



# CYBERARK UNIVERSITY

Vault Availability

Disaster Recovery and the Vault Backup Solution

CyberArk Training

# OBJECTIVES

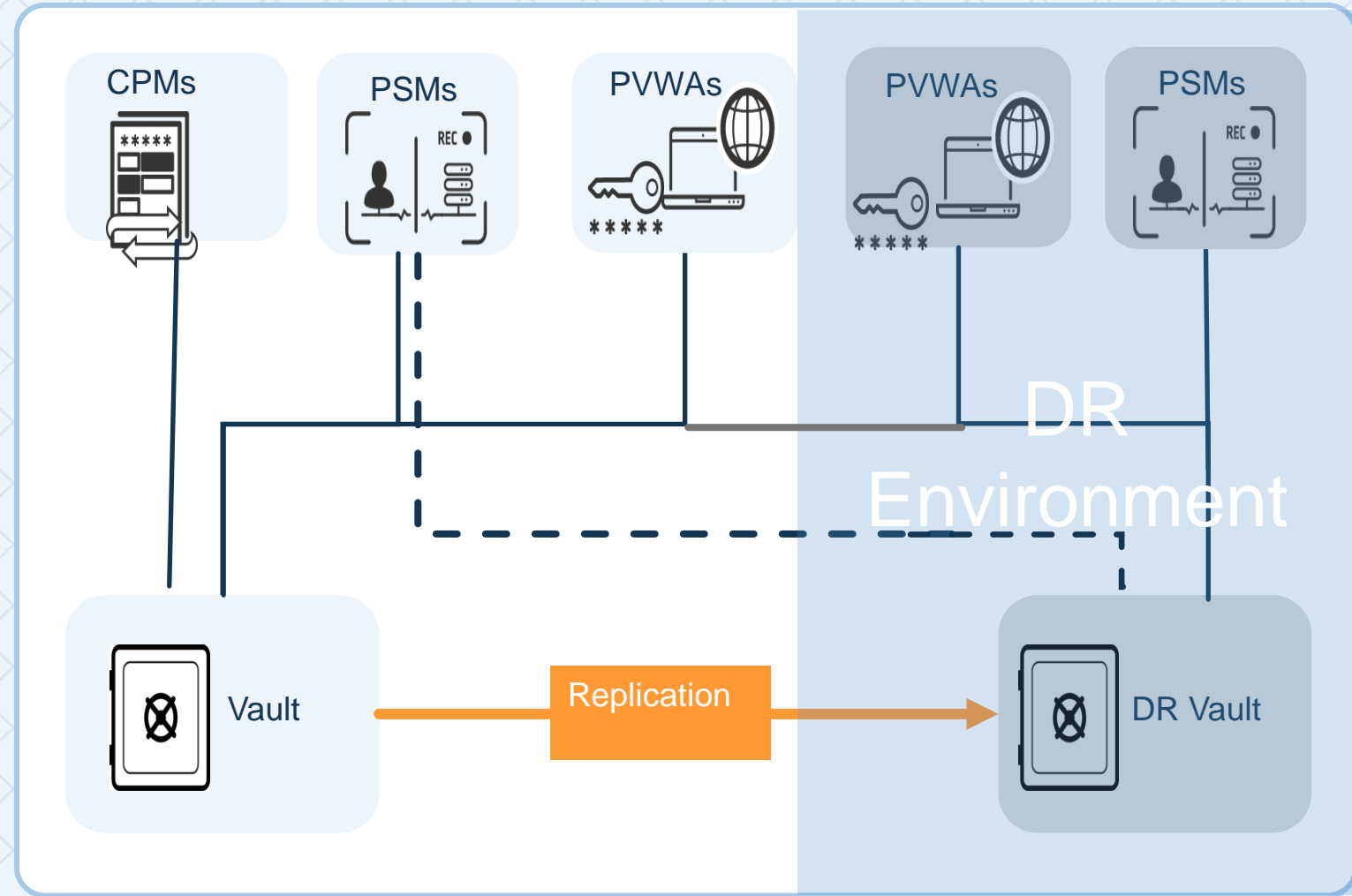
By the end of this lesson, you will be able to:

- Describe the Disaster Recovery and Replicate solutions
- Deploy **Disaster Recovery & Replicator Vault Backup Solution**

# DISASTER RECOVERY OVERVIEW

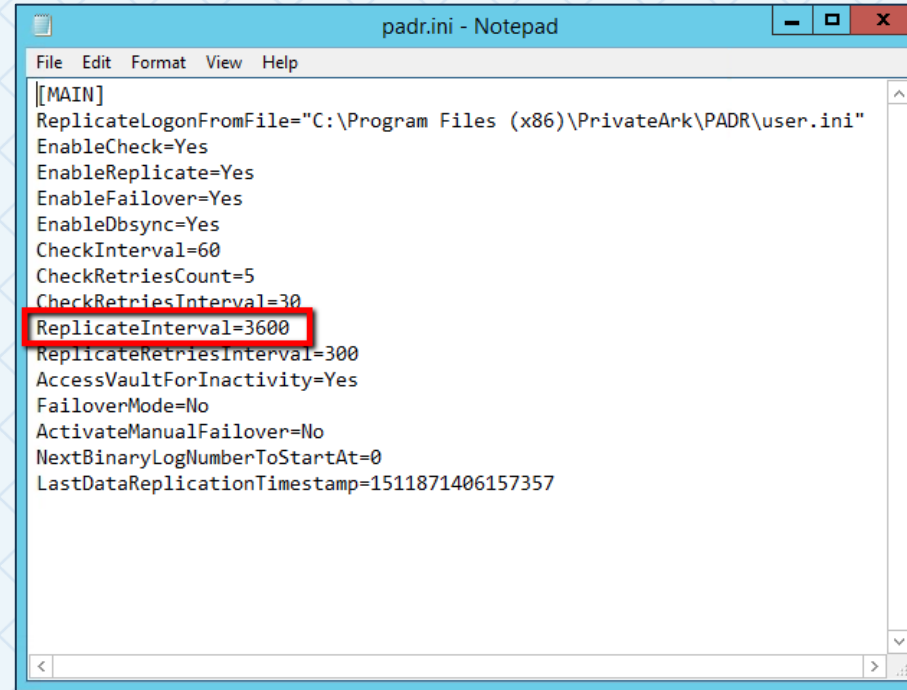
# DISASTER RECOVERY ARCHITECTURE

- The Disaster Recovery vault is a standalone or clustered vault server with an extra software component installed, the Disaster Recovery (DR) service
- The DR Vault must be the same version and use the same Operator and Recovery public Keys used on the Primary Vault
- The DR Service is responsible for replicating data and metadata from the production Vault
- Failover to the DR site can be performed **manually or automatically**

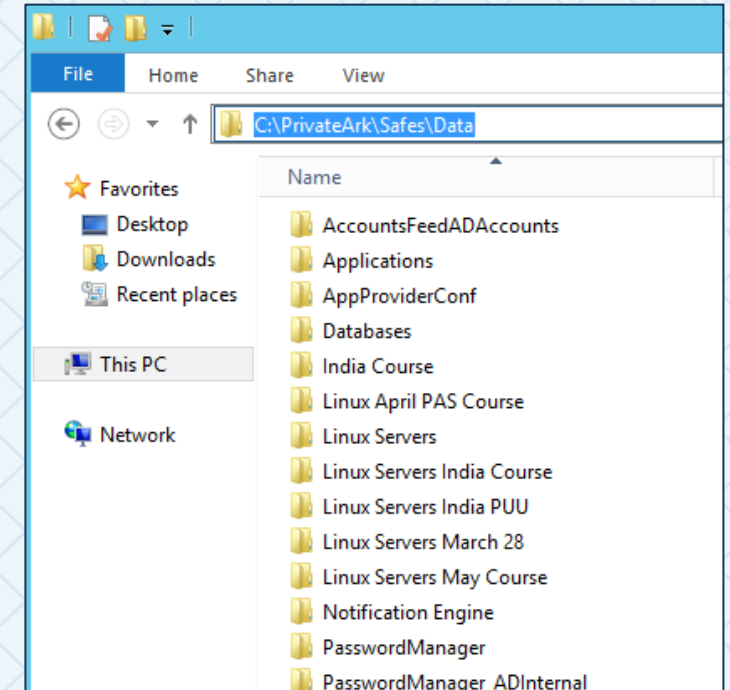


# METADATA REPLICATION

- The DR parameter file determines how frequently the Production Vault will be replicated to the DR Vault
- When setting these parameters, take into consideration that the more frequently a replication is performed, the less chance there is that information will be lost if the Production Vault stops suddenly
- On the other hand, constant replications use Vault resources and may affect other Vault operations
- In PADR.ini, specify the ReplicateInterval parameter sets the minimum time interval in seconds between data replications



```
pdr.ini - Notepad
File Edit Format View Help
[[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR\user.ini"
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=Yes
EnableDbsync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
ActivateManualFailover=No
NextBinaryLogNumberToStartAt=0
LastDataReplicationTimestamp=1511871406157357
```



# ENHANCED DR REPLICATION

- The DR replication process is enhanced to assure faster replication and improved consistency between production and DR sites
- Replicating the accounts information (passwords) to DR sites is immediate and in parallel to files/recordings (metadata) replication in order to avoid delays
- Events are pushed from the production Vault to the DR sites as they happen





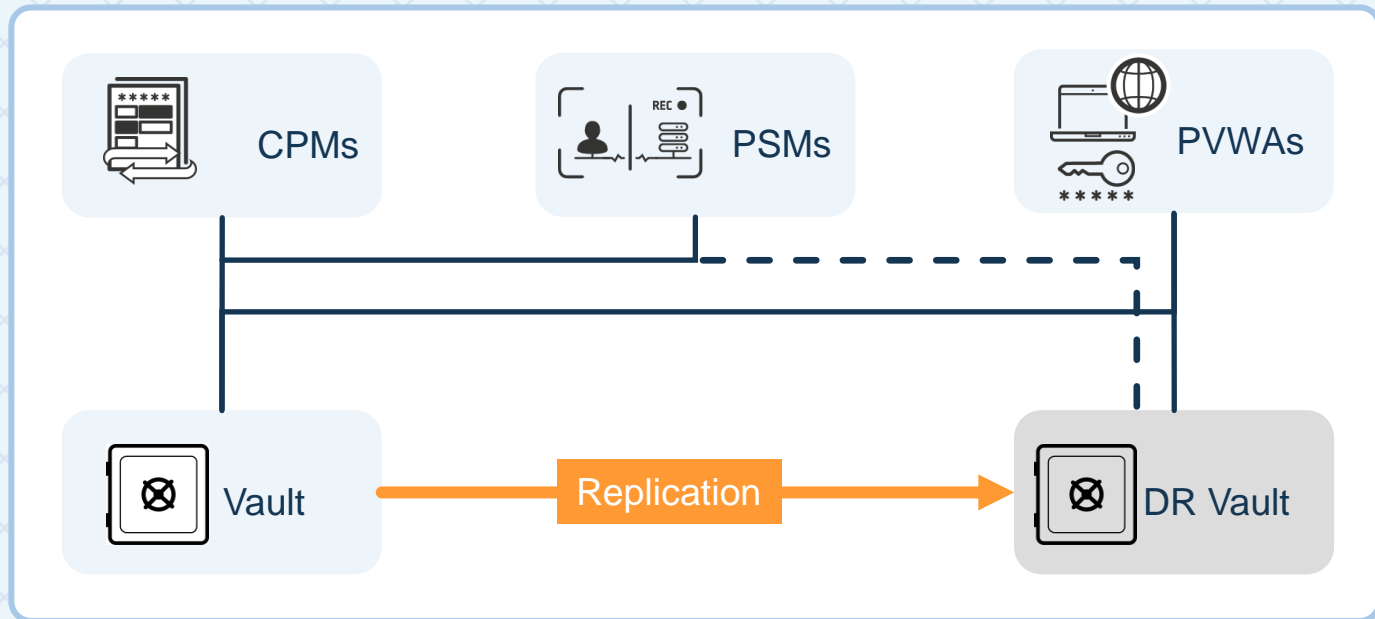
# FAILOVER PROCESS: DISASTER RECOVERY COMPONENT

- When a failover is initiated the Disaster Recovery component will
  - Start the PrivateArk Server service
  - Start the CyberArk Event Notification Engine service
  - Stop the CyberArk Disaster Recovery service
- View the contrast in settings and services as described in the table shown here

<u>Windows Services</u>	<u>Normal Mode</u>	<u>Failover Mode</u>
CyberArk Disaster Recovery	Started	Stopped
PrivateArk Server	Stopped	Running
Event Notification Engine	Stopped	Running
	PADR.ini FailoverMode=No	PADR.ini FailoverMode=Yes

# FAILOVER PROCESS: COMPONENTS

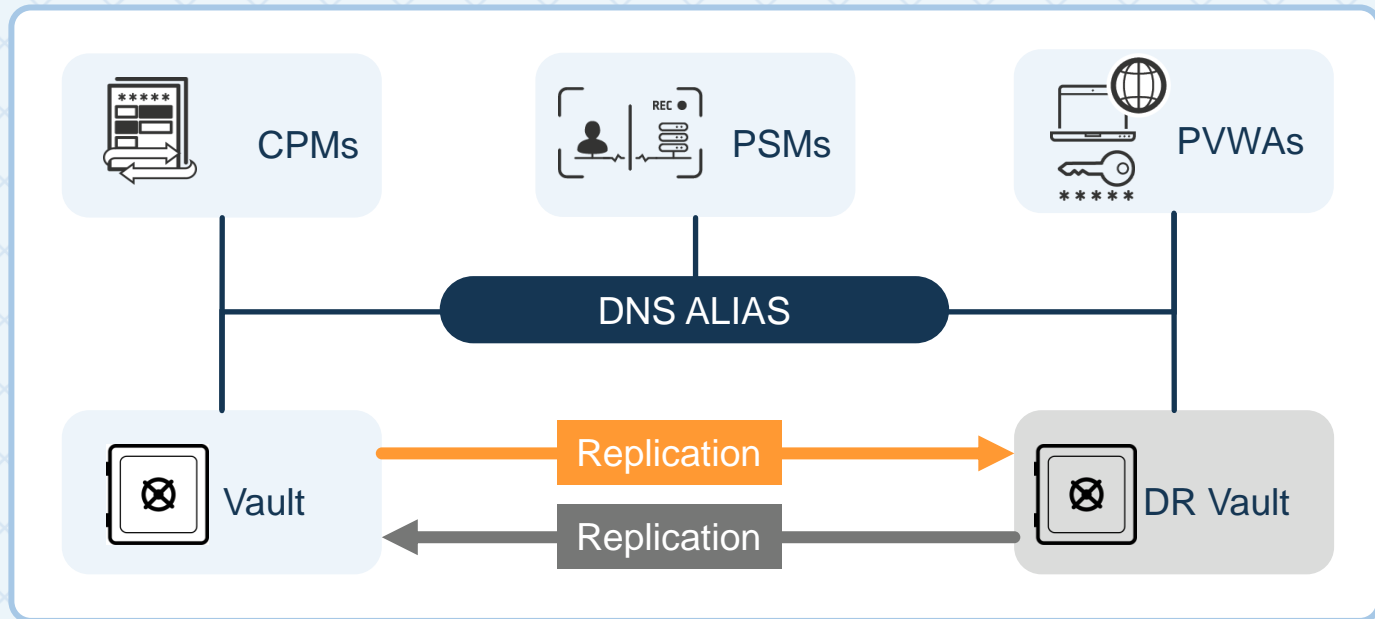
- CPMs should **NEVER** be configured for automatic failover due to the possibility of a split brain scenario
- PVWAs can be configured for automatic failover to allow users to access passwords without interruption
- Consult with CyberArk services to review PSM failover options





# FAILOVER PROCESS: COMPONENTS

- A possible approach to avoiding split brain, is to use a DNS Alias for the vault to control which vault is used by the components
- Data generated on the DR Vault can be replicated from the DR Vault to the Primary Vault before bringing the Primary Vault back online
- DNS name changes and failback replication are manual processes and may extend the outage



# DISASTER RECOVERY INSTALLATION

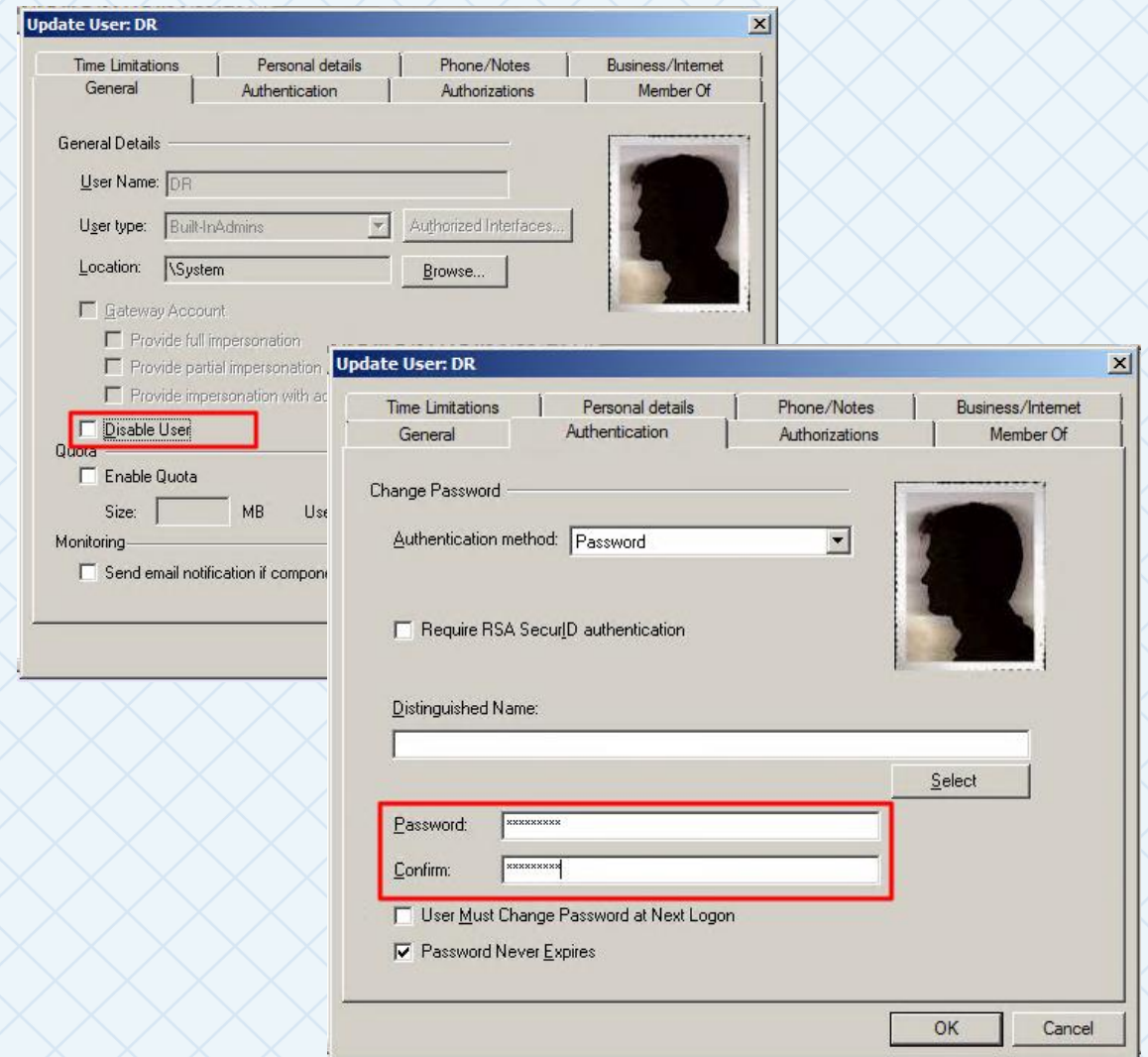
# DISASTER RECOVERY VAULT PREREQUISITES

- A physical vault server with identical requirements to the primary vault
- CyberArk Vault software version must be the same exact version as the primary vault
- The same Operator Keys must be used on the DR Vault that were used on the primary vault
- A CyberArk license.xml file for DR must also be copied locally to the DR server.



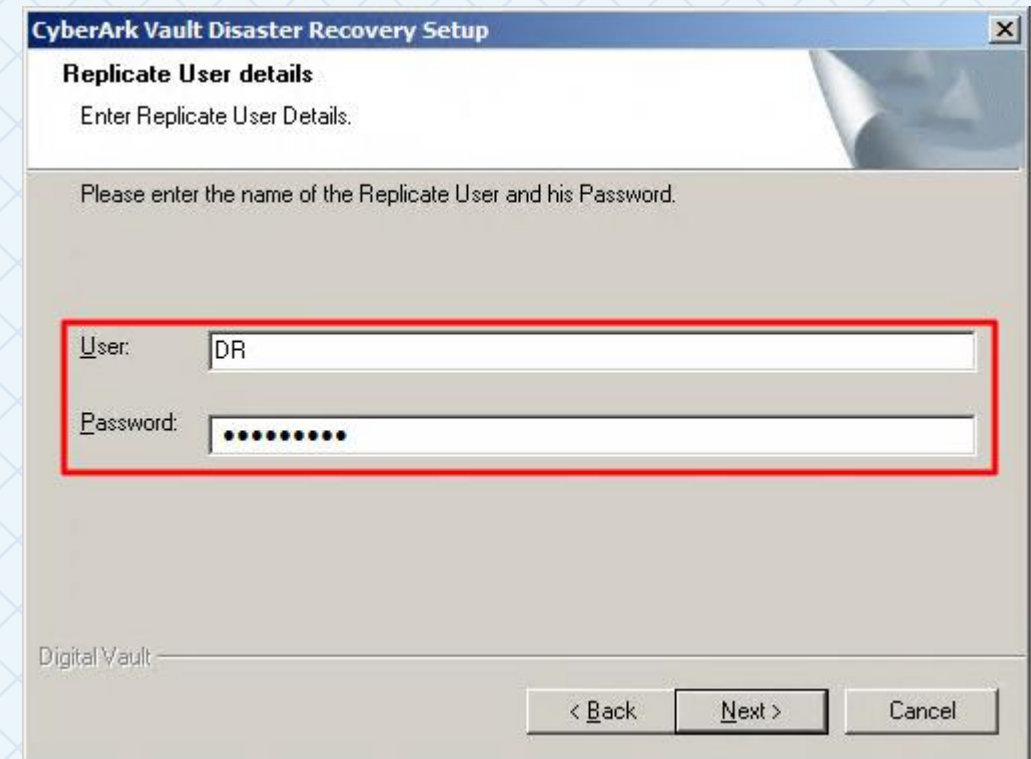
# DISASTER RECOVERY INSTALL PROCESS

- The Disaster Recovery User (DR User) is a predefined User that is added automatically as an Owner to every Safe, and only has the access rights required to replicate the Safes
- Enable the DR user on the Primary Vault and set a password



# DISASTER RECOVERY INSTALL PROCESS

- Install the CyberArk Disaster Recovery software on the DR Vault
- When prompted for the Replicate User Details, provide the DR Username and password that you set for the DR user in the PrivateArk Client

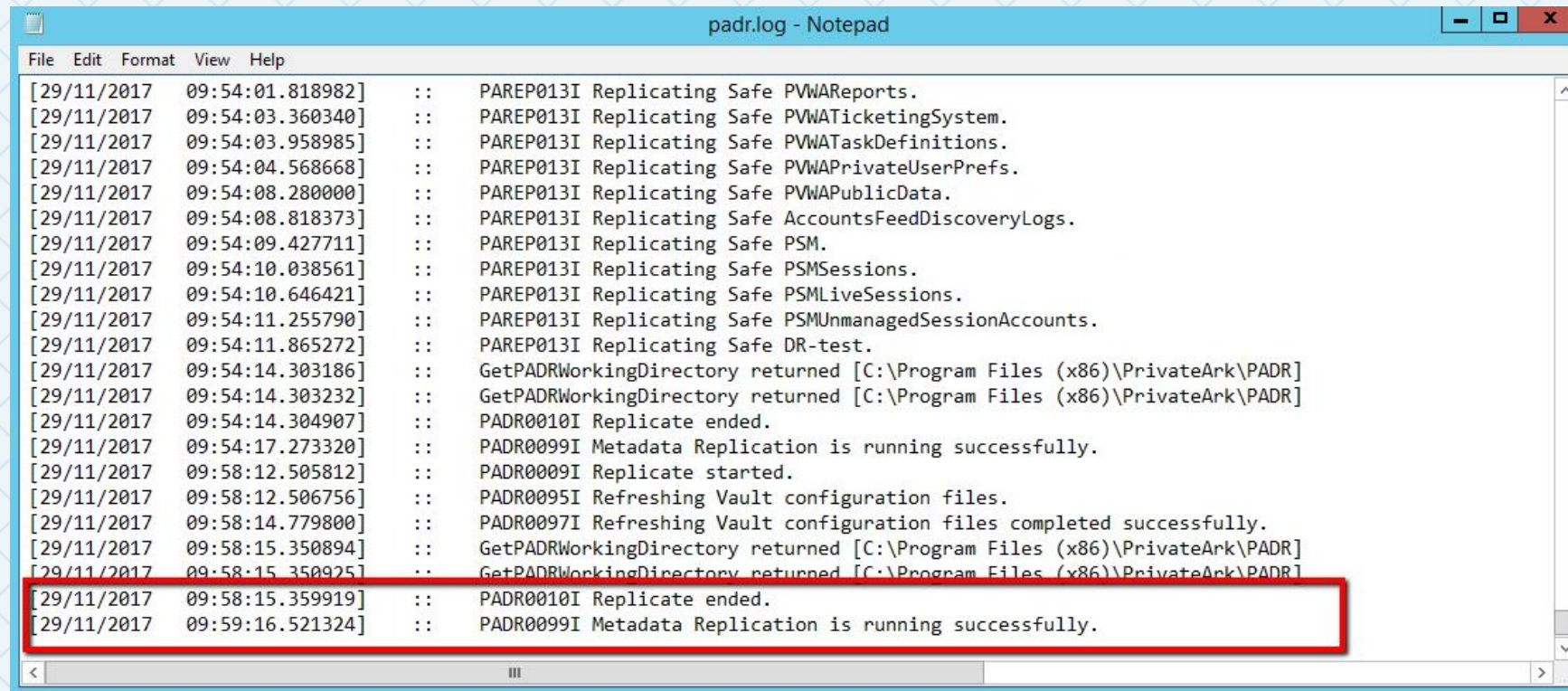


The screenshot shows a Windows-style dialog box titled "CyberArk Vault Disaster Recovery Setup". Inside, the section "Replicate User details" is active, with the instruction "Enter Replicate User Details." and a sub-instruction "Please enter the name of the Replicate User and his Password." Below this, there are two input fields: "User:" with the text "DR" entered, and "Password:" with a masked password represented by ten dots. A red rectangular box highlights both input fields. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel". The "Digital Vault" logo is visible in the bottom left corner of the dialog area.



# DISASTER RECOVERY INSTALL PROCESS

Restart the DR Vault and verify that data replication ended successfully, and that the Metadata replication is running (PADR.log)

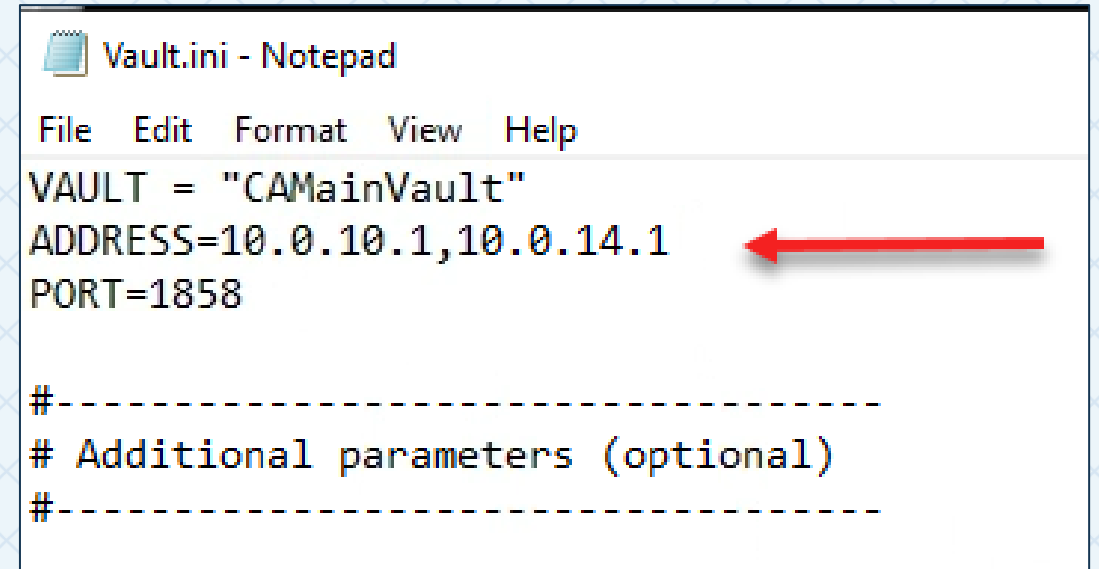


```
pdr.log - Notepad
File Edit Format View Help
[29/11/2017 09:54:01.818982] :: PAREP013I Replicating Safe PVWReports.
[29/11/2017 09:54:03.360340] :: PAREP013I Replicating Safe PVWATicketingSystem.
[29/11/2017 09:54:03.958985] :: PAREP013I Replicating Safe PVWATaskDefinitions.
[29/11/2017 09:54:04.568668] :: PAREP013I Replicating Safe PVWAPrivateUserPrefs.
[29/11/2017 09:54:08.280000] :: PAREP013I Replicating Safe PVWAPublicData.
[29/11/2017 09:54:08.818373] :: PAREP013I Replicating Safe AccountsFeedDiscoveryLogs.
[29/11/2017 09:54:09.427711] :: PAREP013I Replicating Safe PSM.
[29/11/2017 09:54:10.038561] :: PAREP013I Replicating Safe PSM Sessions.
[29/11/2017 09:54:10.646421] :: PAREP013I Replicating Safe PSM LiveSessions.
[29/11/2017 09:54:11.255790] :: PAREP013I Replicating Safe PSMUnmanagedSessionAccounts.
[29/11/2017 09:54:11.865272] :: PAREP013I Replicating Safe DR-test.
[29/11/2017 09:54:14.303186] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 09:54:14.303232] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 09:54:14.304907] :: PADR0010I Replicate ended.
[29/11/2017 09:54:17.273320] :: PADR0099I Metadata Replication is running successfully.
[29/11/2017 09:58:12.505812] :: PADR0009I Replicate started.
[29/11/2017 09:58:12.506756] :: PADR0095I Refreshing Vault configuration files.
[29/11/2017 09:58:14.779800] :: PADR0097I Refreshing Vault configuration files completed successfully.
[29/11/2017 09:58:15.350894] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 09:58:15.350925] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 09:58:15.359919] :: PADR0010I Replicate ended.
[29/11/2017 09:59:16.521324] :: PADR0099I Metadata Replication is running successfully.
```



# CONFIGURE PVWA/PSM COMPONENTS

- For high availability implementations and Disaster Recovery you can specify more than one Vault IP address in the vault.ini file of PVWA and PSM servers
- If these components cannot access the first Vault IP address, they will automatically try to access the next Vault IP address
- To enter multiple Vault IP addresses:
  - In the Vault.ini file, in the Address parameter, enter each Vault IP address separated by a comma
- There is no limit to the number of IP addresses that you can specify



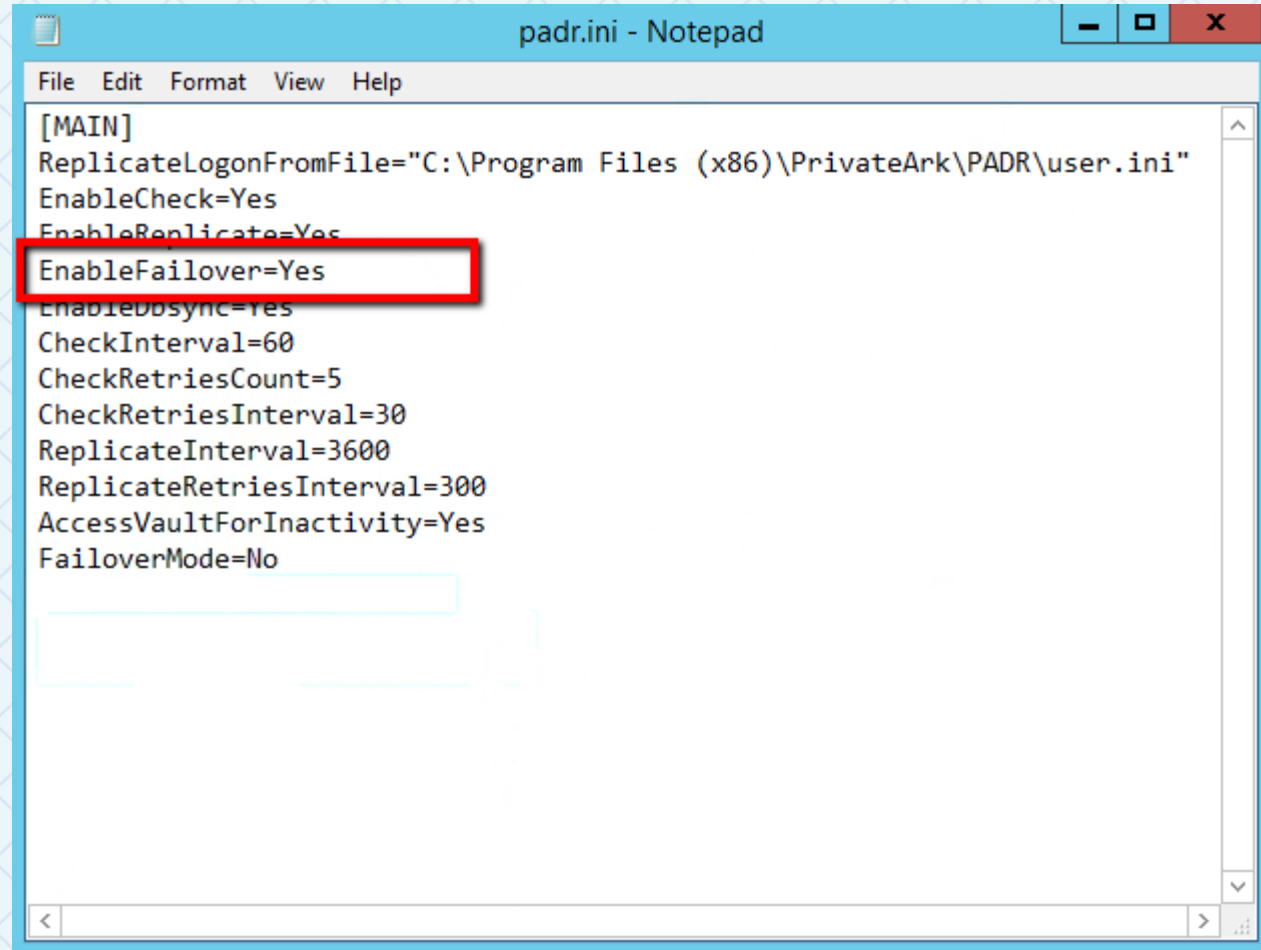
```
Vault.ini - Notepad
File Edit Format View Help
VAULT = "CAMainVault"
ADDRESS=10.0.10.1,10.0.14.1
PORT=1858

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

# DISASTER RECOVERY AUTOMATIC FAILOVER

# TEST AUTOMATIC FAILOVER

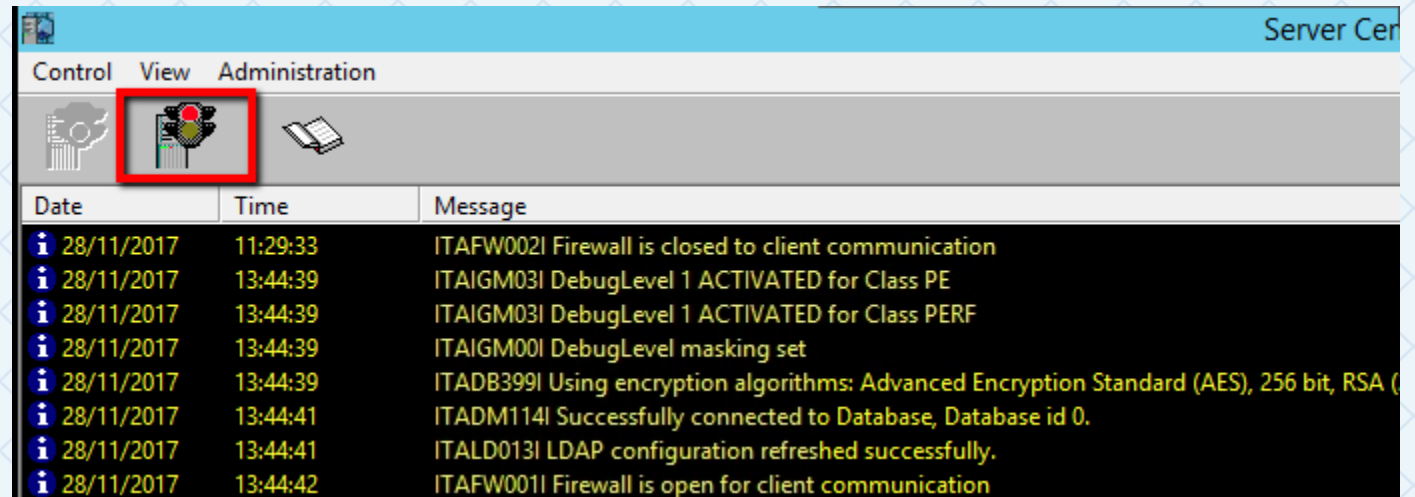
- A failover process is initiated when the DR Vault loses communication with the Production Vault for any reason
- To enable automatic failover confirm **EnableFailover=yes** in the PADR.ini (default)
- The parameter CheckRetriesCount= determines how many times the DR server will retry after a failure
- The parameter CheckInterval= determines how long to wait between checks



```
padr.ini - Notepad
File Edit Format View Help
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR\user.ini"
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=Yes
EnableObsync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
```

# TEST AUTOMATIC FAILOVER

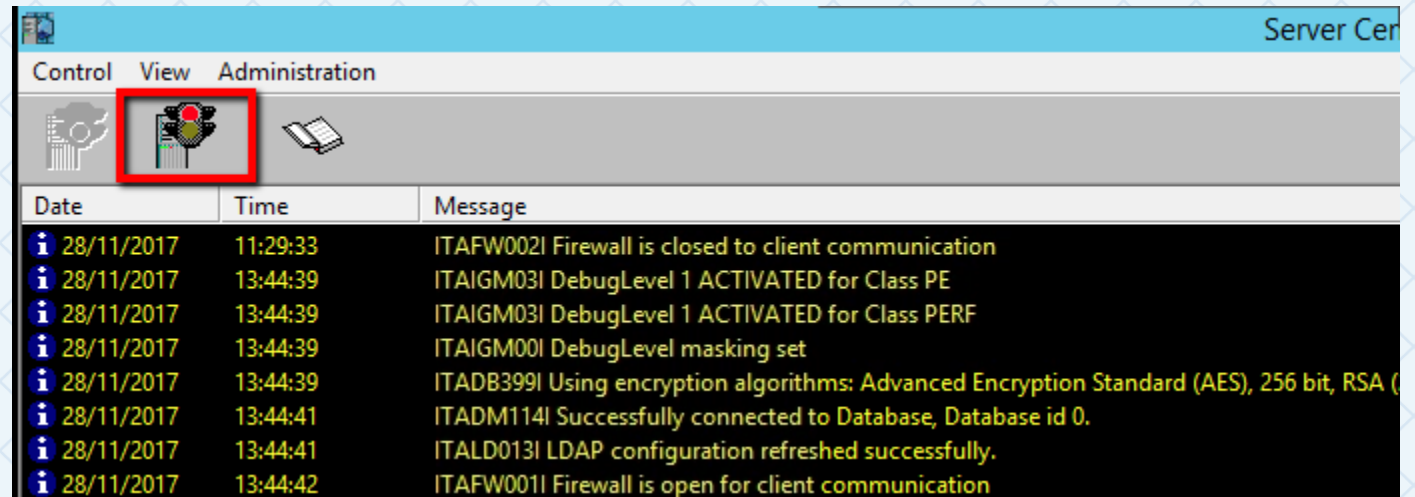
- The Primary Vault will respond to ICMP messages on the network, as long as the PrivateArk Server service is running
- The DR Vault monitors the Primary Vault status 1 of 2 ways. Via ICMP or the DR user will try to initiate Vault activity (default)
- This setting is configured in the PADR.INI file with parameter *AccessVaultForInactivity=Yes*, to initiate Vault activity
- Update the vault to No to use ICMP



Control View Administration		
Date	Time	Message
28/11/2017	11:29:33	ITAFW002I Firewall is closed to client communication
28/11/2017	13:44:39	ITAIGM03I DebugLevel 1 ACTIVATED for Class PE
28/11/2017	13:44:39	ITAIGM03I DebugLevel 1 ACTIVATED for Class PERF
28/11/2017	13:44:39	ITAIGM00I DebugLevel masking set
28/11/2017	13:44:39	ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit, RSA (
28/11/2017	13:44:41	ITADM114I Successfully connected to Database, Database id 0.
28/11/2017	13:44:41	ITALD013I LDAP configuration refreshed successfully.
28/11/2017	13:44:42	ITAFW001I Firewall is open for client communication

# TEST AUTOMATIC FAILOVER

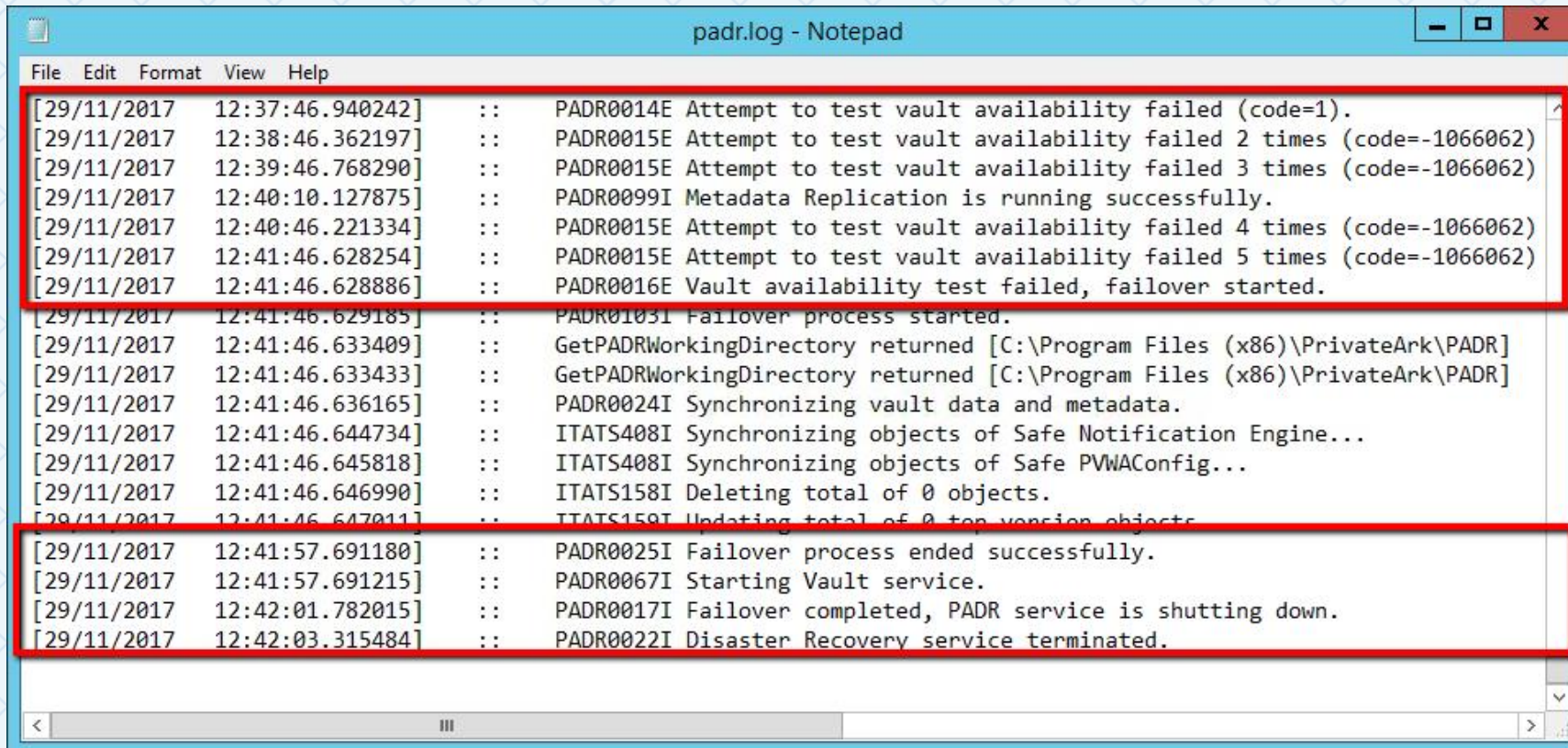
- To initiate an Automatic failover, stop the PrivateArk Server Service on the Primary Server and wait 5 minutes





# TEST AUTOMATIC FAILOVER

Monitor the progress of the test by opening the PADR.LOG file and you can confirm that the DR Vault is testing the Primary Vaults availability, corresponding to the parameters set in the PADR.INI file



```
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 PWVACongfig...
[29/11/2017 12:41:46.646990] :: ITATS158I Deleting total of 0 objects.
[29/11/2017 12:41:46.647011] :: ITATS158I 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.
```



# DISASTER RECOVERY MANUAL FAILOVER

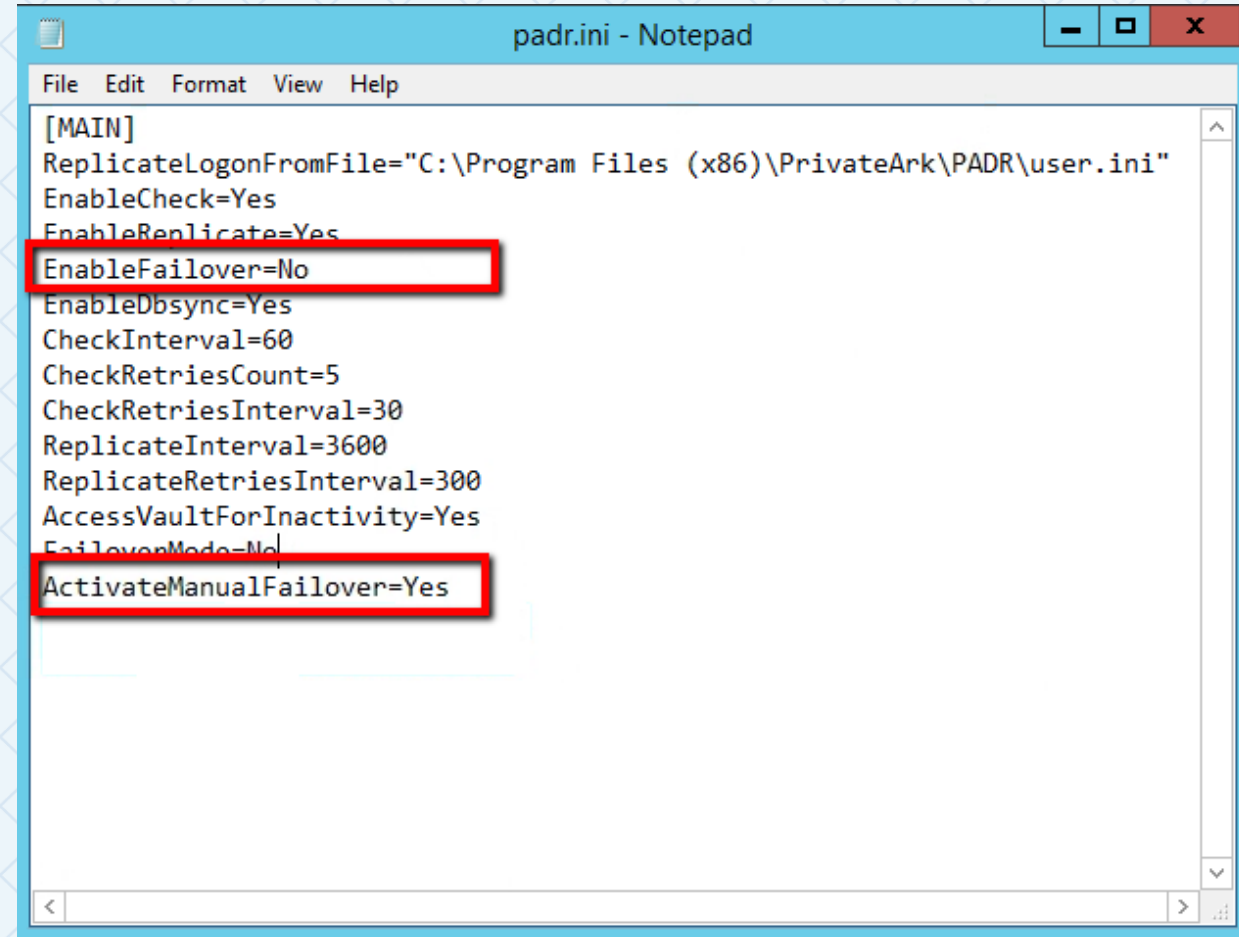
# INITIATE A MANUAL DR FAILOVER

## Edit PADR.INI

- set EnableFailover to **No**
- EnableDBSync parameter to Yes
- ActivateManualFailover to **Yes**
- Restart the CyberArk Vault Disaster Recovery service

DR failover then automatically runs the following process:

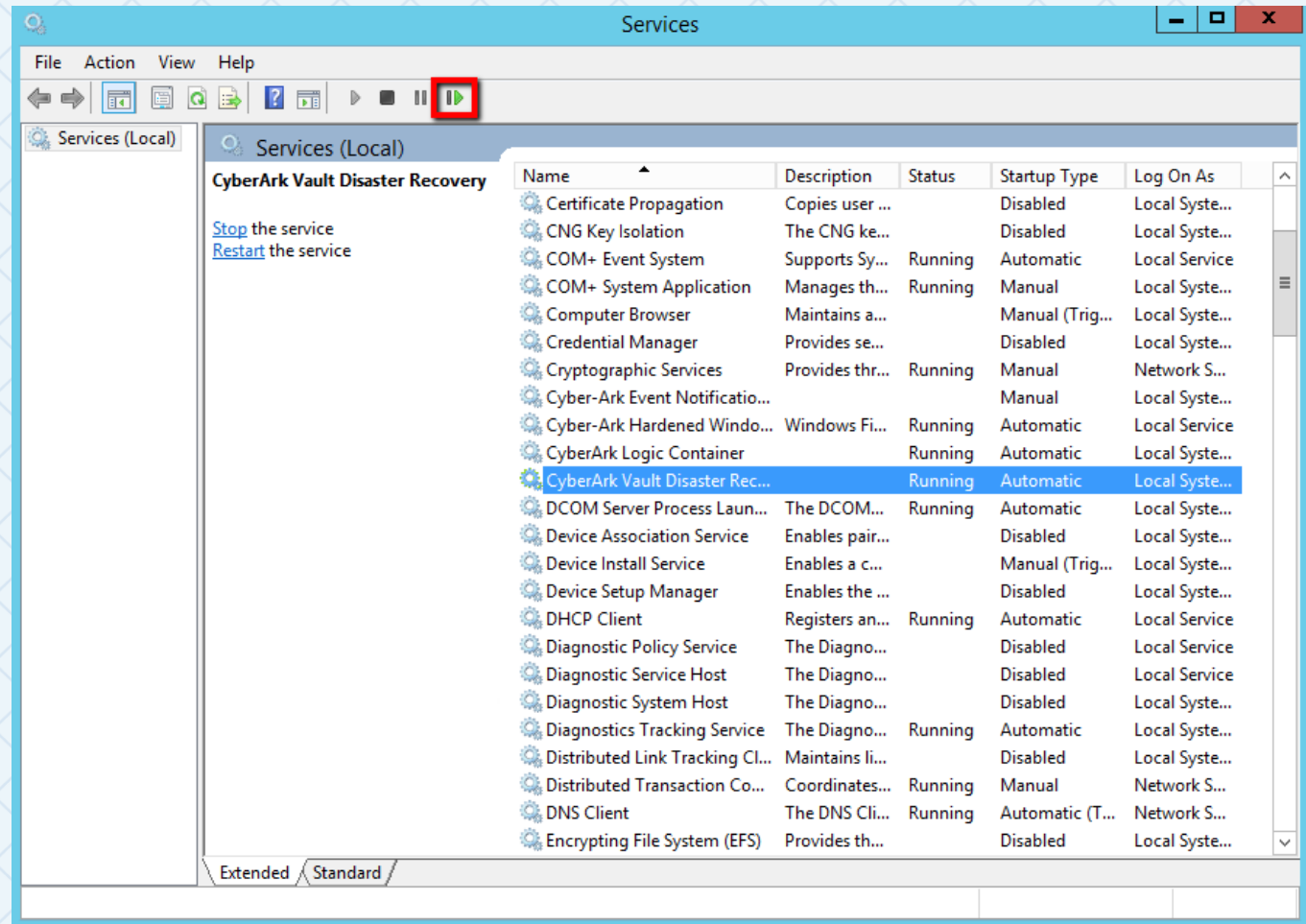
- Synchronize the Vault database
- Starts the PrivateArk Server service
- Starts the ENE service
- Stops the Disaster Recovery service



```
padr.ini - Notepad
File Edit Format View Help
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR\user.ini"
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=No
EnableDBsync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
ActivateManualFailover=Yes
```

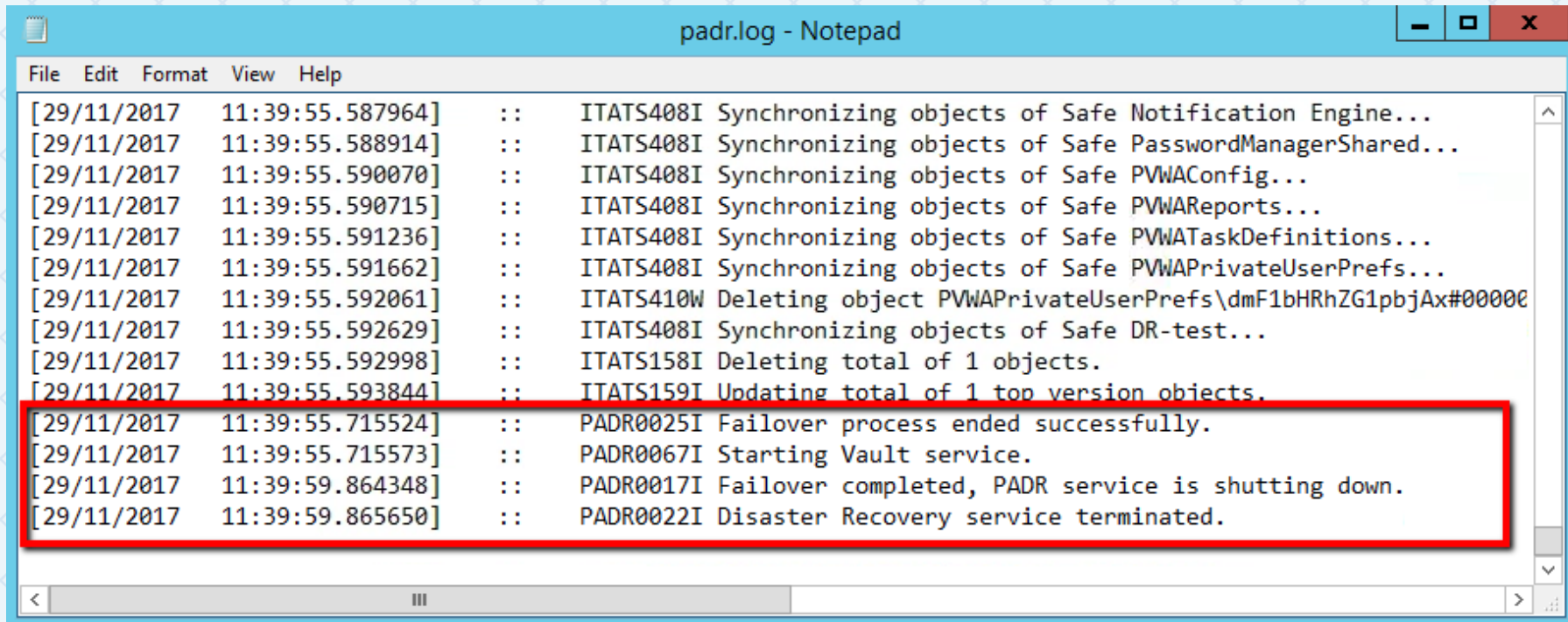
# MANUAL FAILOVER

- Restart the DR service



# MANUAL FAILOVER

Verify that the DR Vault has been activated and that the DR service was stopped (PADR.log)



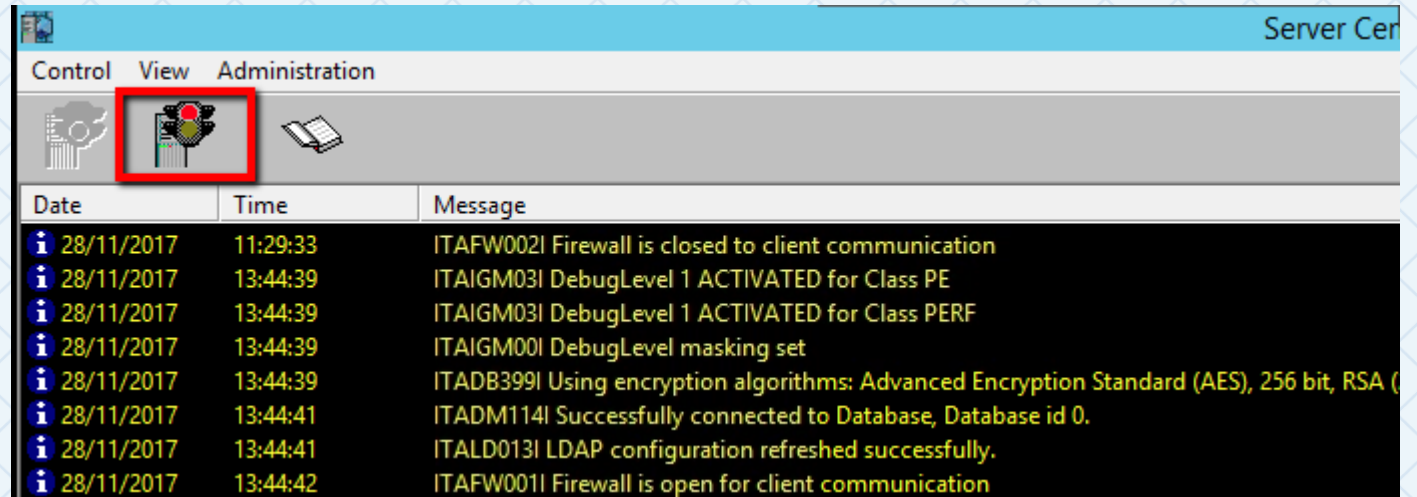
```
padr.log - Notepad
File Edit Format View Help
[29/11/2017 11:39:55.587964] :: ITATS408I Synchronizing objects of Safe Notification Engine...
[29/11/2017 11:39:55.588914] :: ITATS408I Synchronizing objects of Safe PasswordManagerShared...
[29/11/2017 11:39:55.590070] :: ITATS408I Synchronizing objects of Safe PVWAConfig...
[29/11/2017 11:39:55.590715] :: ITATS408I Synchronizing objects of Safe PVWAReports...
[29/11/2017 11:39:55.591236] :: ITATS408I Synchronizing objects of Safe PVWATaskDefinitions...
[29/11/2017 11:39:55.591662] :: ITATS408I Synchronizing objects of Safe PVWAPrivateUserPrefs...
[29/11/2017 11:39:55.592061] :: ITATS410W Deleting object PVWAPrivateUserPrefs\dmF1bHRhZG1pbjAx#00000
[29/11/2017 11:39:55.592629] :: ITATS408I Synchronizing objects of Safe DR-test...
[29/11/2017 11:39:55.592998] :: ITATS158I Deleting total of 1 objects.
[29/11/2017 11:39:55.593844] :: ITATS159I Updating total of 1 top version objects.
[29/11/2017 11:39:55.715524] :: PADR0025I Failover process ended successfully.
[29/11/2017 11:39:55.715573] :: PADR0067I Starting Vault service.
[29/11/2017 11:39:59.864348] :: PADR0017I Failover completed, PADR service is shutting down.
[29/11/2017 11:39:59.865650] :: PADR0022I Disaster Recovery service terminated.
```

# **DISASTER RECOVERY RETURN TO NORMAL MODE**



# RESTORING DR TO NORMAL MODE

- Start the PrivateArk Server on the Primary Vault and stop the PrivateArk Server Service on the DR Vault

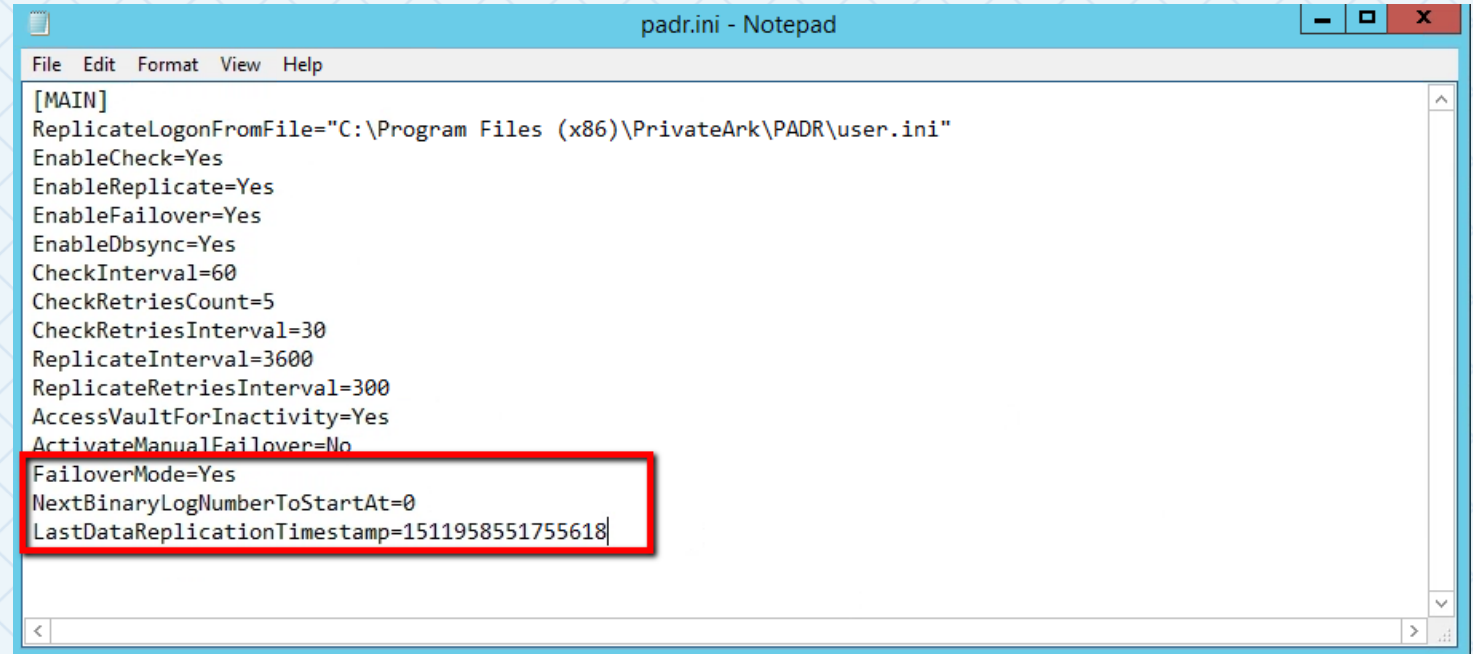




# RESTORING DR TO NORMAL MODE

On the DR Vault server, edit the PADR.INI file and make the following changes

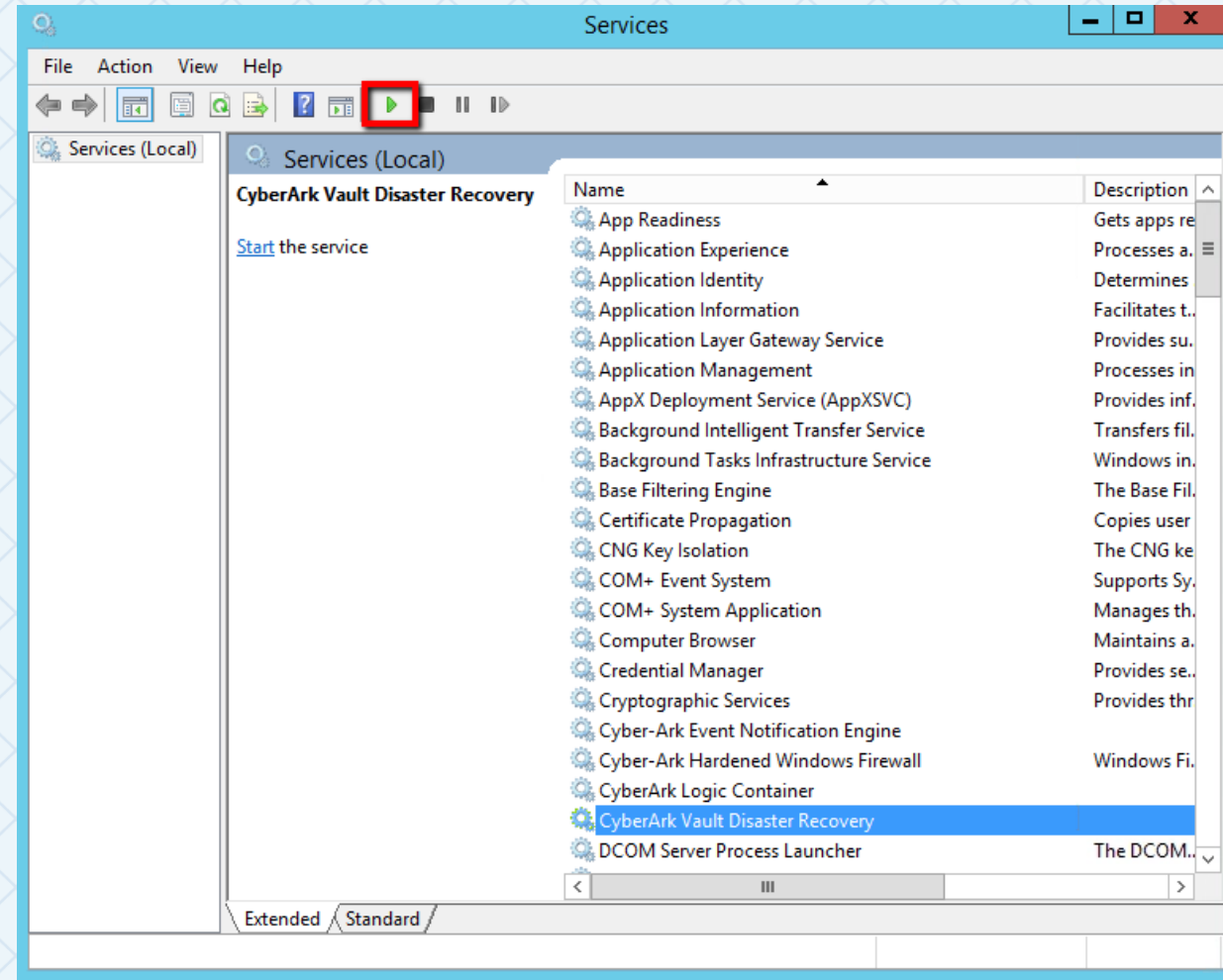
- Set FailoverMode=No
- Delete the last two lines in PADR.ini
- Deleting the last two lines in the file will force a full replication



```
pdr.ini - Notepad
File Edit Format View Help
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR\user.ini"
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=Yes
EnableObsync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
ActivateManualFailover=No
FailoverMode=Yes
NextBinaryLogNumberToStartAt=0
LastDataReplicationTimestamp=1511958551755618
```

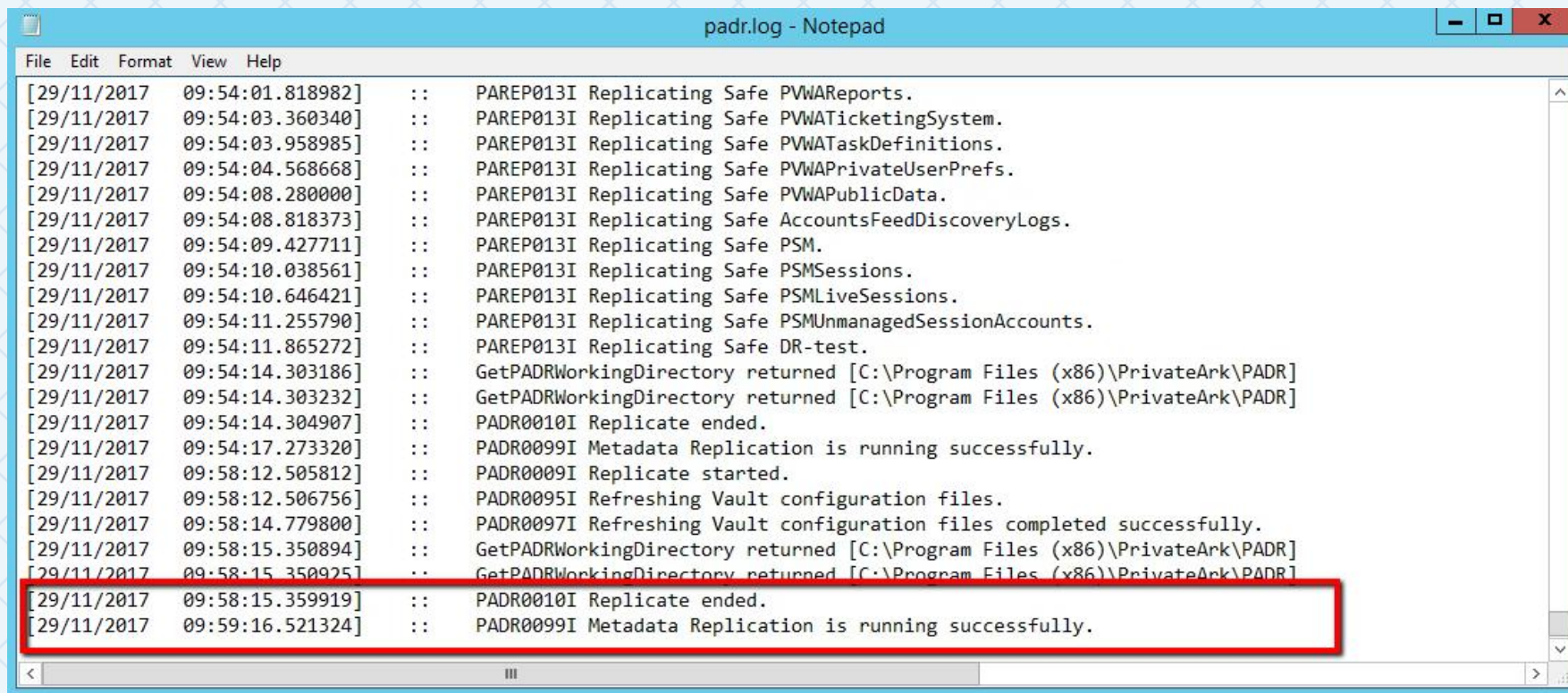
# RESTORING DR TO NORMAL MODE

- Archive or delete the PADR.LOG file
- Start the CyberArk Vault Disaster Recovery Service on the DR Vault



# RESTORING DR TO NORMAL MODE

Verify that the replication to the DR Vault ended successfully and that the metadata replication is running successfully by reviewing the PADR.log



```
pdr.log - Notepad
File Edit Format View Help
[29/11/2017 09:54:01.818982] :: PAREP013I Replicating Safe PVWAreports.
[29/11/2017 09:54:03.360340] :: PAREP013I Replicating Safe PVWATicketingSystem.
[29/11/2017 09:54:03.958985] :: PAREP013I Replicating Safe PVWATaskDefinitions.
[29/11/2017 09:54:04.568668] :: PAREP013I Replicating Safe PVWAPrivateUserPrefs.
[29/11/2017 09:54:08.280000] :: PAREP013I Replicating Safe PVWAPublicData.
[29/11/2017 09:54:08.818373] :: PAREP013I Replicating Safe AccountsFeedDiscoveryLogs.
[29/11/2017 09:54:09.427711] :: PAREP013I Replicating Safe PSM.
[29/11/2017 09:54:10.038561] :: PAREP013I Replicating Safe PSMSessions.
[29/11/2017 09:54:10.646421] :: PAREP013I Replicating Safe PSMLiveSessions.
[29/11/2017 09:54:11.255790] :: PAREP013I Replicating Safe PSMUnmanagedSessionAccounts.
[29/11/2017 09:54:11.865272] :: PAREP013I Replicating Safe DR-test.
[29/11/2017 09:54:14.303186] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 09:54:14.303232] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 09:54:14.304907] :: PADR0010I Replicate ended.
[29/11/2017 09:54:17.273320] :: PADR0099I Metadata Replication is running successfully.
[29/11/2017 09:58:12.505812] :: PADR0009I Replicate started.
[29/11/2017 09:58:12.506756] :: PADR0095I Refreshing Vault configuration files.
[29/11/2017 09:58:14.779800] :: PADR0097I Refreshing Vault configuration files completed successfully.
[29/11/2017 09:58:15.350894] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 09:58:15.350925] :: GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR]
[29/11/2017 09:58:15.359919] :: PADR0010I Replicate ended.
[29/11/2017 09:59:16.521324] :: PADR0099I Metadata Replication is running successfully.
```

# THE VAULT BACKUP UTILITY AKA PRIVATEARK REPLICATOR



# REPLICATE USE CASES

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



# REPLICATE ARCHITECTURE

## Direct Backup (Not Recommended)

- Module is installed on the Vault Server
- PAPreBackup.exe prepares the metadata on the Vault server for direct tape backup
- Warning: Installing a Backup Agent on the Vault may introduce vulnerabilities and is not recommended

## Indirect Backup (Recommended)

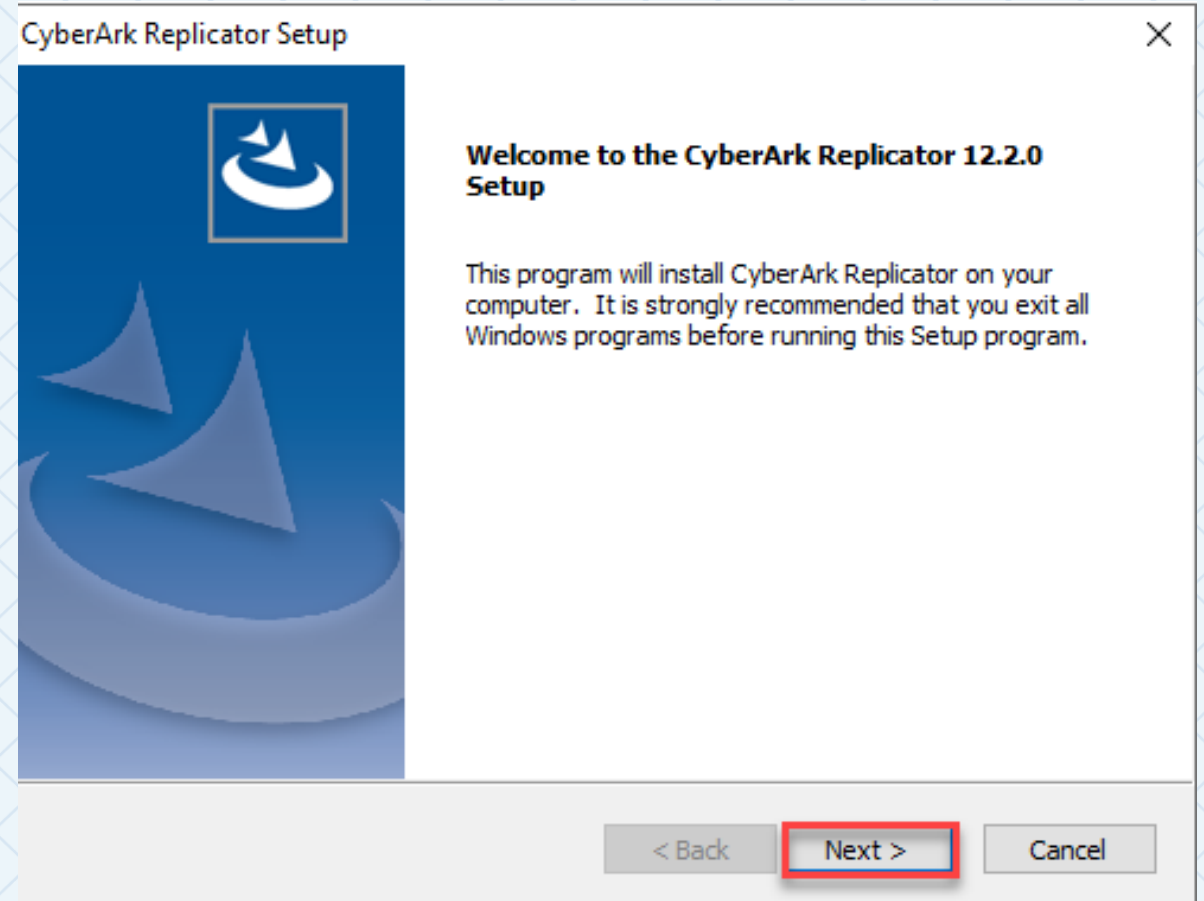
- Module is installed on any Server, typically the same server as other components
- PAReplicate.exe copies vault data as encrypted files to the domain server
- Enterprise Backup Software can then backup these files



# INSTALL PRIVATEARK REPLICATOR

Before installing the Vault Backup 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



# INSTALL THE VAULT BACKUP UTILITY

Enable the Backup User and Set initial Password on the Primary Vault

The screenshot shows the 'Update User: Backup' dialog box with the 'General' tab selected. The 'User Name' is 'Backup' and the 'User type' is 'Built-In Admins'. The 'Location' is '\System'. The 'Disable User' checkbox is highlighted with a red rectangle. Other options include 'Gateway Account', 'Provide full impersonation', 'Provide partial impersonation', 'Provide impersonation with additional Server authentication', 'Enable Quota', and 'Send email notification if component is not connected'.

Update User: Backup

Time Limitations | Personal details | Phone/Notes | Business/Internet

General | Authentication | Authorizations | Member Of

General Details

User Name: Backup

User type: Built-In Admins | Authorized Interfaces...

Location: \System | Browse...

☐ Gateway Account

☐ Provide full impersonation

☐ Provide partial impersonation

☐ Provide impersonation with additional Server authentication

☐ Disable User

Quota

☐ Enable Quota

Size: MB Used: 0 MB

Monitoring

☐ Send email notification if component is not connected

Replace Photo...

OK Cancel

The screenshot shows the 'Update User: Backup' dialog box with the 'Authentication' tab selected. The 'Authentication method' is 'Password'. The 'Require RSA SecurID authentication' checkbox is unchecked. The 'Distinguished Name' field is empty. The 'Password' and 'Confirm' fields are highlighted with a red rectangle. The 'User Must Change Password at Next Logon' checkbox is unchecked, and the 'Password Never Expires' checkbox is checked.

Update User: Backup

Time Limitations | Personal details | Phone/Notes | Business/Internet

General | Authentication | Authorizations | Member Of

Change Password

Authentication method: Password

☐ Require RSA SecurID authentication

Distinguished Name:

Select

Password: xxxxxxxx

Confirm: xxxxxxxx

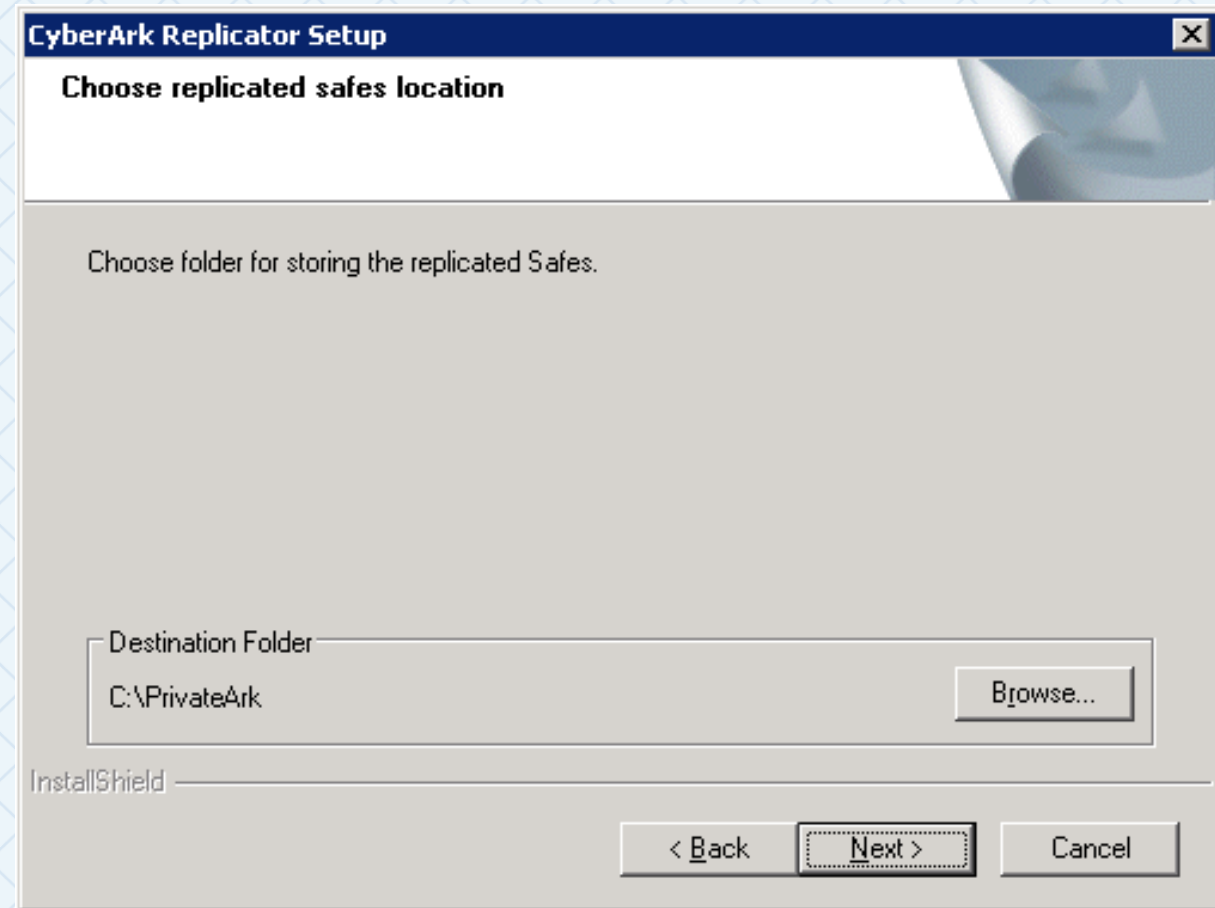
☐ User Must Change Password at Next Logon

☒ Password Never Expires

OK Cancel

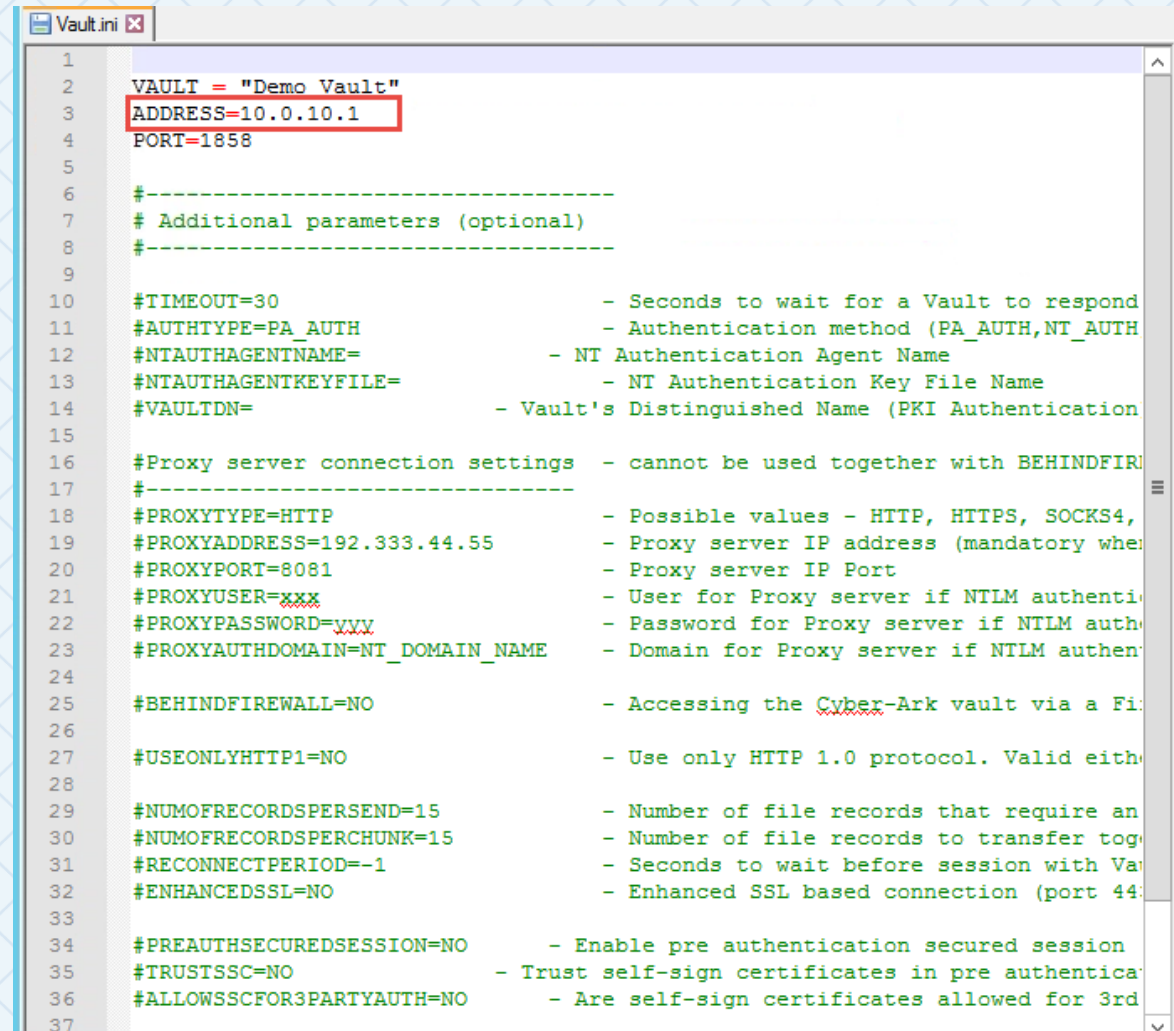
# SETUP SCHEDULED REPLICATIONS

- Install the PrivateArk Replicator and specify a Location to store the data
- No services or agents are installed on the backup server



# SETUP SCHEDULED REPLICATIONS

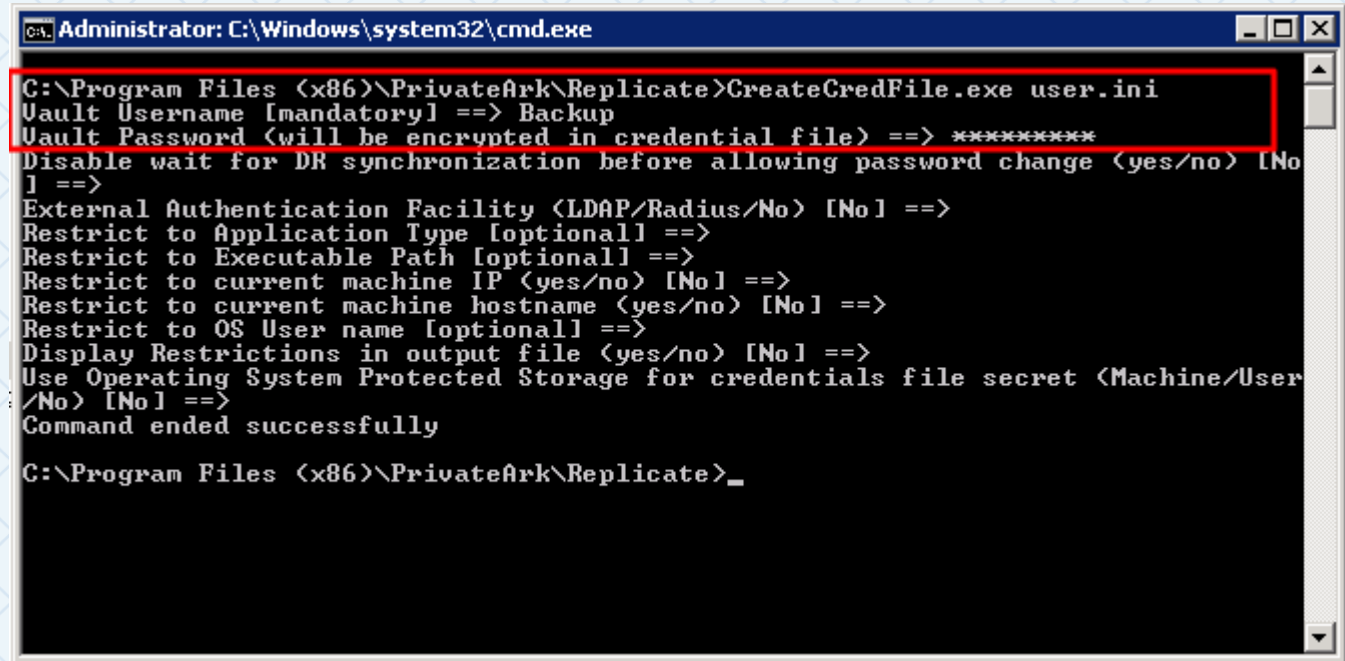
- Edit the Vault.ini to inform the PAReplicate utility the network address of the Vault server



```
1 VAULT = "Demo Vault"
2 ADDRESS=10.0.10.1
3 PORT=1858
4
5
6 #-----
7 # Additional parameters (optional)
8 #-----
9
10 #TIMEOUT=30 - Seconds to wait for a Vault to respond
11 #AUTHTYPE=PA_AUTH - Authentication method (PA_AUTH,NT_AUTH)
12 #NTAUTHAGENTNAME= - NT Authentication Agent Name
13 #NTAUTHAGENTKEYFILE= - NT Authentication Key File Name
14 #VAULTDN= - Vault's Distinguished Name (PKI Authentication)
15
16 #Proxy server connection settings - cannot be used together with BEHINDFIREWALL
17 #-----
18 #PROXYTYPE=HTTP - Possible values - HTTP, HTTPS, SOCKS4,
19 #PROXYADDRESS=192.333.44.55 - Proxy server IP address (mandatory when using proxy)
20 #PROXYPORT=8081 - Proxy server IP Port
21 #PROXYUSER=xxx - User for Proxy server if NTLM authentication
22 #PROXYPASSWORD=vvv - Password for Proxy server if NTLM authentication
23 #PROXYAUTHDOMAIN=NT_DOMAIN_NAME - Domain for Proxy server if NTLM authentication
24
25 #BEHINDFIREWALL=NO - Accessing the CyberArk vault via a Firewall
26
27 #USEONLYHTTP1=NO - Use only HTTP 1.0 protocol. Valid either 1 or 0
28
29 #NUMOFRECORDSPERSEND=15 - Number of file records that require an authentication
30 #NUMOFRECORDSPERCHUNK=15 - Number of file records to transfer together
31 #RECONNECTPERIOD=-1 - Seconds to wait before session with Vault server
32 #ENHANCEDSSL=NO - Enhanced SSL based connection (port 443)
33
34 #PREAUTHSECUREDSESSION=NO - Enable pre authentication secured session
35 #TRUSTSSC=NO - Trust self-sign certificates in pre authentication
36 #ALLOWSSCFOR3PARTYAUTH=NO - Are self-sign certificates allowed for 3rd party
37
```

# SETUP SCHEDULED REPLICATIONS

- Create a Credential File for the Backup User
- The Credential File is used by PAReplicate to authenticate to the Vault
- The password for the Backup user is changed periodically in the Vault



```
Administrator: C:\Windows\system32\cmd.exe
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]
1 ==>
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>_
```



# SETUP SCHEDULED REPLICATIONS

- The backup is launched at a command line using the PAReplicate.exe executable file
- A Scheduled Task should be created to launch the backup at a predetermined interval
- The syntax of the command as shown, specifies the vault.ini file and uses the logonfromfile and fullbackup switch

**Create Basic Task Wizard**

**Start a Program**

**Create a Basic Task**

Trigger: Daily

Action: **Start a Program**

Finish

Program/script: "C:\Program Files (x86)\PrivateArk\Replicate\pareplicate.exe" Browse...

Add arguments (optional): logonfromfile user.ini /fullbackup

Start in (optional): C:\Program Files (x86)\PrivateArk\Replicate

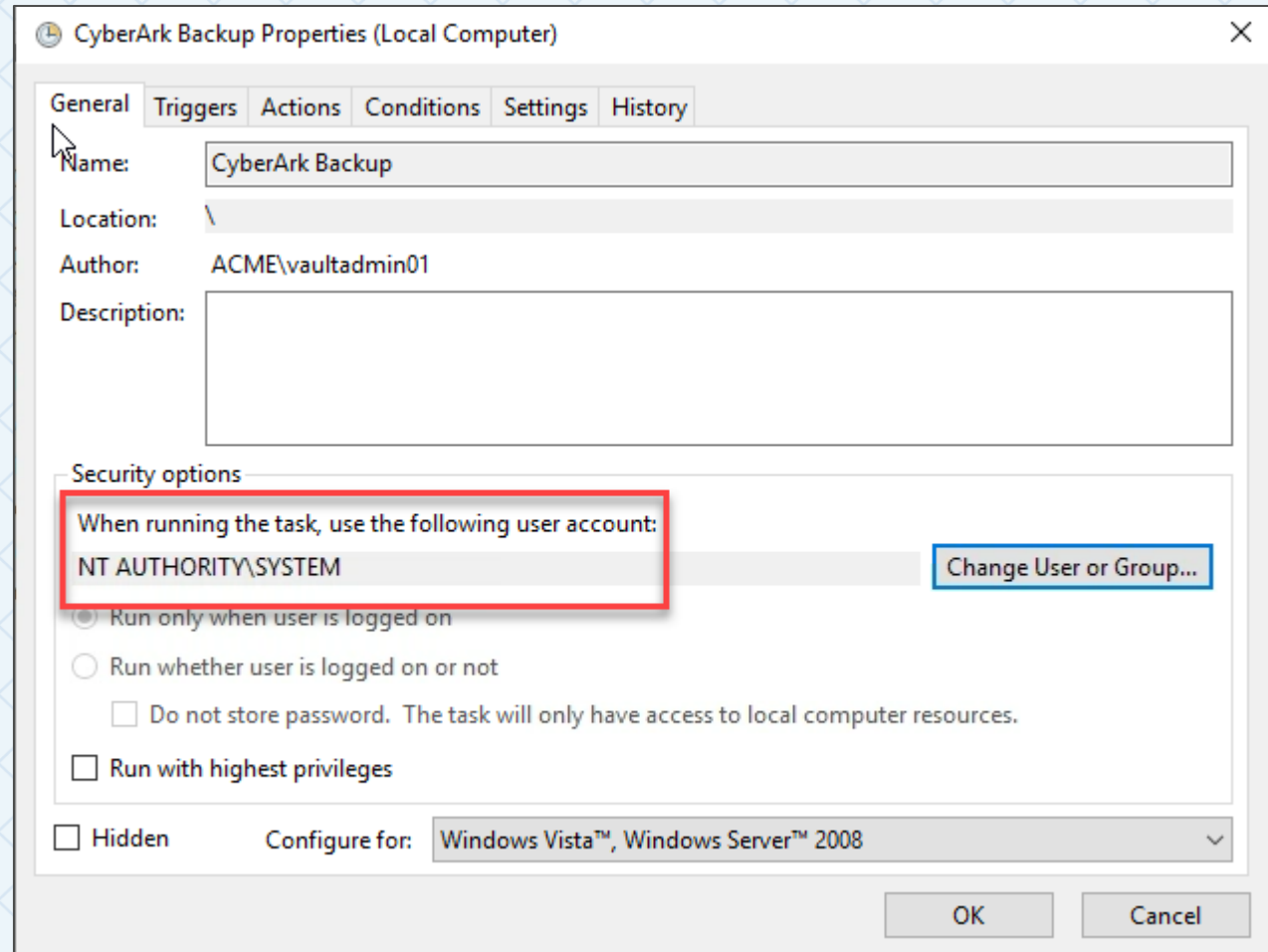
**Command Syntax:**

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

< Back **Next >** Cancel

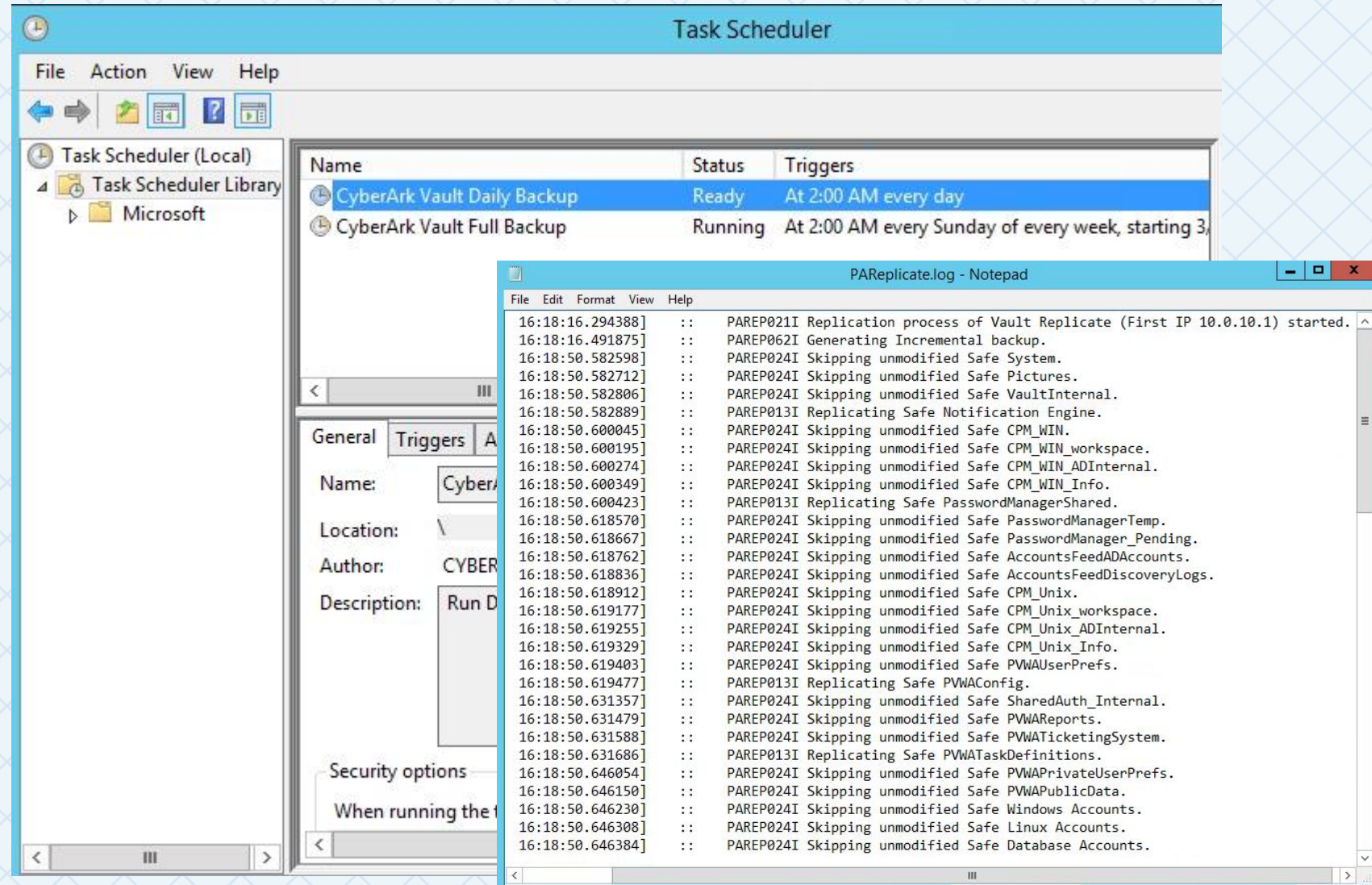
# SETUP SCHEDULED REPLICATIONS

- Run the task using the SYSTEM account or a non-privileged service account
- Never run services or scheduled tasks using privileged accounts or accounts assigned to an individual!



# PERFORMING REPLICATION

- Create a Windows Scheduled task
- One task running daily as an incremental backup will perform an initial full backup
- Each subsequent backup job will only backup changed files
- Logs can be found in the root of the \Replicate folder



# PERFORMING RESTORE

- The PARestore utility enables you to restore Safes that have previously been backed up
- The Safe data files are restored to the PrivateArk\Restored Safes folder in the same structure as that in which they were backed up

```
C:\Program Files (x86)\PrivateArk\Replicate>PARestore.exe Vault.ini dr /RestoreSafe Linux02 /targetSafe LinuxRestore
Password: *****
PARS1011I Restore process of Vault Restore (10.0.1.20) started at Thu May 05 02:43:50 2016
PARS1021I Restoring Metadata file backup-dump.sql.gz.
PARS1009I Restoring file backup-dump.sql.gz.
PARS1021I Restoring Metadata file cfg.backup-encrfile.ini.gz.
PARS1009I Restoring file cfg.backup-encrfile.ini.gz.
PARS1021I Restoring Metadata file cfg.backup-replicationuser.pass.gz.
PARS1009I Restoring file cfg.backup-replicationuser.pass.gz.
PARS1019I 1 out of 1 dump files restored successfully.
PARS1020I 0 out of 0 Binary Logs restored successfully.
PARS1027I 2 out of 2 Configuration files restored successfully.
PARS1009I Restoring file root\root.backup.#000000000000001#.test.
PARS1008I 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 PUMAGWAccounts 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.#000000000000001#.test to Root\root.backup.#000000000000001#.test.
PARS1012I Restore process of Vault Restore (10.0.1.20) ended at Thu May 05 02:44:17 2016
```



# PERFORMING RESTORE

- After the metadata backup files are restored, users will be able to work with the files immediately
- 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: *****
PARSI011I Restore process of Vault Restore (10.0.1.20) started at Thu May 05 02:43:56 2016
PARSI021I Restoring Metadata file backup-dump.sql.gz.
PARSI009I Restoring file backup-dump.sql.gz.
PARSI021I Restoring Metadata file cfg.backup-encrfile.ini.gz.
PARSI009I Restoring file cfg.backup-encrfile.ini.gz.
PARSI021I Restoring Metadata file cfg.backup-replicationuser.pass.gz.
PARSI009I Restoring file cfg.backup-replicationuser.pass.gz.
PARSI019I 1 out of 1 dump files restored successfully.
PARSI020I 0 out of 0 Binary Logs restored successfully.
PARSI027I 2 out of 2 Configuration files restored successfully.
PARSI009I Restoring file root\root.backup.#000000000000001#.test.
PARSI008I 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 PUWAGWAccounts 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.#000000000000001#.test to Root\root.backup.#000000000000001#.test.
PARSI012I Restore process of Vault Restore (10.0.1.20) ended at Thu May 05 02:44:17 2016

```



# SUMMARY

In this session we covered:

- Disaster Recovery Deployment
- Backup Solution Deployment

# THANK YOU