CYBERARK®

PAM Administration

Disaster Recovery

Agenda

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

- Describe the **CyberArk PAM Disaster Recovery** solution
- Configure and test Disaster Recovery

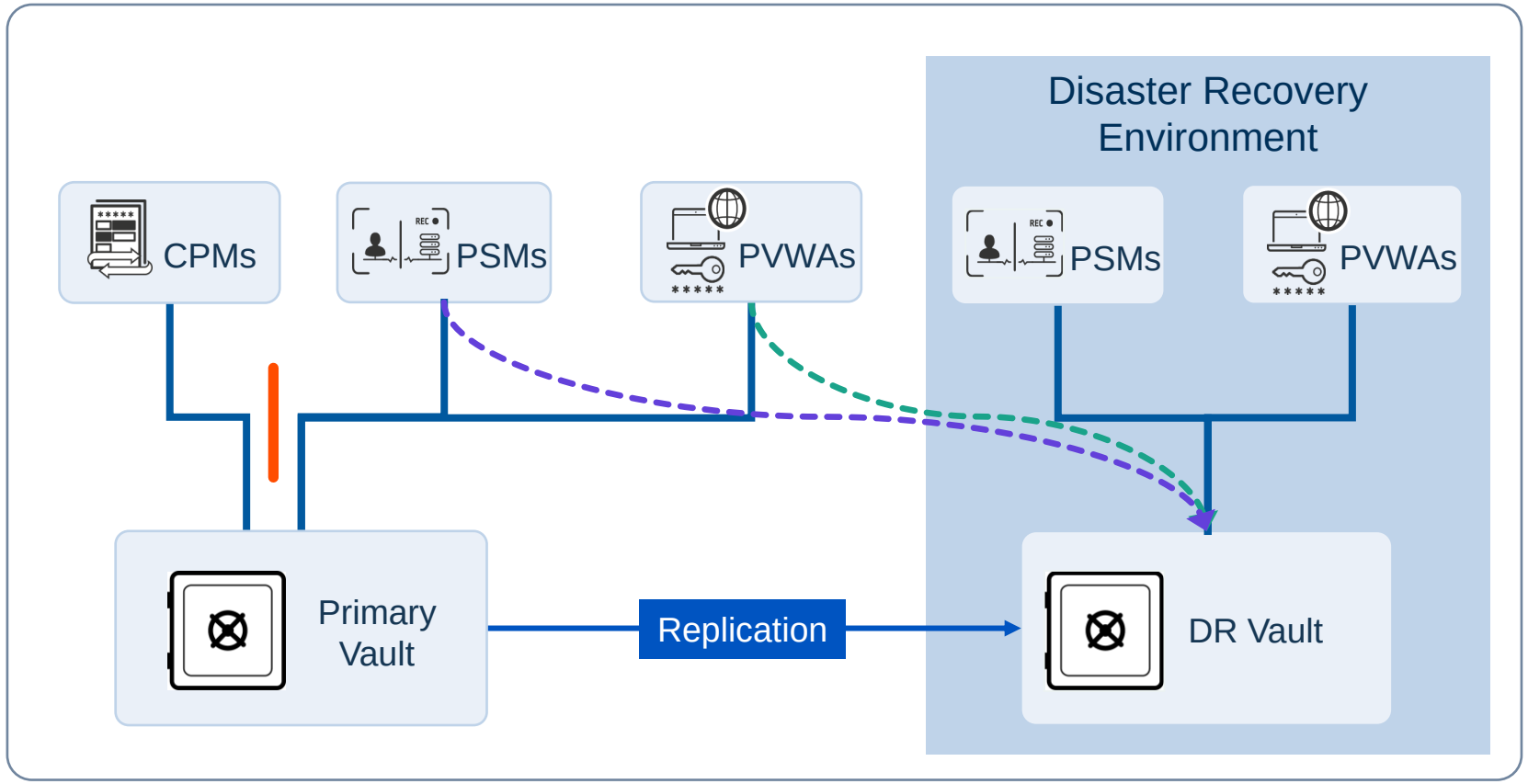
Disaster Recovery

- DR architecture
- Setup DR
- Vault failover
- Component failover
- Return to primary site

Architecture

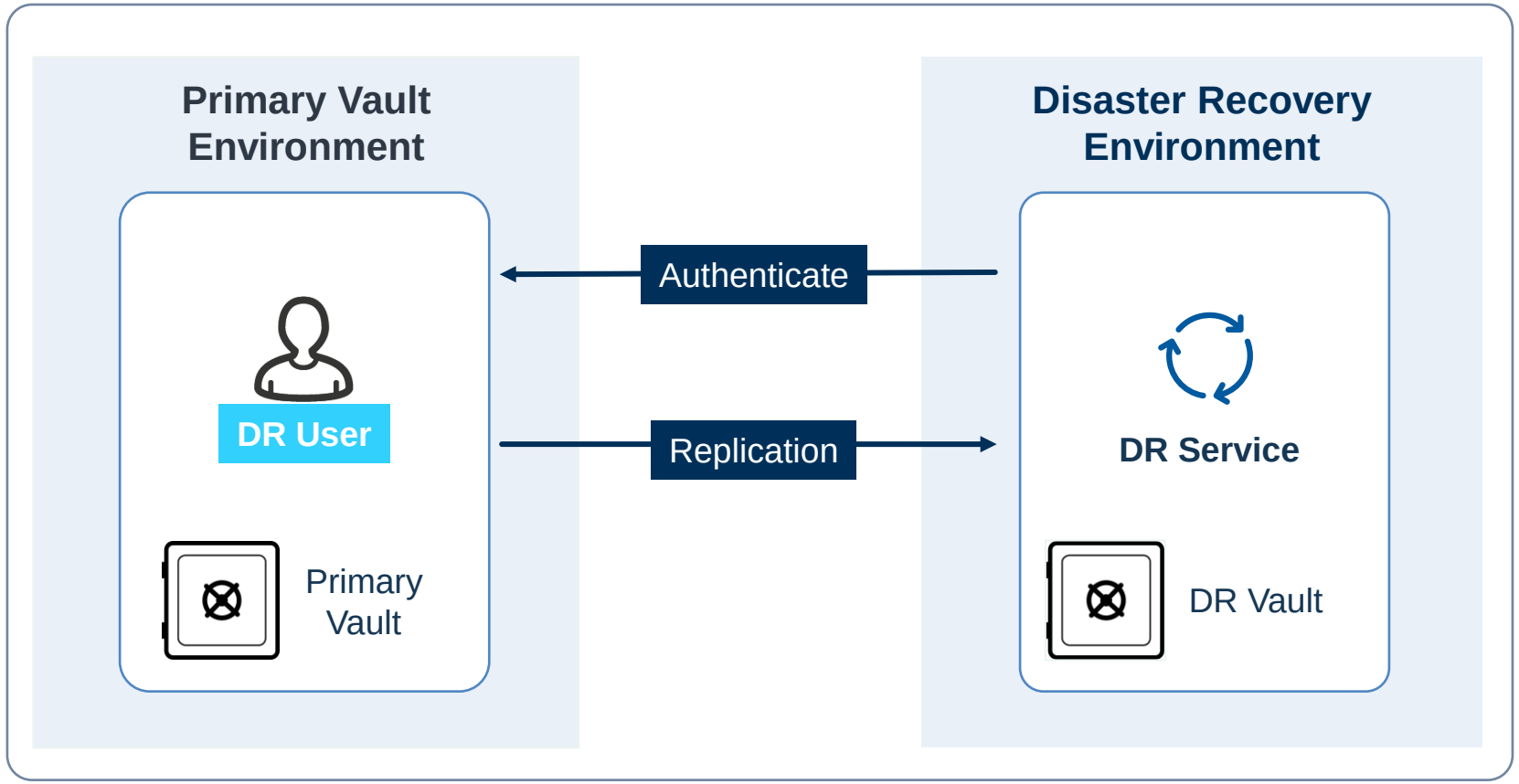
Disaster Recovery Architecture

- The ***Disaster Recovery*** (DR) Vault is a standalone or clustered Vault server with an extra software component installed: the DR service
- **PSM** and **PVWA** should be deployed at the DR site to provide access to users in the event of a disaster
- The **CPM** should never be configured for automatic failover



DR User

- The DR user is created automatically
- The DR service is installed on the **DR Vault**
- The DR service on the **DR Vault** authenticates to the **Primary Vault** using the credentials of the DR user to replicate data from the **Primary Vault** to the **DR Vault**

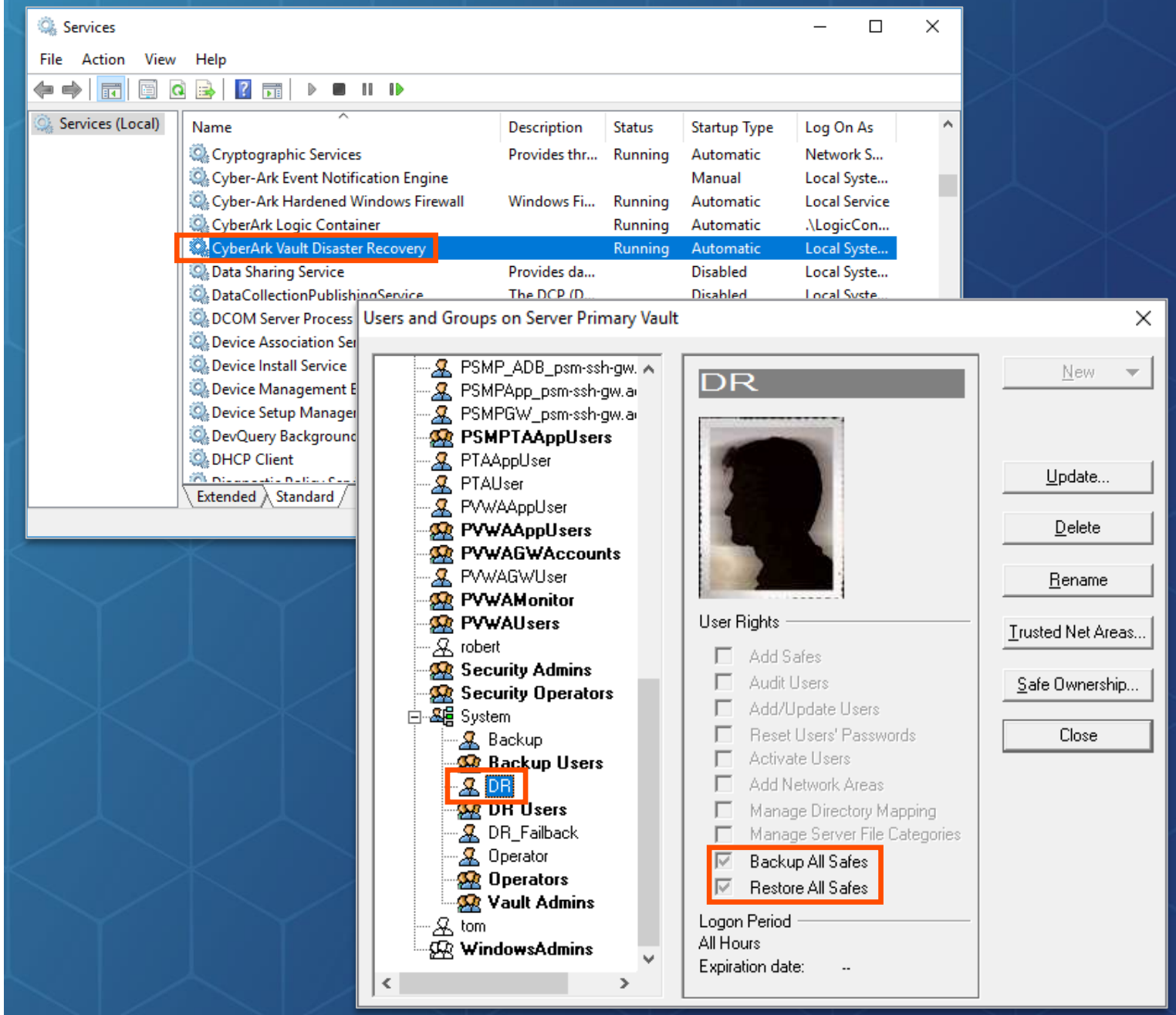


The DR Service and User

- The **DR** service runs on the **DR Vault**

- The **DR** user authenticates to the **Primary Vault** from the **DR Vault** as a user with permissions to:
  - ***Backup All Safes***
  - ***Restore All Safes***

- The built-in **DR** user has these permissions by default

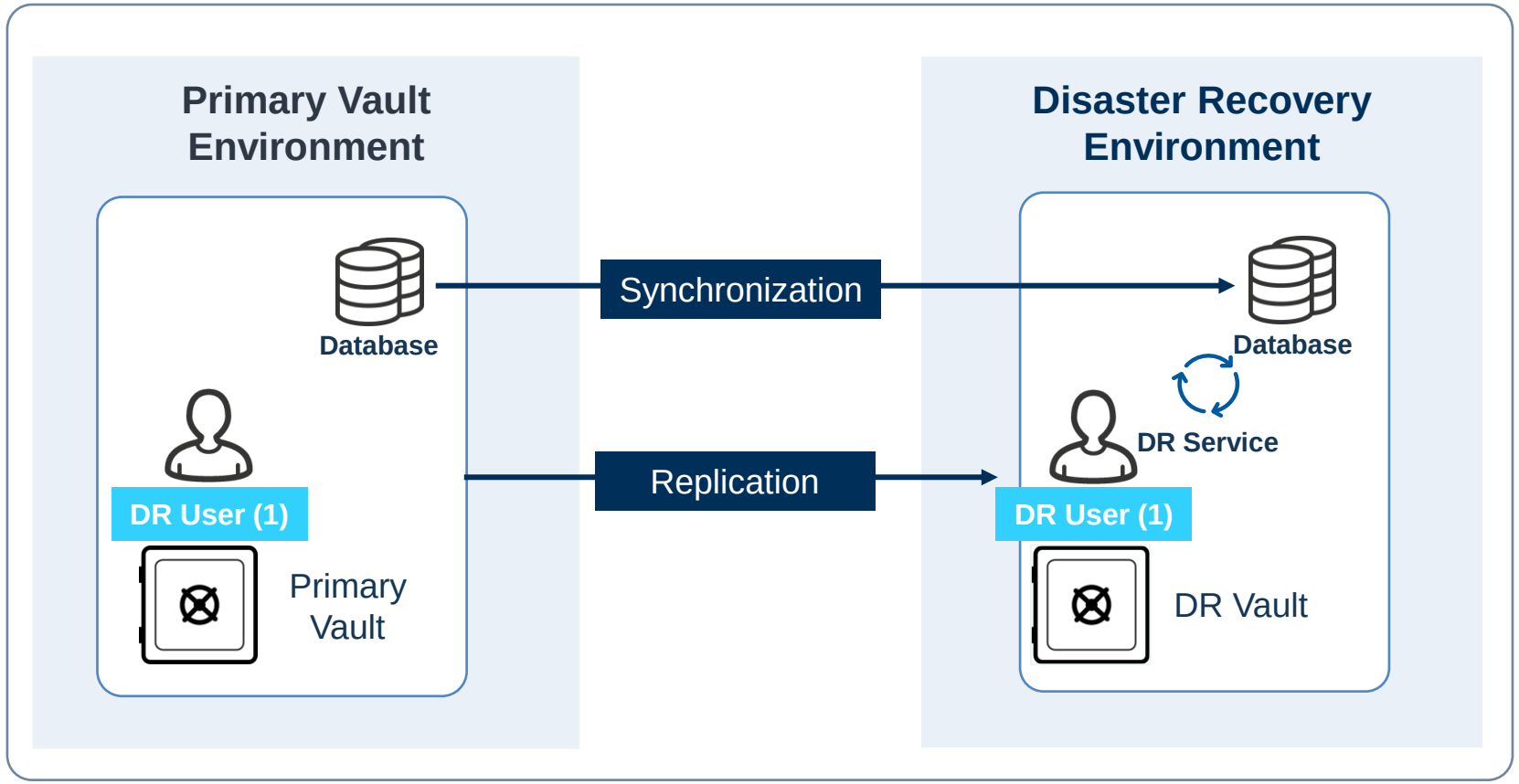


Enhanced DR Replication

- In the past, the replication of passwords was done based on an interval defined in the DR configuration file
- In version 9.3, the DR replication process was enhanced to ensure faster replication of passwords and improved consistency between production and DR sites
- Replicating the current passwords to DR sites is now done instantly and in parallel to files/recordings replication in order to avoid delays
- In the new replication mechanism, metadata (which includes the current passwords) is pushed from the production Vault to the DR sites as it is created

Enhanced DR Replication

- Database synchronization
- Near real-time



Set up Disaster Recovery

Enable Data and Metadata Synchronization

- When a failover occurs (automatic or manual), the DR service first synchronizes the information in its database with the information in the Safe data files
- This is enabled in the configuration file ***padr.ini*** with the default setting ***EnableDbsync=Yes***

padr.ini - Notepad

File Edit Format View Help

```
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR
\Conf\user.ini"
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=Yes
EnableDbsync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
NextBinaryLogNumberToStartAt=0
LastDataReplicationTimestamp=1573742661455341
```

Setup Data Replication Interval

The ***ReplicateInterval*** parameter determines the length of time between synchronization of the Vault file system, which by default is 3,600 seconds (one hour)

padr.ini - Notepad

File Edit Format View Help

```
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR
\Conf\user.ini"
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=Yes
EnableDbsync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
NextBinaryLogNumberToStartAt=0
LastDataReplicationTimestamp=1573742661455341
```

Vault Failover

Automatic Failover

- Automatic failover is switched on with the parameter ***EnableFailover=Yes***
- The ***CheckInterval*** indicates the **DR Vault** will contact the **Primary Vault** every 60 seconds. If it fails…

  it will try again ***5*** times…

  once every ***30*** seconds

After which, the **DR Vault** considers that the **Primary** is down and it goes into DR mode

padr.ini - Notepad

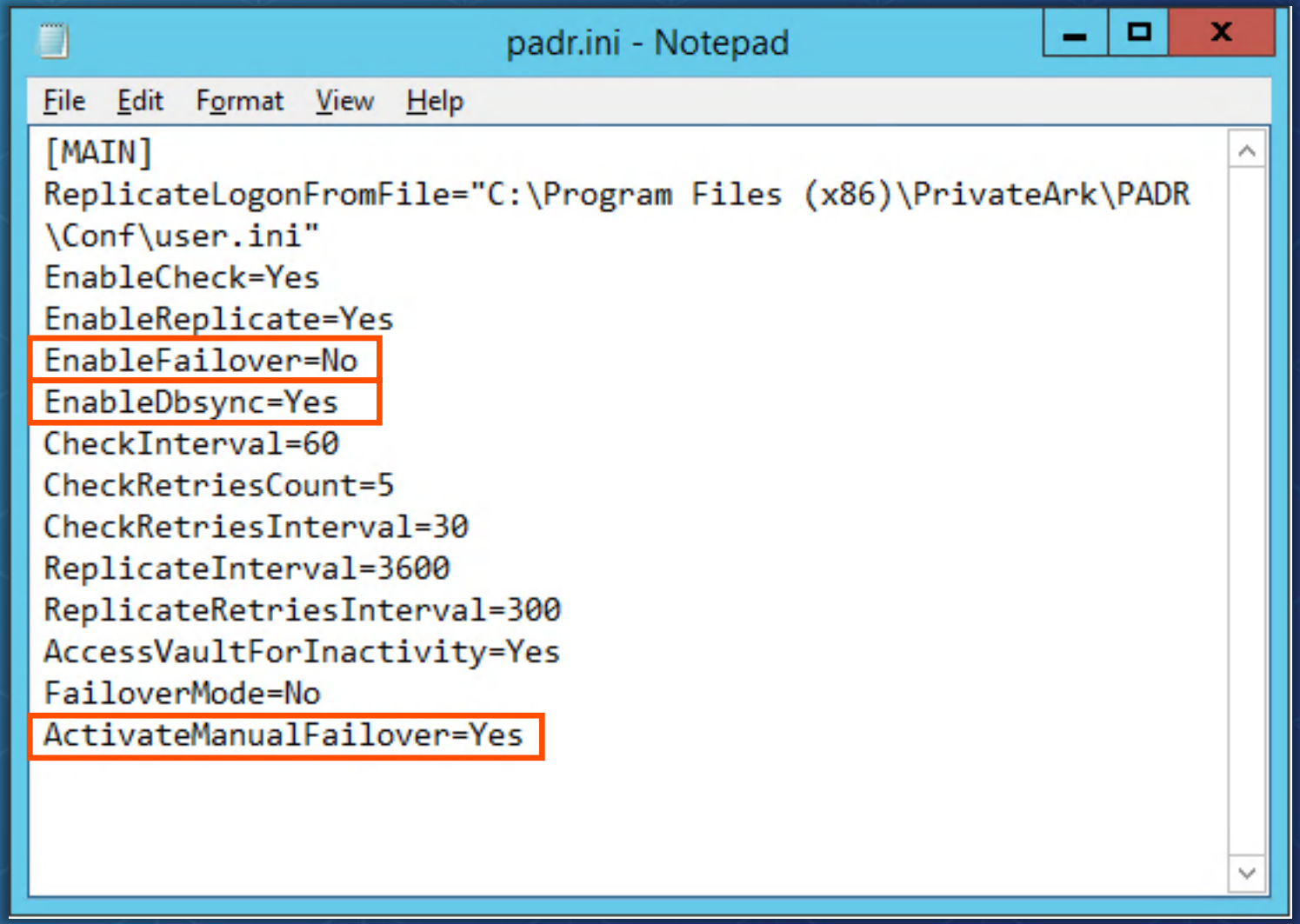
File Edit Format View Help

```
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR
\Conf\user.ini"
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=Yes
EnableDbsync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
NextBinaryLogNumberToStartAt=0
LastDataReplicationTimestamp=1573742661455341
```

Manual Failover

- To perform a proper Manual Failover, set the following parameters in ***padr.ini***:
  - ***EnableFailover*** to ***No*** (disables auto failover).
  - ***EnableDbsync*** to ***Yes*** (default setting).
  - ***ActivateManualFailover*** to ***Yes***.
- Restart the DR service

Restarting the DR service in this configuration will trigger a proper manual failover



The Failover Process

- Connection fails
- Retry attempts, failover started
- Data synchronization
- Start PrivateArk Server
- Stop Disaster Recovery service

```
[15/11/2019   03:37:19.579740]   ::   PADR0097I Refreshing Vault configuration files completed successfully.
[15/11/2019   03:37:19.583130]   ::   GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR\Conf]
[15/11/2019   03:37:19.583156]   ::   GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR\Conf]
[15/11/2019   03:37:19.585119]   ::   PADR0010I Replicate ended.
[15/11/2019   03:39:49.461321]   ::   PADR0005E CASTM003E Vault transaction failed. Reason: ITACM012S Timeout has expired
[15/11/2019   03:39:49.461373]   ::   PADR0014E Attempt to test vault availability failed (code=1).
[15/11/2019   03:40:48.820556]   ::   PADR0005E CASTM003E Vault transaction failed. Reason: ITACM062S Communication error
[15/11/2019   03:40:48.820603]   ::   PADR0015E Attempt to test vault availability failed 2 times (code=-1066062).
[15/11/2019   03:41:49.164344]   ::   PADR0005E CASTM003E Vault transaction failed. Reason: ITACM062S Communication error
[15/11/2019   03:41:49.164388]   ::   PADR0015E Attempt to test vault availability failed 3 times (code=-1066062).
[15/11/2019   03:42:48.586131]   ::   PADR0005E CASTM003E Vault transaction failed. Reason: ITACM062S Communication error
[15/11/2019   03:42:48.586204]   ::   PADR0015E Attempt to test vault availability failed 4 times (code=-1066062).
[15/11/2019   03:42:48.587974]   ::   PADR0099I Metadata Replication is running successfully.
[15/11/2019   03:43:48.992889]   ::   PADR0005E CASTM003E Vault transaction failed. Reason: ITACM062S Communication error
[15/11/2019   03:43:48.992962]   ::   PADR0015E Attempt to test vault availability failed 5 times (code=-1066062).
[15/11/2019   03:43:48.993396]   ::   PADR0016E Vault availability test failed, failover started.
[15/11/2019   03:43:48.993586]   ::   PADR0103I Failover process started.
[15/11/2019   03:43:48.998678]   ::   GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR\Conf]
[15/11/2019   03:43:48.998706]   ::   GetPADRWorkingDirectory returned [C:\Program Files (x86)\PrivateArk\PADR\Conf]
[15/11/2019   03:43:49.000938]   ::   PADR0024I Synchronizing vault data and metadata.
[15/11/2019   03:43:49.046952]   ::   ITATS408I Synchronizing objects of Safe Notification Engine...
[15/11/2019   03:43:49.082602]   ::   ITATS408I Synchronizing objects of Safe PVWATaskDefinitions...
[15/11/2019   03:43:49.094407]   ::   ITATS158I Deleting total of 0 objects.
[15/11/2019   03:43:49.094439]   ::   ITATS159I Updating total of 0 top version objects.
[15/11/2019   03:44:00.175729]   ::   PADR0025I Failover process ended successfully.
[15/11/2019   03:44:00.175766]   ::   PADR0067I Starting Vault service.
[15/11/2019   03:44:09.987674]   ::   PADR0017I Failover completed, PADR service is shutting down.
[15/11/2019   03:44:10.180106]   ::   PADR0022I Disaster Recovery service terminated.
```

Component Failover

Setup Components Failover

- It is possible to configure components to failover automatically to the **DR Vault** by configuring addresses for both the **Primary** and **DR Vaults** in the ***Vault.ini*** file
- The component will attempt to connect according to the order set in ***Vault.ini***

REMEMBER: Not all components should be allowed to automatically failover

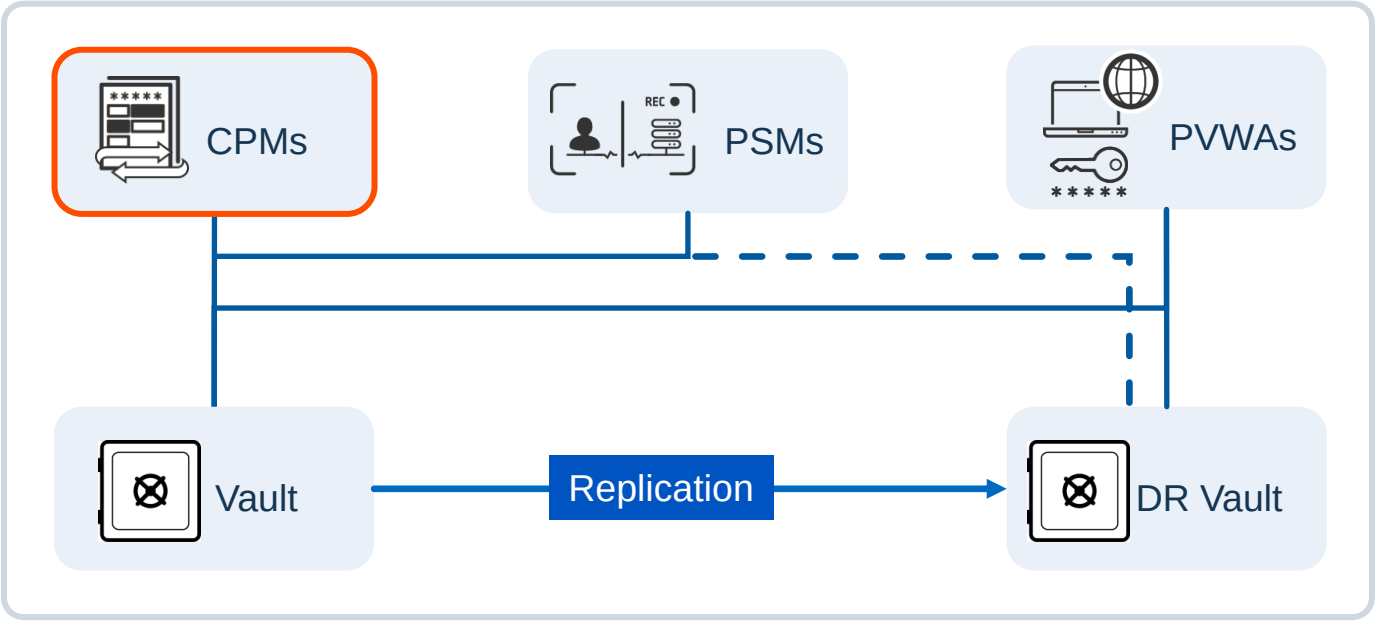
Vault.ini - Notepad

File Edit Format View Help

```
VAULT = "Prod","DR"
ADDRESS=10.0.10.1,10.0.14.1
Port=1858

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

#TIMEOUT=30                        - Seconds to wait for a Vault to respond to a request

#VAULTDN=                                 - Vault's Distinguished Name (PKI Authentication)

#Proxy server connection settings  - cannot be used together with BEHINDFIREWALL
#--------------------------------
#PROXYTYPE=HTTP                    - Possible values - HTTP, HTTPS, SOCKS4, SOCKS5
#PROXYADDRESS=10.0.10.1
#PROXYPORT=8081                    - Proxy server IP Port
#PROXYUSER=xxx                     - User for Proxy server if NTLM authentication is required
#PROXYPASSWORD=yyy                 - Password for Proxy server if NTLM authentication is required
#PROXYAUTHDOMAIN=NT_DOMAIN_NAME    - Domain for Proxy server if NTLM authentication is required

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

#USEONLYHTTP1=NO                   - Use only HTTP 1.0 protocol. Valid either with proxy settings Or with
```

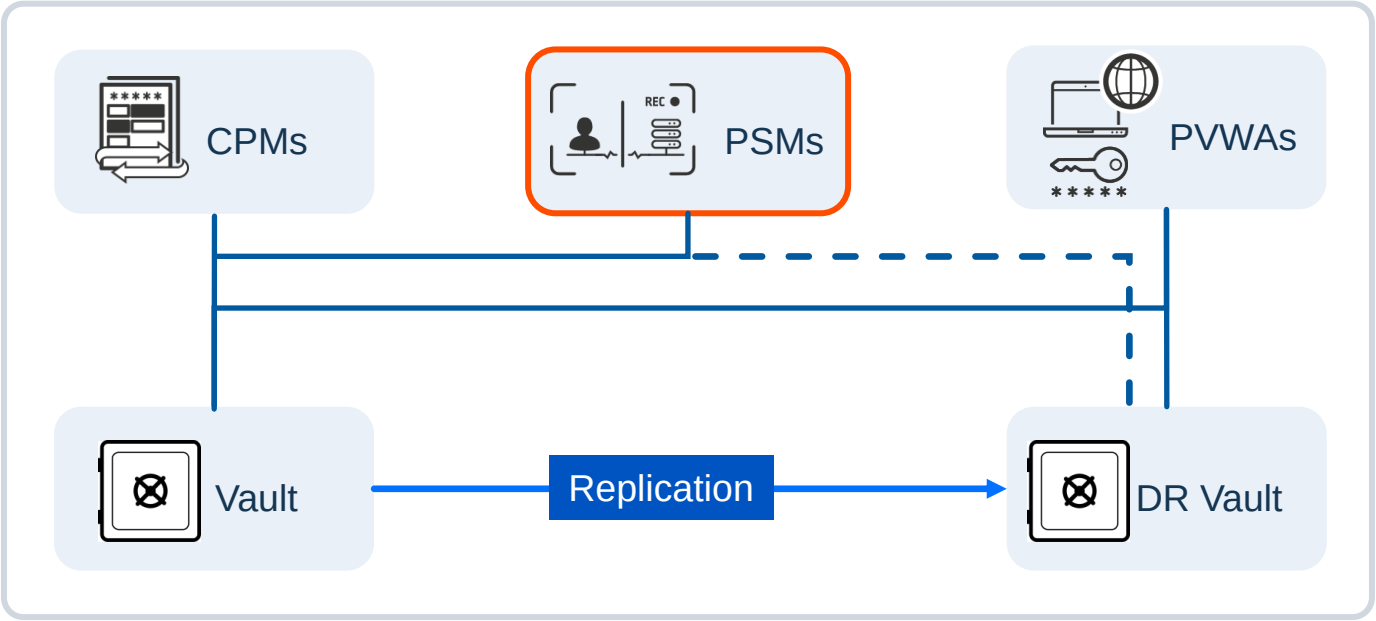
CPM Failover Setup

- **CPM** should **NEVER** be configured for automatic failover due to the possibility of a split-brain scenario
- Split-brain occurs when the passwords in the **Production Vault** and **DR Vault** are out of sync
- **CPM** failover must always be a manual process



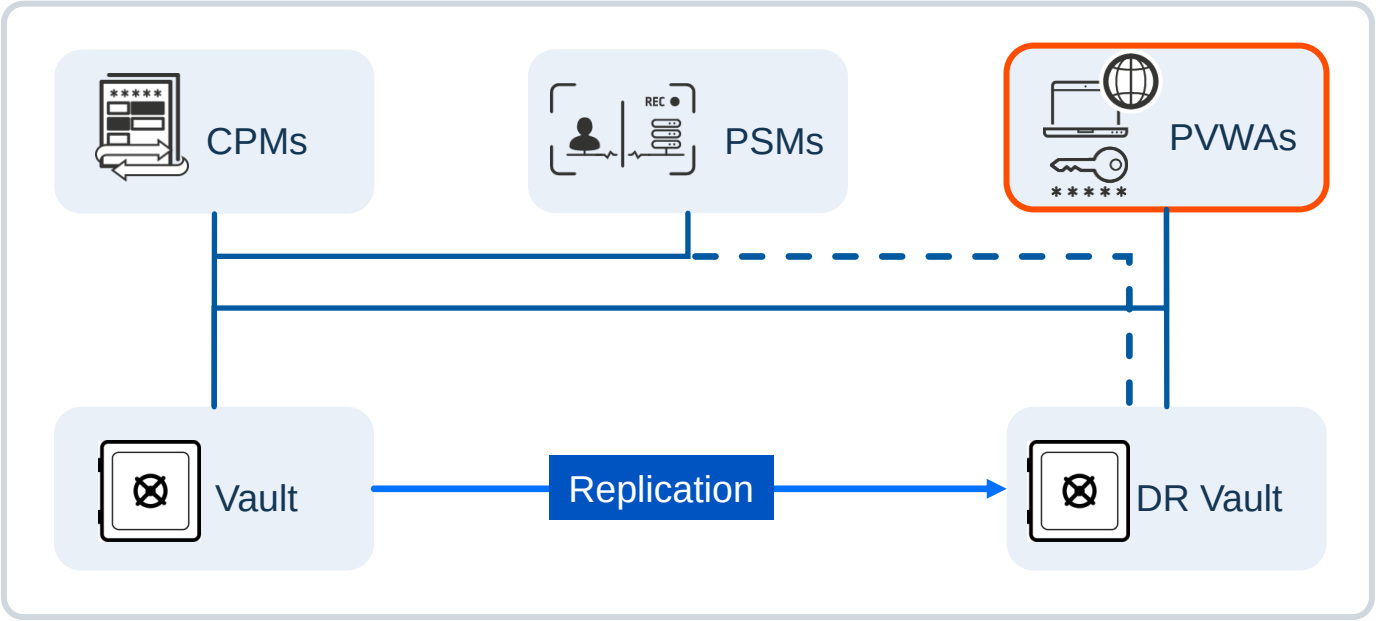
PSM Failover Setup

- Automatic failover of the **PSM** servers is optional
- Any recordings captured on the **DR Vault** must be backed up or replicated back the **Primary Vault** before returning to normal operations
- Consult with **CyberArk** services to review **PSM** failover options



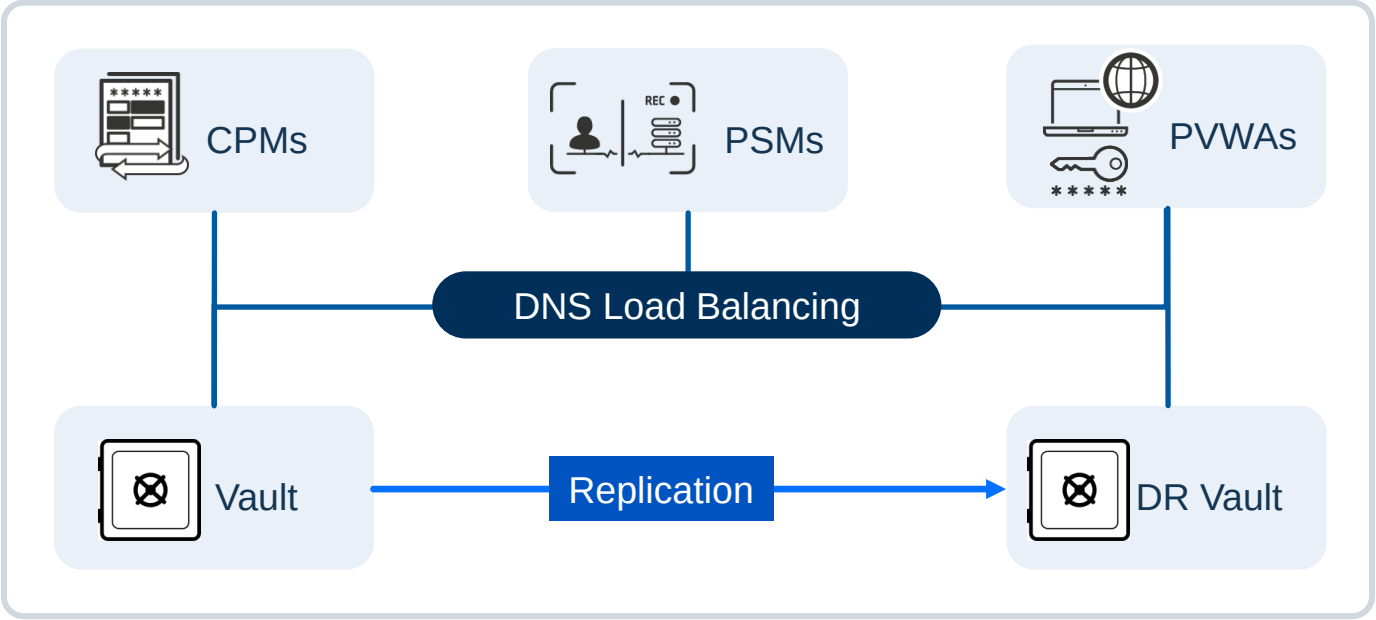
PVWA Failover Setup

- **PVWA** servers can be configured for automatic failover to allow users to access passwords without interruption
- Audit data should be saved via the activity log before re-enabling replication, however SIEM integration will mitigate this issue



DNS Load Balancing

- A possible approach to avoiding split-brain is to use a DNS Alias for the Vaults to control which Vault is used by the components
- The **DNS Alias** will be set in the ***Vault.ini*** file

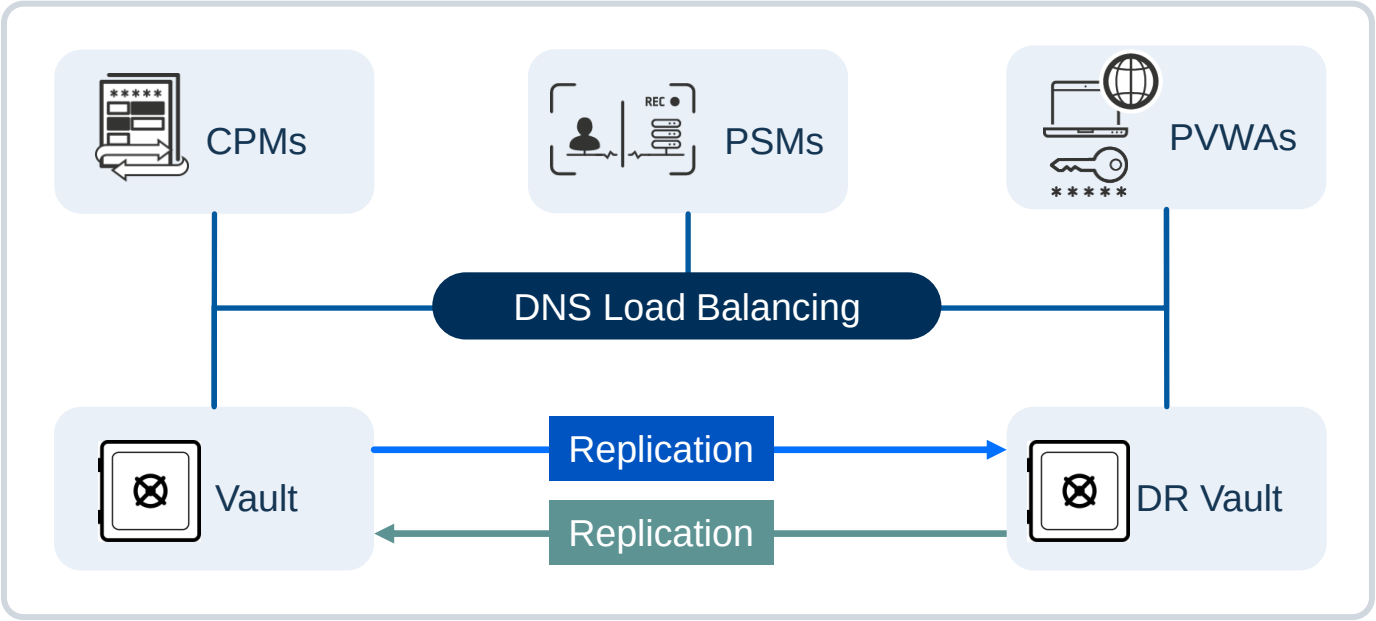


Remember that DNS Alias updates is a manual process and will extend the outage

Return to Primary Site

Return to Primary Site

- Data generated on the DR Vault should be replicated back to the Primary Vault before bringing it back online
- DNS Alias updates and failback replication are manual processes and will extend the outage



Restoring the DR Vault to DR 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 (this will force a full replication)
- Restart the DR service

padr.ini - Notepad

File Edit Format View Help

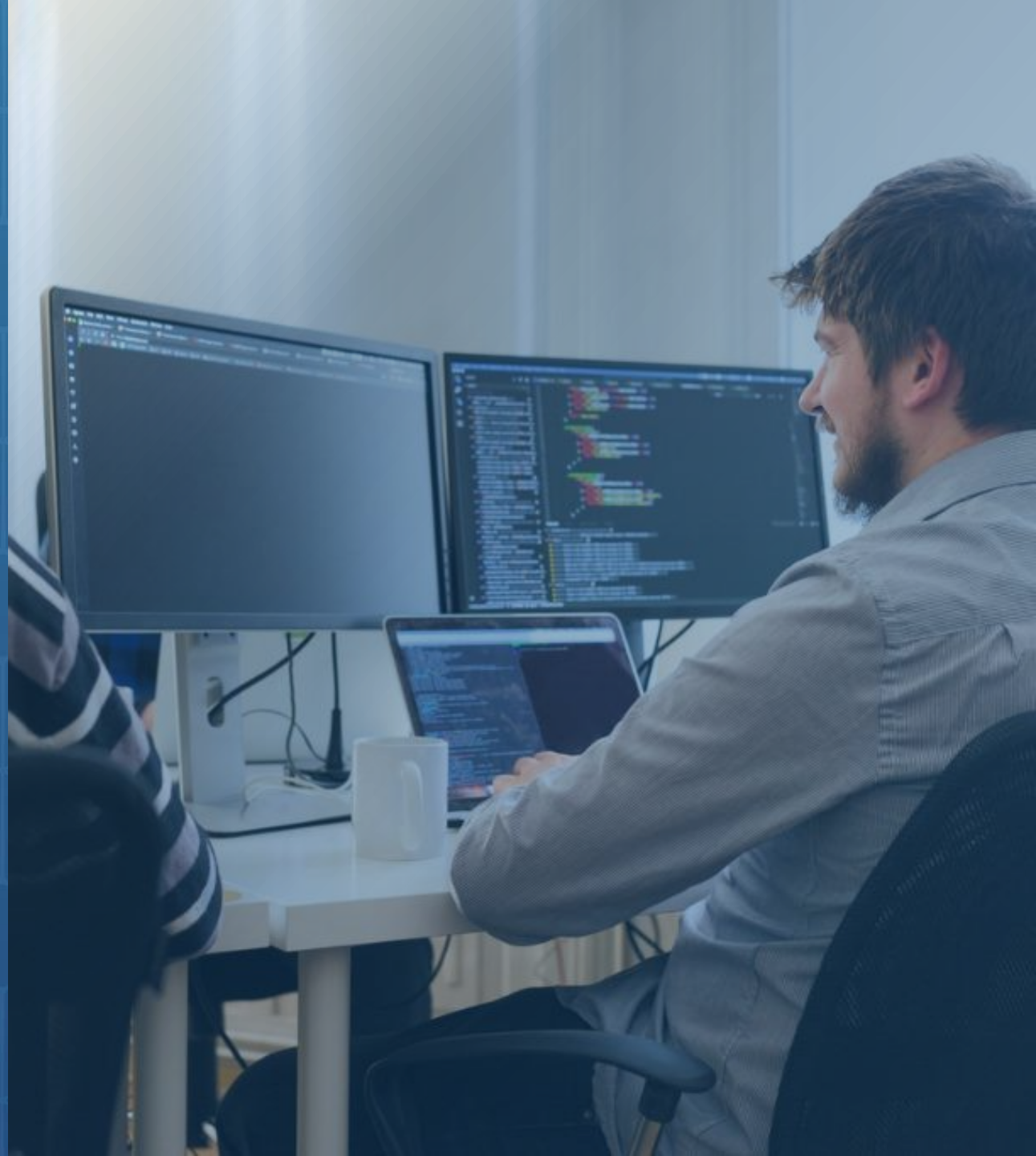
```
[MAIN]
ReplicateLogonFromFile="C:\Program Files (x86)\PrivateArk\PADR\Conf\user.ini"
EnableCheck=Yes
EnableReplicate=Yes
EnableFailover=Yes
EnableDbsync=Yes
CheckInterval=60
CheckRetriesCount=5
CheckRetriesInterval=30
ReplicateInterval=3600
ReplicateRetriesInterval=300
AccessVaultForInactivity=Yes
FailoverMode=No
```

Summary

Summary

In this session we covered the **CyberArk PAM Disaster Recovery** solution:

- Describe the CyberArk PAM Disaster Recovery solution
- Configure and test Disaster Recovery



You may now proceed to completing the following exercises:

Disaster Recovery

Step 1 – Enable Automatic Failover On The DR Vault

Step 2 – Execute A Full Replication To The DR Vault

Step 3 – Execute Automatic Failover Test

- Confirm Automatic Failover on the DR Vault
- Confirm Automatic Failover of PVWA and PSM

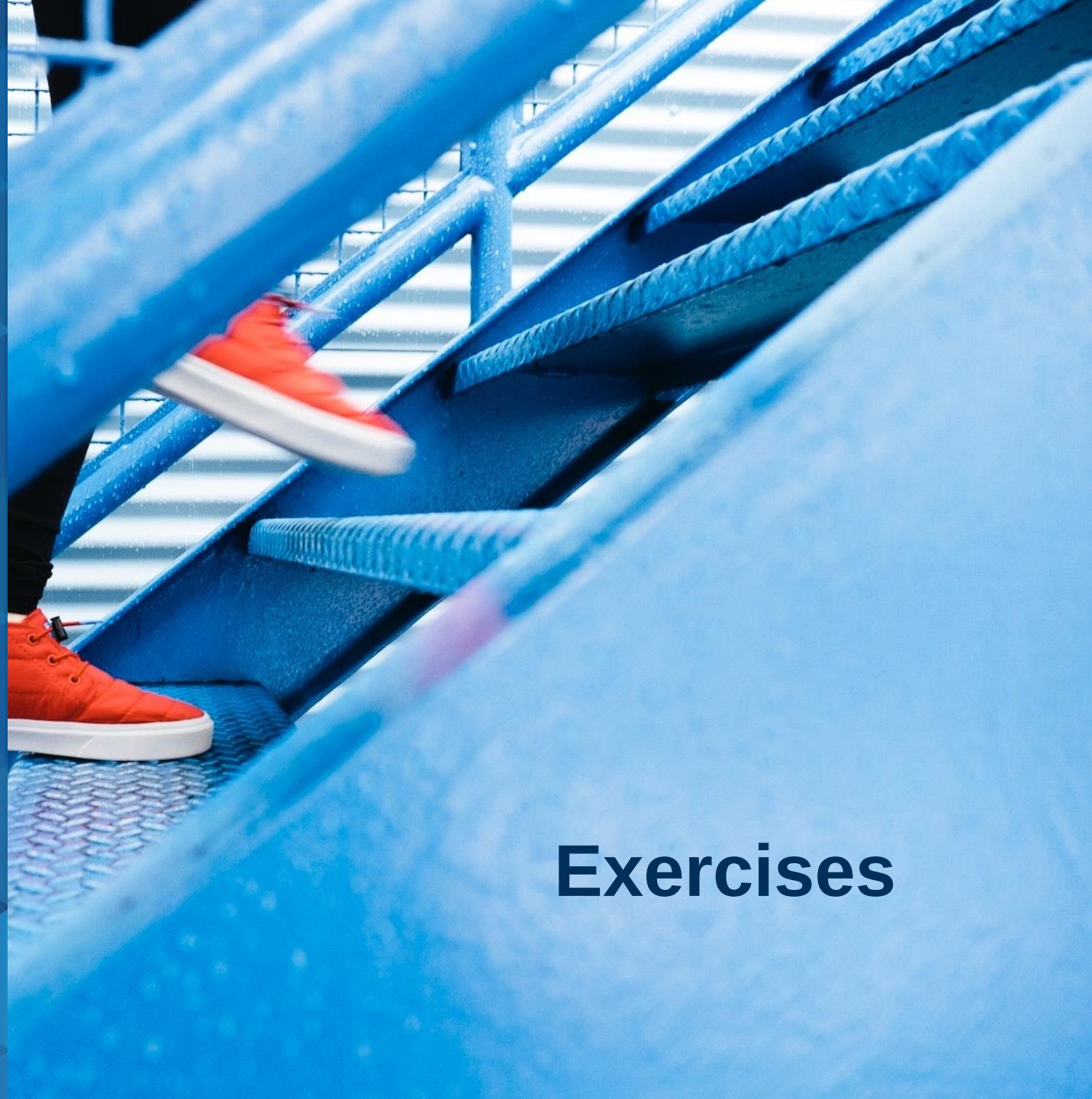
Step 4 – Execute a Full Replication back to the Primary Vault

Step 5 – Execute Failback Procedure by using Manual Failover

- Confirm Manual Failover on the Primary Vault

Step 6 – Set the DR Server back to DR mode

- Confirm Automatic Failover for PVWA and PSM



Exercises