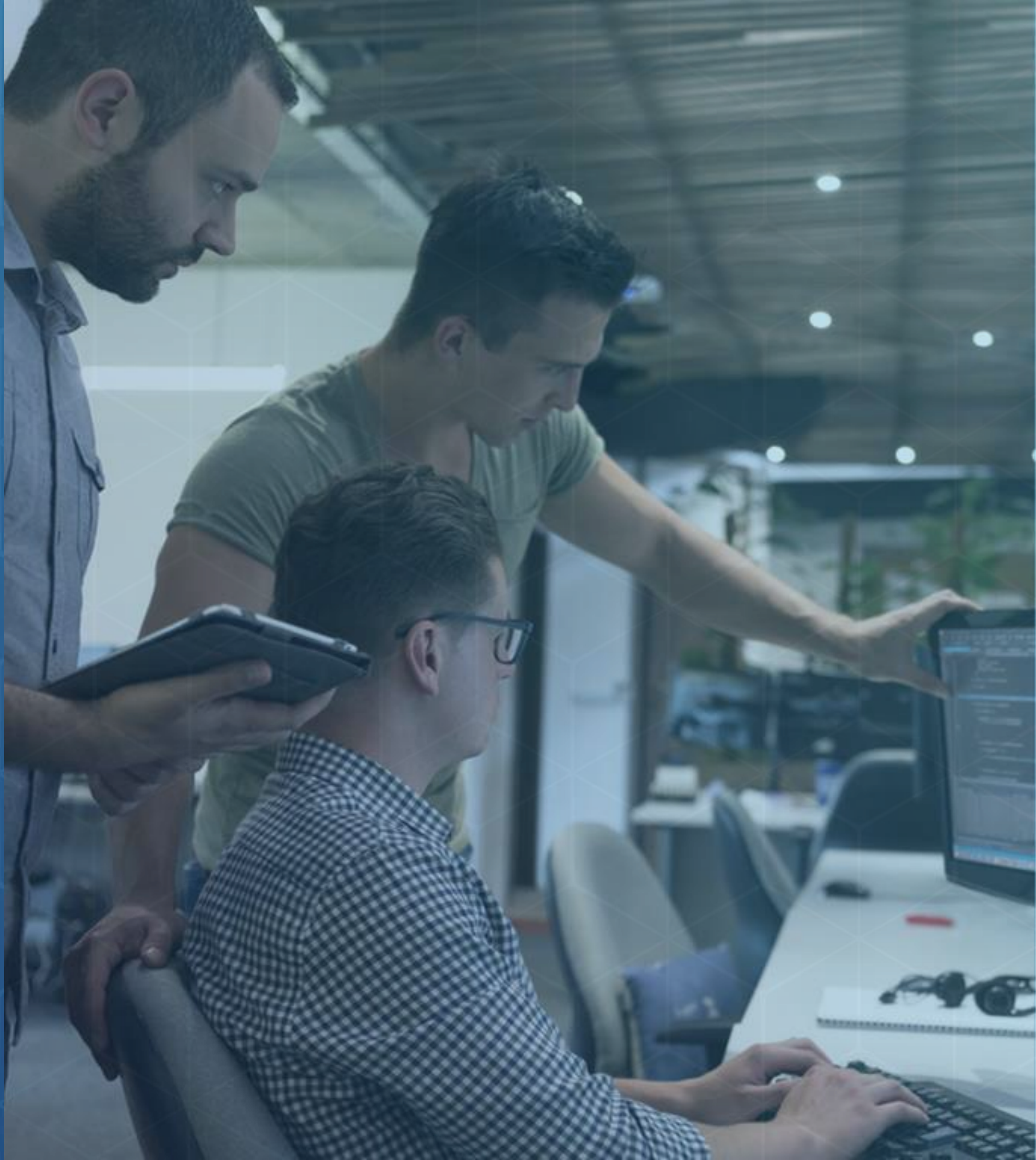
```
16:18:16.294388]    ::    PAREP021I Replication process of Vault Replicate (First IP 10.0.10.1) started.
16:18:16.491875]    ::    PAREP062I Generating Incremental backup.
16:18:50.582598]    ::    PAREP024I Skipping unmodified Safe System.
16:18:50.582712]    ::    PAREP024I Skipping unmodified Safe Pictures.
16:18:50.582806]    ::    PAREP024I Skipping unmodified Safe VaultInternal.
16:18:50.582889]    ::    PAREP013I Replicating Safe Notification Engine.
16:18:50.600045]    ::    PAREP024I Skipping unmodified Safe CPM_WIN.
16:18:50.600195]    ::    PAREP024I Skipping unmodified Safe CPM_WIN_workspace.
16:18:50.600274]    ::    PAREP024I Skipping unmodified Safe CPM_WIN_ADInternal.
16:18:50.600349]    ::    PAREP024I Skipping unmodified Safe CPM_WIN_Info.
16:18:50.600423]    ::    PAREP013I Replicating Safe PasswordManagerShared.
16:18:50.618570]    ::    PAREP024I Skipping unmodified Safe PasswordManagerTemp.
16:18:50.618667]    ::    PAREP024I Skipping unmodified Safe PasswordManager_Pending.
16:18:50.618762]    ::    PAREP024I Skipping unmodified Safe AccountsFeedADAccounts.
16:18:50.618836]    ::    PAREP024I Skipping unmodified Safe AccountsFeedDiscoveryLogs.
16:18:50.618912]    ::    PAREP024I Skipping unmodified Safe CPM_Unix.
16:18:50.619177]    ::    PAREP024I Skipping unmodified Safe CPM_Unix_workspace.
16:18:50.619255]    ::    PAREP024I Skipping unmodified Safe CPM_Unix_ADInternal.
16:18:50.619329]    ::    PAREP024I Skipping unmodified Safe CPM_Unix_Info.
16:18:50.619403]    ::    PAREP024I Skipping unmodified Safe PVWAUserPrefs.
16:18:50.619477]    ::    PAREP013I Replicating Safe PVWAConfig.
16:18:50.631357]    ::    PAREP024I Skipping unmodified Safe SharedAuth_Internal.
16:18:50.631479]    ::    PAREP024I Skipping unmodified Safe PVWAReports.
16:18:50.631588]    ::    PAREP024I Skipping unmodified Safe PVWATicketingSystem.
16:18:50.631686]    ::    PAREP013I Replicating Safe PVWATaskDefinitions.
16:18:50.646054]    ::    PAREP024I Skipping unmodified Safe PVWAPrivateUserPrefs.
16:18:50.646150]    ::    PAREP024I Skipping unmodified Safe PVWAPublicData.
16:18:50.646230]    ::    PAREP024I Skipping unmodified Safe Windows Accounts.
16:18:50.646308]    ::    PAREP024I Skipping unmodified Safe Linux Accounts.
16:18:50.646384]    ::    PAREP024I Skipping unmodified Safe Database Accounts.
```

# Summary

# Summary

In this session we covered:

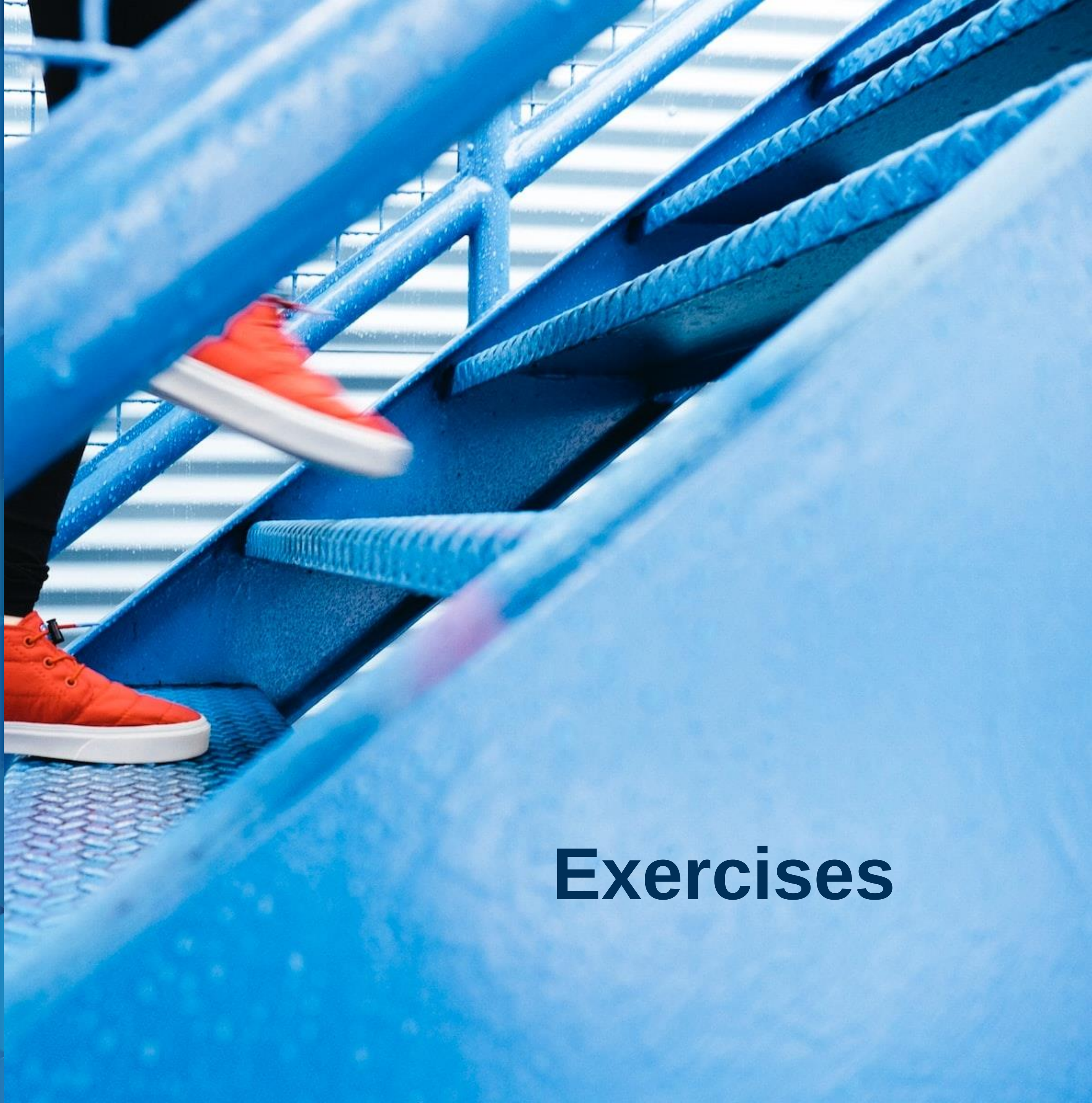
- Backup and Restore (**Replicator** utility)
- How to perform backups and restores



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



# Exercises