

Restore From IFM

<https://github.com/ldapangel>

Contents

Restore From IFM	1
What is Restore From IFM ?	3
How it works	4
Requirements.....	6
Installation	8
Steps to recover a forest.....	9
Logging	15
Settings.....	15
Compilation.....	16
Limitations/What missing in this version.....	16
Issues/Enhancements	17

What is Restore From IFM ?

Restore from IFM (RIFM) is based on the excellent work by the author of DSInternals (<https://github.com/MichaelGrafnetter/DSInternals>), Michael Grafnetter and IMHO is the God of active directory !

One of the powershell commands that DSInternals has is New-ADDBRestoreFromMediaScript, which generates a powershell script that will take an IFM and restore this to server thus restoring to a domain controller.

I've taken what Michael has done and enhanced this in RIFM

- A console application which allows you to deploy an agent to each server to be restored in the forest. The console will also show each stage of the restore process as it progresses on each server being restored.
- An agent which once started performs the restore without the need of any further interaction and reports the status of the restore back to the console.
- Seizing FSMO roles if needed.
- Metadata clean-up in active directory of all servers which are not restored.
- RID pool increase
- DNS clean-up, so you can restore to servers with different IP addresses than the original active directory.
- Global catalog clean-up, so if your IFM backups from a multi domain forest were done at different times, the GC is rebuilt.

This tool can therefore be used to restore an active directory forest, providing you have at least one IFM for each domain in the forest. You can even use the tool to create an identical lab environment based on your production active directory in an isolated environment.

NOTE: This tool will only restore active directory, if you had other services such as DHCP, ADCS installed on the domain controller (BTW don't be a knobhead and install such services on a domain controller), these are not restored.

How it works

RIFM console is run on a workstation, such as Windows 11 or even Windows server 20xx.

You then define the domain controllers to be restored, needing only the following information :-

- Fully qualified domain name of the original domain controller e.g. dc01.myad.local
- IP address of the original domain controller
- New IP address i.e. the IP address of the server you are restoring this domain controller to

If the forest being restored is multi domain, then you must have at least one domain controller per domain.

You can of course have multiple domain controllers for each domain.

The agent (RIFMSvc and RIFMCore.dll) will then be deployed from the console to each server along with the DSInternals files. This is done by mapping a network drive and copying the files over this network drive. The agent will communicate back to the console over port 9000 UDP (port can be changed in the settings)

Once you start the process, the following steps happen on the server by the agent

- NTDS.DIT is opened and information extracted from it.
- NTDS.DIT is then mounted using dsmain.exe and information about the previous forest extracted.
- If the FSMO roles are on domain controllers which are being not restored, these are seized to one of the restored servers for each domain. The forest FSMO roles (schema and naming) will be restored to a domain controller in the root domain.
- Netbios over TCP/IP is disabled
- Windows Update service is disabled (as this can slow down the reboot processes)
- The server is then promoted to a domain controller
- The NTDS.DIT from the IFM is copied
- The SYSVOL from the IFM is copied
- The Bootkey is then replaced in IFM
- The LSA policy is reconfigured

- Registry settings are made
- The domain controller is rebooted
- As soon as LDAP services are available, the msDS-ReplicationEpoch is set to a random value which is different on all the servers being restored. This ensures that each domain controller being restored is isolated as various steps are being performed.
- DFSR services are restored
- KDC is stopped on all domain controllers except RID master
- DNS will be cleaned up, for any domain controllers not restored, their A record, SRV records, NS records will be removed. For the domain controllers restored, their IP address will be changed from the old to new IP address, delegations will be adjusted to restored domain controllers. Any AD conditional forwarders will be updated.
- Metadata clean up – all previous replication connections are deleted, domain controllers not restored are removed.
- Replication is set to intrasite on the sitelinks
- On the RID master the following steps are performed
 - RID pool increased by 100,000
 - RID pool invalidated
 - An account called DATempRIFM created and added to domain admins
 - Domain controller computer account is reset
 - msDS-ReplicationEpoch is set to a common value
 - DFSR is restarted
 - Restore on RID master is complete
 - Wait until all servers have completed restore
- On servers which are not the RID master, the following steps are performed
 - Wait until the RID master has signalled that it has completed
 - Domain controller computer account is reset and replicated to RID master
 - msDS-ReplicationEpoch is set to a common value
 - KDC is started
 - RID pool invalidated
 - DFSR is restarted
 - Restore is complete on this domain controller
 - Wait until all servers have completed restore

- When all servers have completed
 - Domain controller accounts are replicated
 - FSMO roles are replicated
 - Global catalog is dropped
 - KCC is initiated
 - Replication is forced in forest
 - Wait until successful replication

- When all restored domain controllers have signalled a successful replication
 - Global catalogs are reenabled
 - Site link options are restored
 - Netbios settings are restored
 - DATempRIFM account is deleted
 - Agent service stopped and disabled

Requirements

Each server that will be restored as a domain controller must already have the operating system installed on it. The operating system version must match the operating system version from which the IFM was taken

e.g. If the IFM was taken on the original domain controller which was running Windows 2019, then the server you are restoring this to must be Windows 2019. The edition e.g. standard vs enterprise does not matter.

The IFM must have already been copied to the server and MUST be in a directory C:\IFM

A local admin account is used to deploy the agent. This must be the same on each server and have the same password on each server. Its best to use the built in Administrator account, however if you create your own account make sure you add this to the local administrators group and also set LocalAccountTokenFilterPolicy registry setting (<https://learn.microsoft.com/en-us/troubleshoot/windows-server/windows-security/user-account-control-and-remote-restriction>)

.NET Framework 4.7.2 or above must be installed already on the server

The ADDS role can be installed, but the server MUST not already be a domain controller. If the ADDS role is not installed, RIFM will install.

The firewall should be disabled on the workstation where RIFMConsole is running. This will allow the console to communicate with the agents.

No antivirus software should be installed on the server. We are trying to recover an active directory and any software that may interfere with this process may impede this process !

DNS must be hosted as an integrated DNS zone in the original forest.

FRS has been eliminated and only DFSR is running in the original forest.

RODC's cannot be restored

Installation

There is no installation required on the servers that will become domain controllers

On the workstation where you will run the console

Create a directory (e.g. C:\RIFM) and copy the following files

- RIFMConsole.exe
- RIFMCore.dll
- RIFMCore.pdb
- RIFMSvc.exe

Download DSInternals Version 5.1 from <https://github.com/MichaelGrafnetter/DSInternals>

https://github.com/MichaelGrafnetter/DSInternals/releases/download/v5.1/DSInternals_v5.1.zip

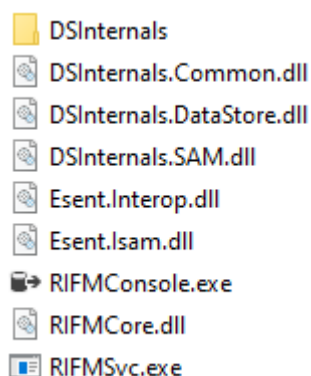
Unblock the download zip file

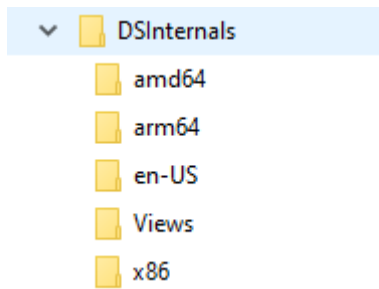
Extract the zip file and copy the DSInternals directory to the directory where you copied RIFMConsole.exe (e.g. C:\RIFM)

Also copy just the following files to the same directory you copied RIFMConsole.exe from the DSInternals directory.

- DSInternals.Common.dll
- DSInternals.DataStore.dll
- DNInternals.SAM.dll
- Esent.Interop.dll
- Esent.Isam.dll

You should then have a directory structure





Make sure the firewall on this workstation/server where RIFM console is running is able to communicate with the agents that will be installed on the servers.

The following ports will need to be opened to allow inbound communication from the agent to the console

- UDP 9000 (can be changed in the settings)

You can use the following PS script

```
New-NetFirewallRule -Name RIFMAgent -DisplayName RIFMAgent -Direction Inbound -Protocol UDP -LocalPort 9000 -RemoteAddress 192.168.4.120, 192.168.4.121, 192.168.4.122
```

The above command will allow the agent on servers 192.168.120 to 192.168.4.122 to communicate back to the console.

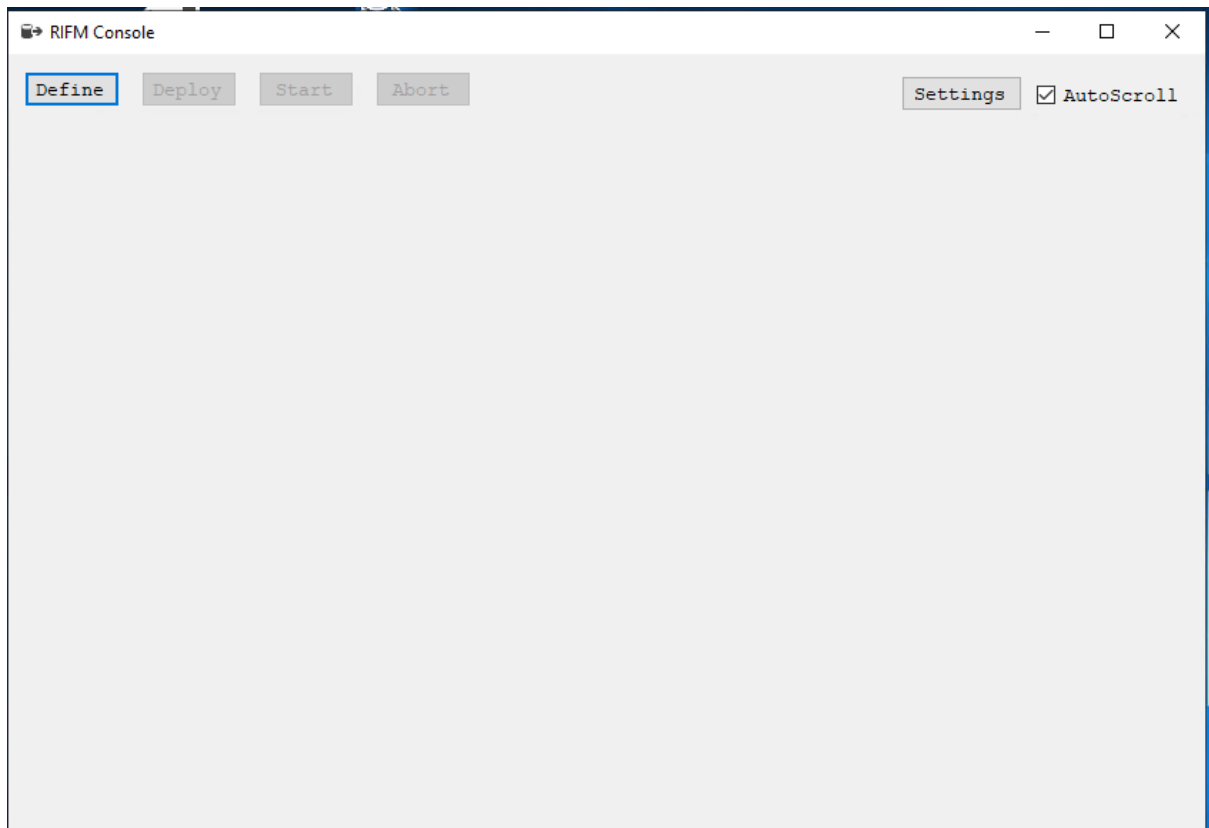
Steps to recover a forest

Prepare you servers that the forest will be recovered to

- Install the OS – this must be the same version as the domain controller being recovered
- You must have an administrator or equivalent account on all servers that is the same with the same password

On a workstation, follow the installation steps to install the RIFM console

Start RIFMconsole.exe



Select Define



Right click the mouse to bring up the menu



Select Add

Enter the fqdn of the domain controller to be restore e.g. mydc.myad.local

Enter the old IP address i.e. the IP address that this domain controller had in the original forest

Enter the new IP address i.e. the IP address of the server this domain controller will be restored to.

To edit or delete an existing entry, just select the entry and select edit/delete.

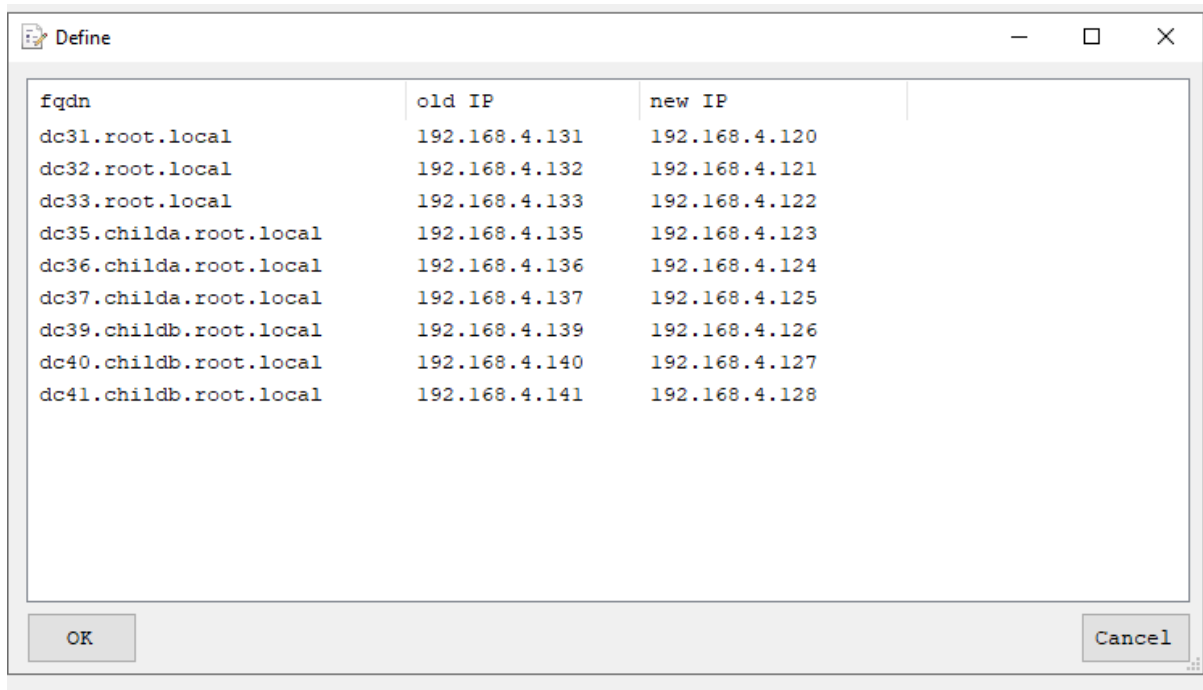
You can also load and save the entries defined in a file. The format is a simple text file, with one line per server

fqdn,oldIP,newIP

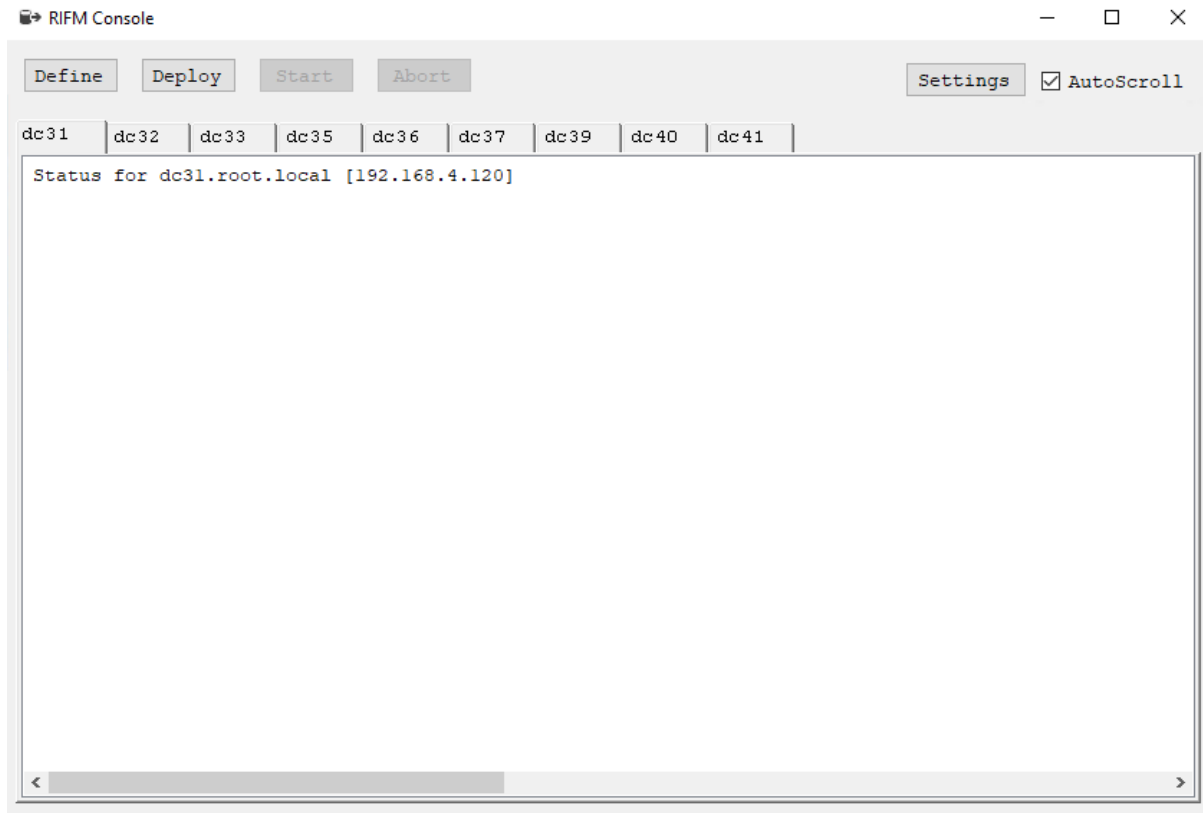
e.g.

mydc.myad.local,192.168.1.100,192.168.2.200

define all the servers you wish to recover

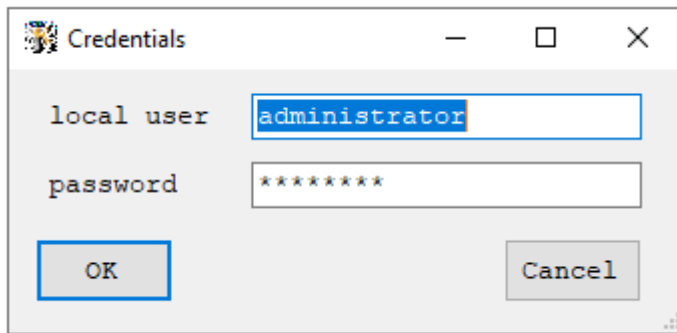


A separate tab will be created for each server to be restored

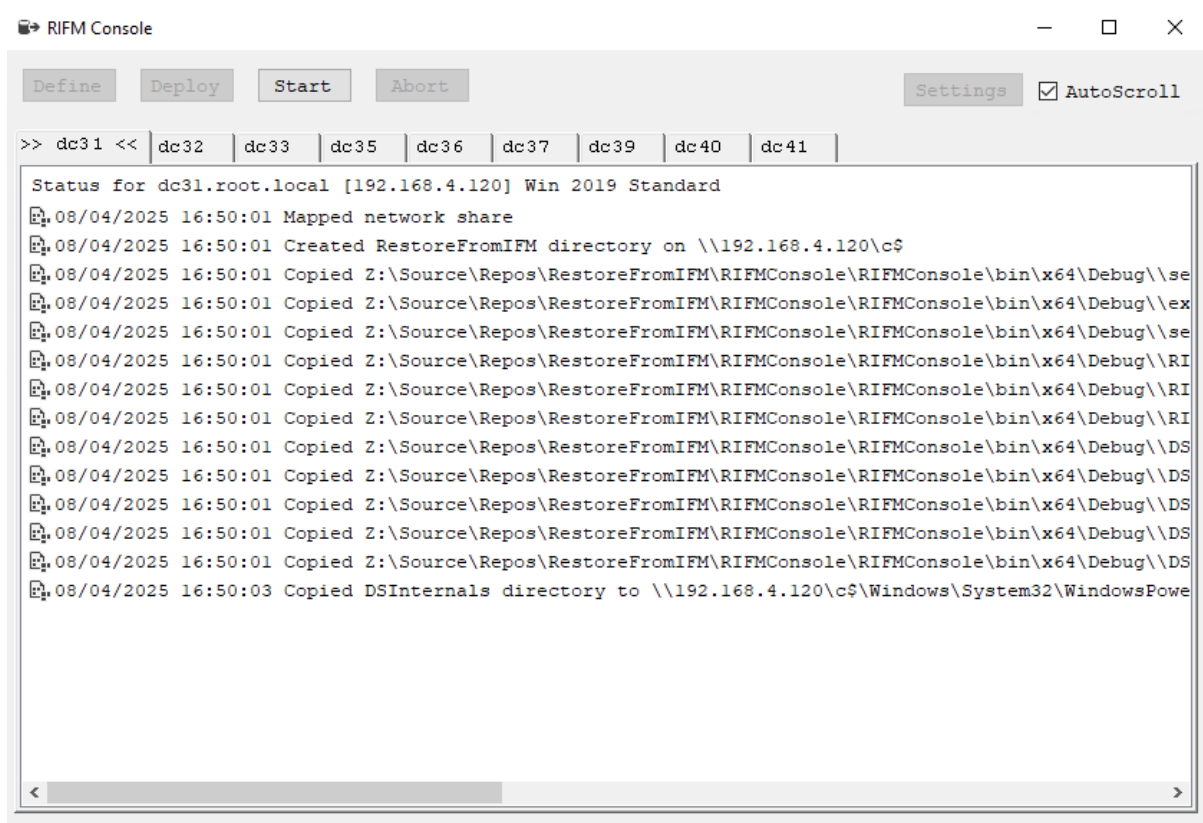


Adjust any settings as required

Select Deploy, enter the local administrator credentials

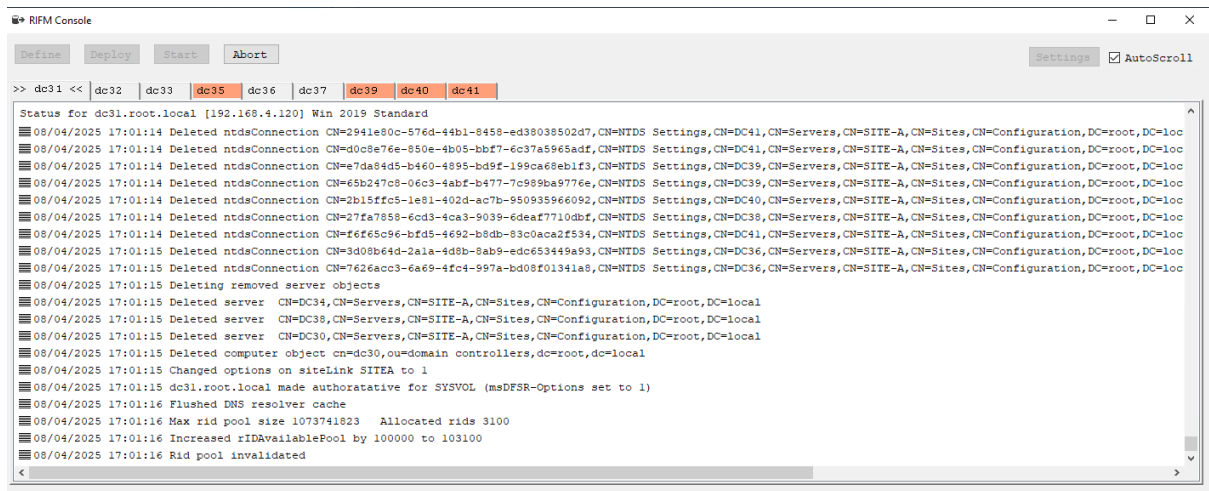


the agent will be deployed to each server



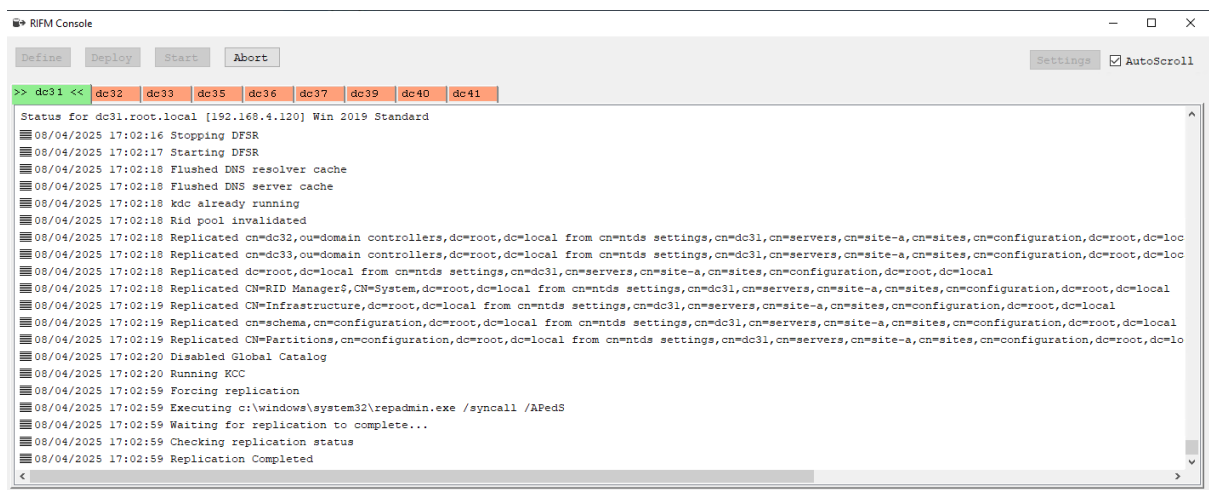
Select Start and sit back and watch as the magic happens

The tab colour will change at two milestones



```
>> dc31 << | dc32 | dc33 | dc35 | dc36 | dc37 | dc39 | dc40 | dc41 |
Status for dc31.root.local [192.168.4.120] Win 2019 Standard
08/04/2025 17:01:14 Deleted ntdsConnection CN=2941e80c-576d-44b1-8458-ed38038502d7,CN=NTDS Settings,CN=DC41,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=loc
08/04/2025 17:01:14 Deleted ntdsConnection CN=d0c8e76e-850e-4b05-bbf7-6c37a5965adf,CN=NTDS Settings,CN=DC41,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=loc
08/04/2025 17:01:14 Deleted ntdsConnection CN=e7da84d5-b460-4895-bd9f-199ca68eb1f3,CN=NTDS Settings,CN=DC39,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=loc
08/04/2025 17:01:14 Deleted ntdsConnection CN=65b247c8-06c3-4abf-b477-7c989ba9776e,CN=NTDS Settings,CN=DC39,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=loc
08/04/2025 17:01:14 Deleted ntdsConnection CN=2b15ffc5-1e81-4024-ac7b-950935966092,CN=NTDS Settings,CN=DC40,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=loc
08/04/2025 17:01:14 Deleted ntdsConnection CN=27fa7858-6cd3-4ca3-9039-6deaf7710dbf,CN=NTDS Settings,CN=DC38,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=loc
08/04/2025 17:01:14 Deleted ntdsConnection CN=f6f65c96-bfd5-4692-b8db-83c0aca2f534,CN=NTDS Settings,CN=DC41,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=loc
08/04/2025 17:01:15 Deleted ntdsConnection CN=3d08b64d-2a1a-4d8b-8ab9-edc653449a93,CN=NTDS Settings,CN=DC36,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=loc
08/04/2025 17:01:15 Deleted ntdsConnection CN=7626acc3-6a69-4fc4-997a-bd08f01341a8,CN=NTDS Settings,CN=DC36,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=loc
08/04/2025 17:01:15 Deleting removed server objects
08/04/2025 17:01:15 Deleted server CN=DC34,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=local
08/04/2025 17:01:15 Deleted server CN=DC38,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=local
08/04/2025 17:01:15 Deleted server CN=DC30,CN=Servers,CN=SITE-A,CN=Sites,CN=Configuration,DC=root,DC=local
08/04/2025 17:01:15 Deleted computer object cn=dc30,ou=domain controllers,dc=root,dc=local
08/04/2025 17:01:15 Changed options on siteLink SITEA to 1
08/04/2025 17:01:15 dc31.root.local made authoratative for SYSVOL (msDFS-Options set to 1)
08/04/2025 17:01:16 Flushed DNS resolver cache
08/04/2025 17:01:16 Max rid pool size 1073741823 Allocated rids 3100
08/04/2025 17:01:16 Increased rIDAvailablePool by 100000 to 103100
08/04/2025 17:01:16 Rid pool invalidated
```

This indicates the restore process has completed on this server and its now waiting for all restores on other servers to complete



```
>> dc31 << | dc32 | dc33 | dc35 | dc36 | dc37 | dc39 | dc40 | dc41 |
Status for dc31.root.local [192.168.4.120] Win 2019 Standard
08/04/2025 17:02:16 Stopping DFSR
08/04/2025 17:02:17 Starting DFSR
08/04/2025 17:02:18 Flushed DNS resolver cache
08/04/2025 17:02:18 Flushed DNS server cache
08/04/2025 17:02:18 kdc already running
08/04/2025 17:02:18 Rid pool invalidated
08/04/2025 17:02:18 Replicated cn=dc32,ou=domain controllers,dc=root,dc=local from cn=ntds settings,cn=dc31,cn=servers,cn=site-a,cn=sites,cn=configuration,dc=root,dc=loc
08/04/2025 17:02:18 Replicated cn=dc33,ou=domain controllers,dc=root,dc=local from cn=ntds settings,cn=dc31,cn=servers,cn=site-a,cn=sites,cn=configuration,dc=root,dc=loc
08/04/2025 17:02:18 Replicated dc=root,dc=local from cn=ntds settings,cn=dc31,cn=servers,cn=site-a,cn=sites,cn=configuration,dc=root,dc=local
08/04/2025 17:02:18 Replicated CN=RID Manager,CN=System,dc=root,dc=local from cn=ntds settings,cn=dc31,cn=servers,cn=site-a,cn=sites,cn=configuration,dc=root,dc=local
08/04/2025 17:02:19 Replicated CN=Infrastructure,dc=root,dc=local from cn=ntds settings,cn=dc31,cn=servers,cn=site-a,cn=sites,cn=configuration,dc=root,dc=local
08/04/2025 17:02:19 Replicated cn=schema,cn=configuration,dc=root,dc=local from cn=ntds settings,cn=dc31,cn=servers,cn=site-a,cn=sites,cn=configuration,dc=root,dc=local
08/04/2025 17:02:19 Replicated CN=Partitions,cn=configuration,dc=root,dc=local from cn=ntds settings,cn=dc31,cn=servers,cn=site-a,cn=sites,cn=configuration,dc=root,dc=lo
08/04/2025 17:02:20 Disabled Global Catalog
08/04/2025 17:02:20 Running KCC
08/04/2025 17:02:59 Forcing replication
08/04/2025 17:02:59 Executing c:\windows\system32\repadmin.exe /syncall /APedS
08/04/2025 17:02:59 Waiting for replication to complete...
08/04/2025 17:02:59 Checking replication status
08/04/2025 17:02:59 Replication Completed
```

This domain controller has completed replication with other servers and is now waiting for all servers to complete replication.

UDP Port	<p>This is the port that the console communicates over to the agent running on the server.</p> <p>It's also the same port that the agent communicates back to the console</p>
Common ePoch	<p>Each server as its being restored will be isolated to other servers to ensure replication does NOT happen.</p> <p>When all servers have successfully restored, replication will be enabled and the common ePoch is the replication epoch that is set to ensure they can all replicate with each other.</p>
DSRM Password	The DSRM password that will be assigned to each restored server

Compilation

Although the binaries have been provided, you may wish to compile the code yourself after reviewing the code or maybe you have adjusted the code to suit your needs.

I complied this with

- Visual Studio 2019
- .NET Framework 4.6.2
- DSInternals version 5.1

Limitations/What missing in this version

Test out in you labs and provide feedback on any issues you encounter or any enhancements you would like to see.

This initial version does not handle if one of the servers to be promoted fails during the restore process. In the current version, if one fails (e.g. rename fails) then the whole process fails. This feature to continue if one fails will be added in due course.

DNS must be AD integrated and data for DNS present in the ForestDnsZones and DomainDnsZones.

Any conditional forwarders must be AD integrated.

RODC's cannot be restored, they must be repromoted.

Issues/Enhancements

Log these via Github