HITACHI
Inspire the Next

Hitachi Dynamic Replicator - Scout File Server Solution

Hitachi Data Systems

MK-98DF8225-00

Contents

Conventions

Keywords, command buttons and other such fields are enclosed in " "while being bold (for example, to denote 

"**Next**" is used)

Inputs for commands and Variables are shown in ***Italics***
File names and paths are shown in **bold**
Commands are shown in **`Courier new font`**
Mandatory keywords, arguments and inputs are enclosed within < >.
Optional arguments are enclosed in [ ]

 **Notes:**

Contain suggestions or tips.

 **Caution:**

Contains critical information

1 How this solution works

1.1 Concept of failover failback

With rise in the number of File server users, the need to address the risk of downtime has become a priority. This risk can be addressed through Scout file server solution. This is possible by failing over to the DR server while the production file server is down. The following picture shows failover of a production file server to a DR server.

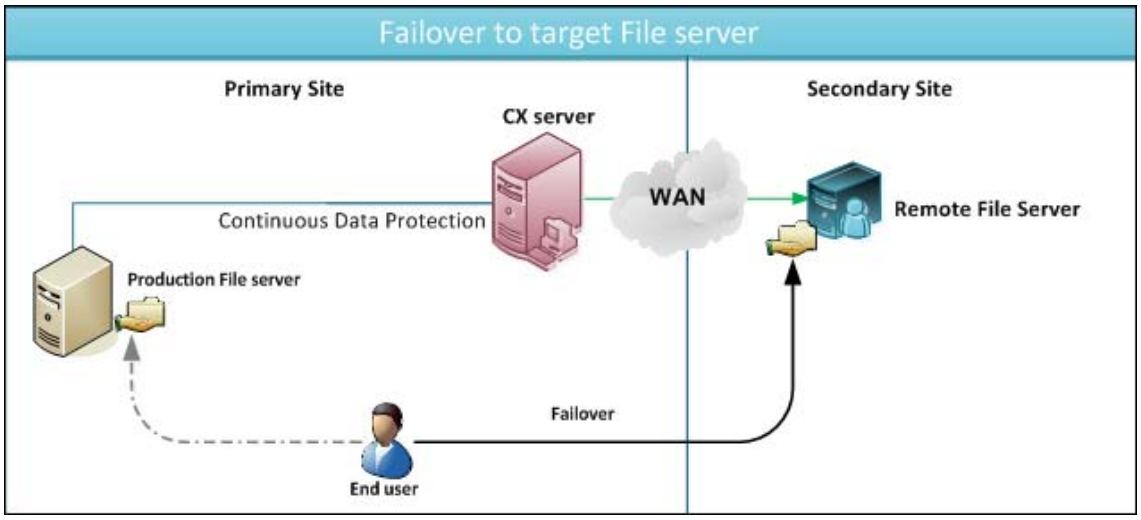

Figure 1:

Rather than just maintaining a backup, the DR server can replace the production server during outage. All the shared folders, files will be shared on the DR server as well. This failover process will be transparent to the end users. Once the production server has recovered from the outage a failback can be performed which again is end user transparent. **Please note that Hitachi Dynamic Replicator - Scout does not currently support fabric-based solutions.**

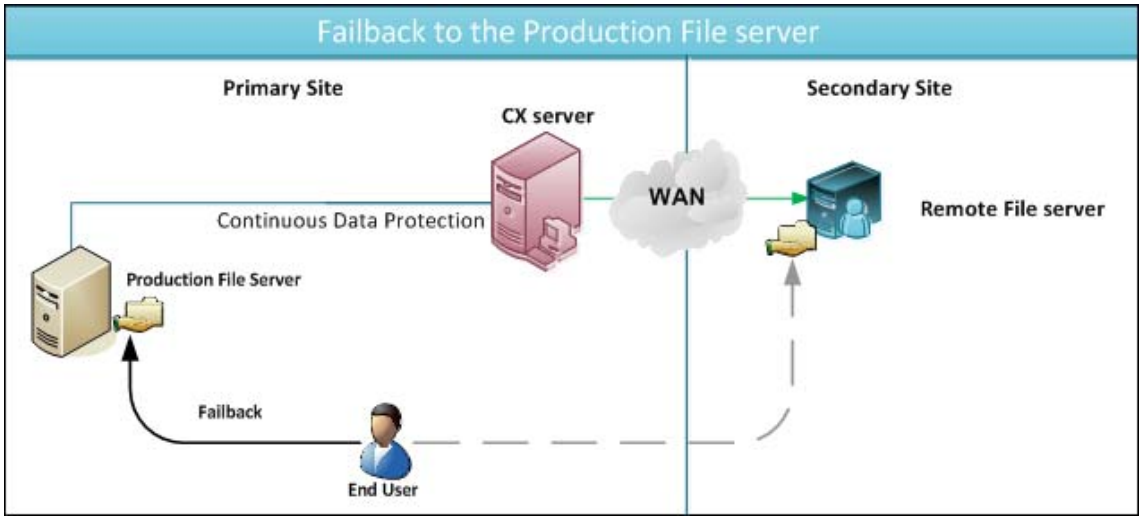

Figure 2:

1.2 Protecting File server

File Server can be protected in two different ways i.e. FX agent services running under Domain user or Local System account. File server is protected in four steps i.e. Discovery, VX Replication, Consistency, and Recovery. Before protecting a file server determine if the FX agent is going to be started with a special user as explained in Privileges for File server failover and failback section on page 14 or local system account. (Refer section Determine FX Agent Service User on page 12.

When FX agent is started with local system privilege then an additional step is performed while protecting the file server

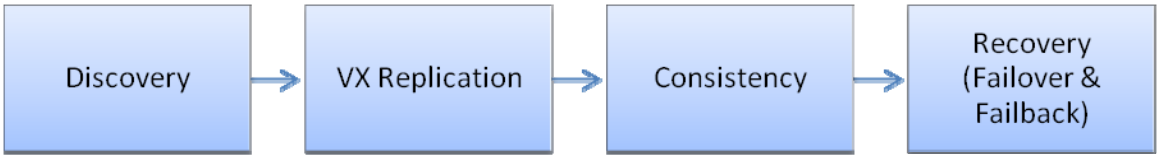

Figure 3

Discovery
After the volumes are replicated, perform a discovery job. This will scan the production server for all the "shared" information and restore it on the DR server.

VX Replication
In this step the production file server volumes are replicated to the DR file server with CDP retention enabled. Only the shares/folders on the replicated volumes are protected.

Consistency
File system consistency tags are issued at regular intervals through the FX job which internally calls the vacp.exe on the production server.

Recover
File Server can be recovered either through Planned Failover, Un-Planned Failover and Failback.

1.3 File Server failover

There are two types of failovers; the first is a planned failover where the production server is prepared for a failover and then a failover is performed. The second is an unplanned failover where the production server is not considered (assuming that the production server is unreachable). Both types of failovers may be performed either through FX jobs (CX UI) or through CLI

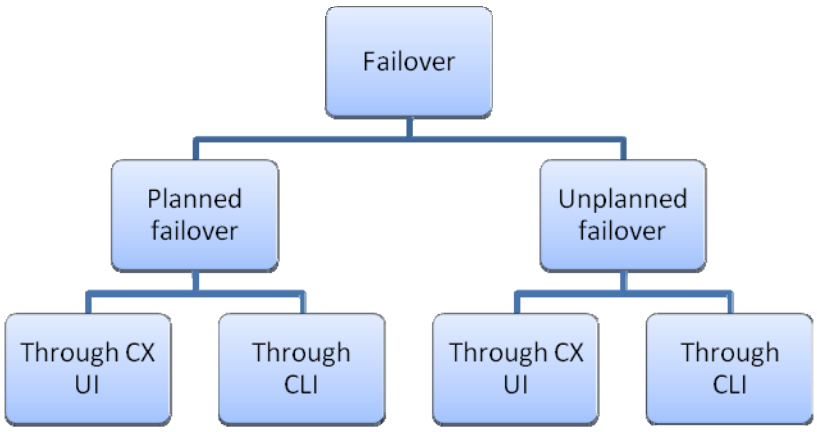

Figure 4

A planned failover is primarily used when the production exchange server and the CX server both are reachable by the DR exchange server. An ideal example is a logical corruption on the production server, DR drills or any planned outages.

An unplanned failover on the other hand is performed when:

- The production server is unreachable and CX server is up and running
- The production server and the CX server are both unreachable

Differences between planned and unplanned failover

Table 1: Differences between unplanned failover and planned failover

	Unplanned failover	Planned failover
When to use	Real-time outages or unexpected outages	Mock drills, To test the setup. Any expected outages
Recovered to	To latest consistent tag common for all file server replication pairs	Issues a consistency tag on the File server volumes. Target is recovered to the same consistent tag.
Performed through CX UI	Yes, unless the CX is down.	Yes
Performed through CLI	Yes	Yes

1.4 File server failback

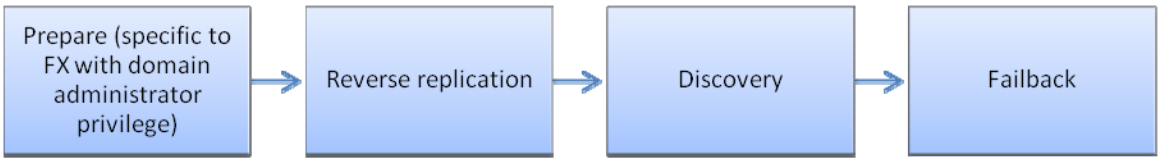

Figure 5

Prepare
A failback is performed when the production server is back online and ready to take over from the DR file server. The FX agent refuses to start post failover when it is configured with domain administrator privileges. This is because the host SPN entries are missing on the production server. You may add the host SPN entry back to the production host in this step.

Reverse replication
A reverse replication is performed to update the production server with all the data changes occurred during its outage.

Discovery
After data replication, proceed to perform a discovery to sync the latest shared folder information

Failback
A failback is performed through the FX job. This will restore the production server back to its original state with all the data and shared updates.

1.5 FX templates involved

Name of the template	Purpose	When is it used	Misc
FileServer Discovery	To discover Shared information on the production server	Discovery job is performed after setting the replication pairs or after any share level changes on the production server.	Exchange Discovery is required to perform an unplanned failover at a later time
FileServer Consistency	To issue file system consistency tags on the production volumes	After the VX replication pair has reached differential Sync	Consistency is required at least once to perform an unplanned failover at a later time
FileServer Failover Without Retention	To perform file server failover for replication pairs without CDP retention	Used while the pair is in Differential sync for pairs without CDP retention.	
File server planned Failback	To perform a planned Failback	Used after a failover	
File server planned Failover	To perform a planned failover	To test the DR setup, mock drills etc	
File server unplanned Failover	To perform an unplanned failover	When the production server is down	Ensure that you select the source and target as the DR server when the production server is down

2 Prerequisites

- Ensure that firewall is not blocking any of the Scout components
- Ensure VX agents are installed on both the source and target hosts
- Install CX configuration server within the same LAN as of the source host
- Point all Process servers, VX, FX agents to the same CX server and assign appropriate licenses.
- FX agent may be started with Domain administrator privileges or Local System account. The table below shows the differences in the steps to be performed when FX is running under domain administrator privileges or with local system privileges.

2.1 Determine FX Agent Service User

FX agent may be started with Domain administrator privileges or Local System account. The table below shows the differences in the steps to be performed when FX is running under domain administrator privileges or with local system privileges. When the FX service is configured to run with local system privileges, you will need to enter the domain administrator credentials or the special user created under the section Privileges for File server failover and failback on page 14. Refer section Storing Domain User Credentials (FX up with local system account) on page 13.

Table 2

Phase of solution	FX up with Domain administrator privileges	FX up with Local System privileges
Protecting	File server is protected in three steps: • VX replication • Discovery • Consistency	File server is protected in four steps: • VX replication • Discovery • Consistency • Store encrypted domain credentials through winop.exe.
Failover	No need to edit the FX job setting	Need to append the source prescript and target post script with the "–useuseraccount" switch
Failback	After failover, add the SPN entries back to the production File server from DR File server through winop.exe	The failback FX job's source prescript and target post script need to be appended with the "–useuseraccount" switch

Notes:

While performing a failover or a failback through CLI, you may use –failover with the –ip switch Or
Use the –failback switch

Caution:

For clustered environment, always run the FX service with domain administrator privileges.

2.2 Storing Domain User Credentials (FX up with local system account)

This step is required only when the FX agent is configured to run with local system account privileges. Access the production file server's command prompt, and then navigate to the VX agent installation path to issue the following command

```
Winop security –encrypt
```

You will be prompted for three inputs, the domain name, domain user name and corresponding password.

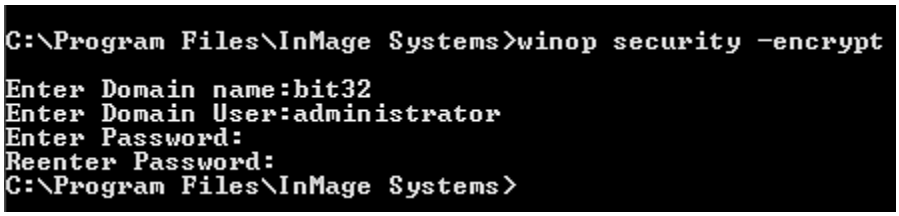

Figure 6

Notes:

The user name entered here should either be the special user created under the section Privileges for File server failover and failback on page 14 or the domain administrator.

Similarly repeat the same process on the DR file server. Whenever this user's password changes, ensure that you repeat this step on both the production and DR file servers.

2.3 Privileges for File server failover and failback

2.3.1 Introduction

The FX agent plays a critical role while performing a failover or a failback. It is important that the FX agent on both production and DR servers have appropriate privileges. It is always recommended that you create a special user with appropriate privileges and start the FX agent with that user's privileges.

This part describes the process to create a user with appropriate privileges require for the FX agent to start. It also describes the granular permissions required to allow the InMage service to successfully perform a file server failover and failback. To set privileges you need to create domain user first then full control over the DNS for each source and target. The process involved is:

- Create a Domain User
- Add this domain user to the Production Server and DR Server record in DNS Server management console to give local administrator privileges.
- Add this user to Production Server and DR Server in Active Directory using ADSI Edit and give full permissions.

 **Notes:**

You will need domain administrator privileges for following the steps given below.

Detailed procedure to set privileges is as follows.

2.3.2 Create a Domain User

Step 1. Log on to the domain controller as a domain administrator where Production Server and DR Server are part of the domain.

Step 2. Click on **"Start->Programs->Administrative Tools ->Active Directory Users and Computers".**

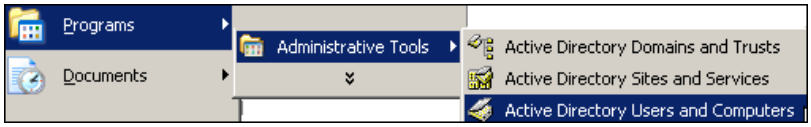

Figure 7:

Step 3. You should now see the "**Active Directory Users and Computers"** window. Under "**Active Directory Users and Computers",** select **"Domain Users",** a list of users appears on the right hand side, right click, and select **"New->User"**.

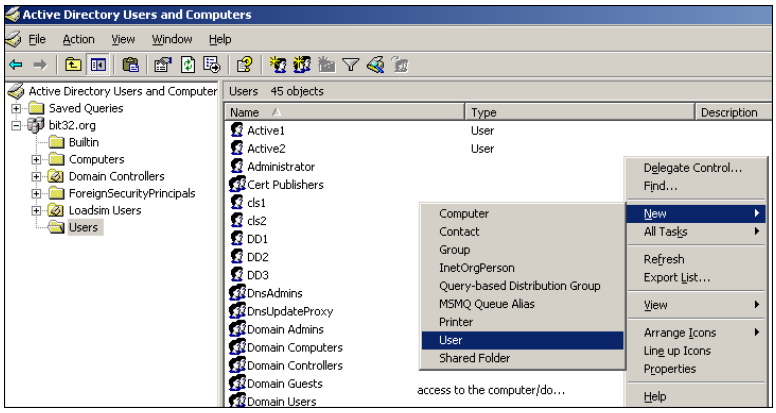

Figure 8:

Step 4. You should now see the **"New Object-User"** screen. Enter the **"Name"** and **"User Logon Name"** then click on **"Next"**. For this example "**InMageUser**" is used for first name and user logon name.

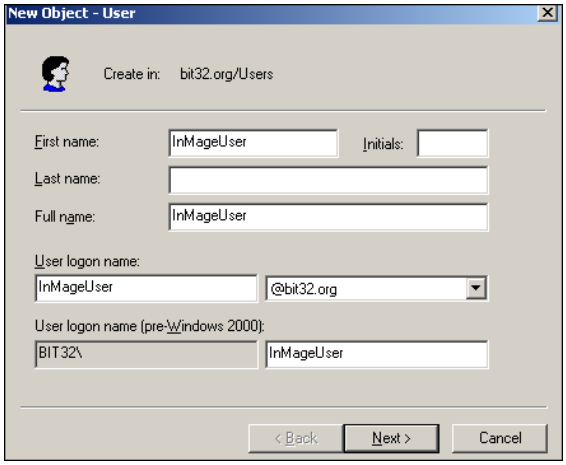

Figure 9:

Step 5. Enter the **"Password"** and enable the **"Password Never Expires"** check box. A dialog box appears indicating that you will not be required to change the password at next logon, click on **"OK"** then click **"Next"**.

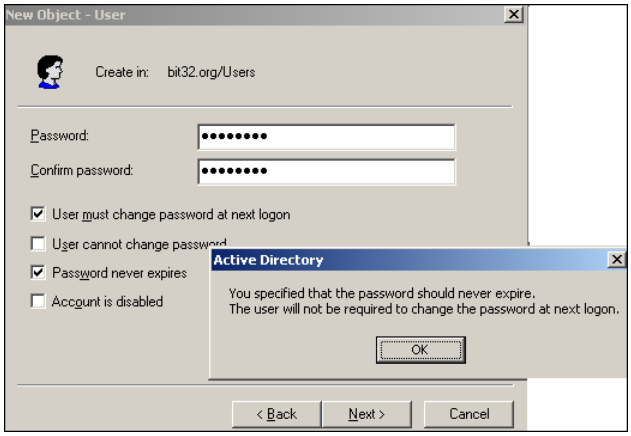

Figure 10:

Step 6. You should now see the user name details and click on **"Finish"**.

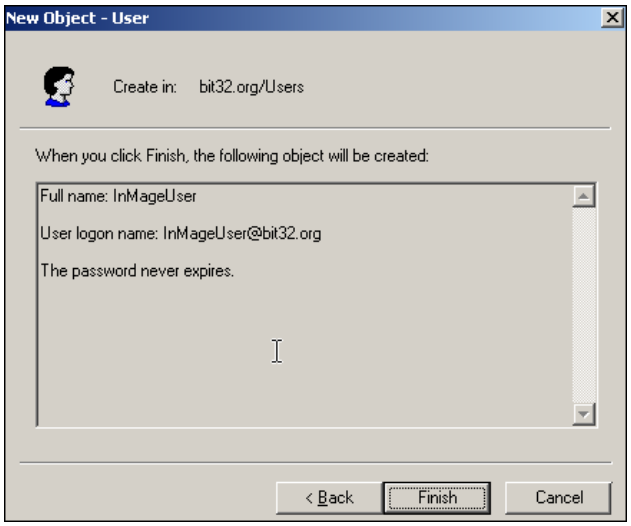

Figure 11:

2.3.3 Permission for DNS Record Change

Step 1. Click on "**Start->Run**" then type **"dnsmngmt.msc**" and hit enter. You should see the DNS management screen. Expand the **"Domain"** then right click on the production host to click on the **"Properties"**.

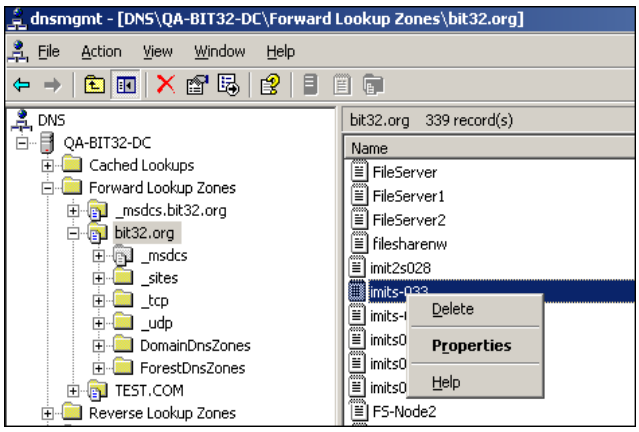

Figure 12:

Step 2. You should see the source host properties screen. Click on the **"Security"** tab. Click on **"Add"**.

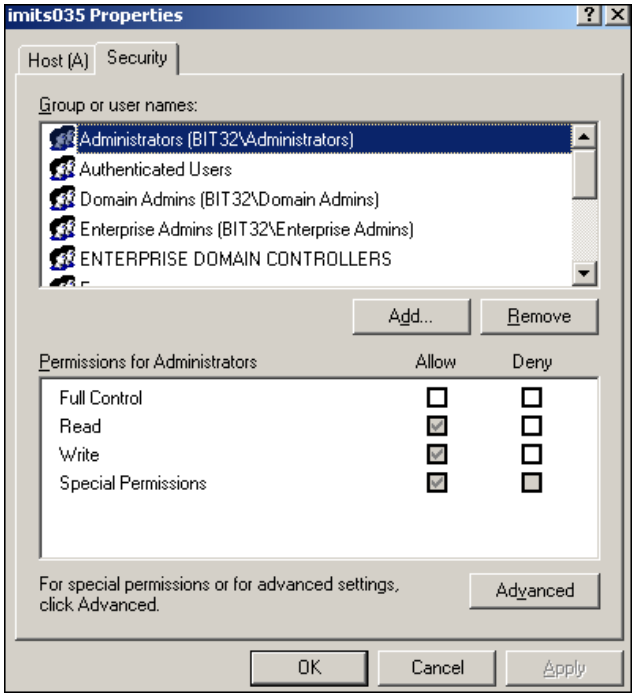

Figure 13:

Step 3. You should see the **"Select Users, Computers, or Groups"** screen. Select the domain user name (InMageUser) created in the previous steps and check if this username is available or not by clicking on the **"Check Names"**. Click on "**OK**".

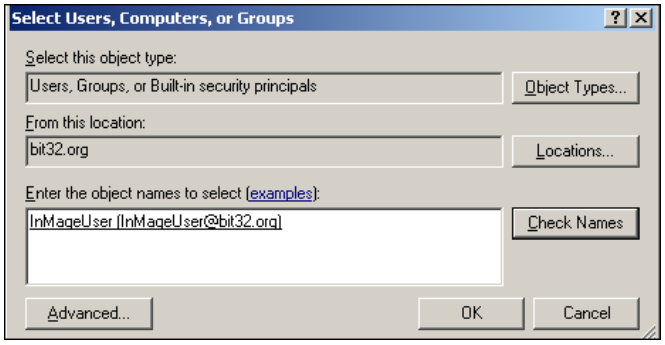

Figure 14:

Step 4. You should be able to see the previous screen. Click on **"Full Control"** check box. Click on **"OK".** Repeat the same process for the DR server

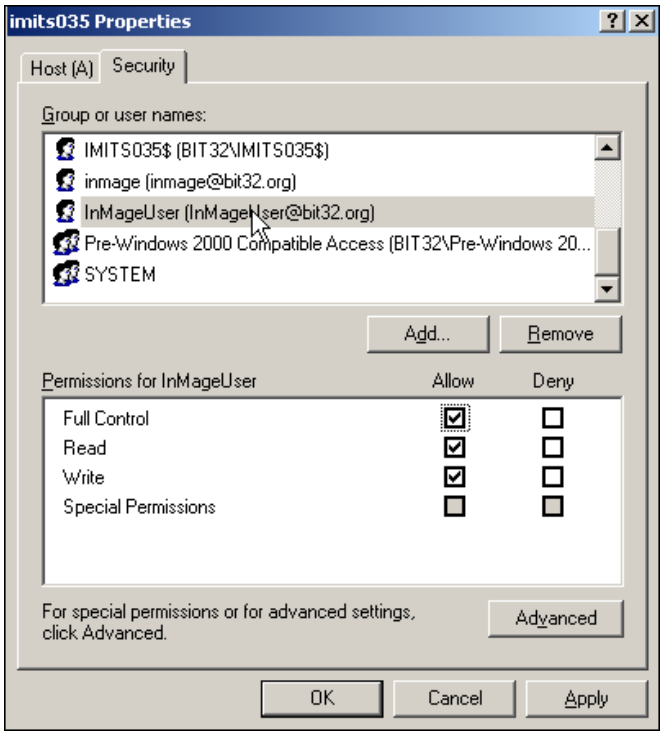

Figure 15:

Notes:

In Cluster case, you need to select the network name (Virtual Server Name) and give DNS privileges by repeating steps 1 to 4.

2.3.4 Permission for AD Changes

Step 5. Click **"Start->Run->MMC"**, select **"Add/Remove Snap"**-from File Menu, and Click on **"Add"**.

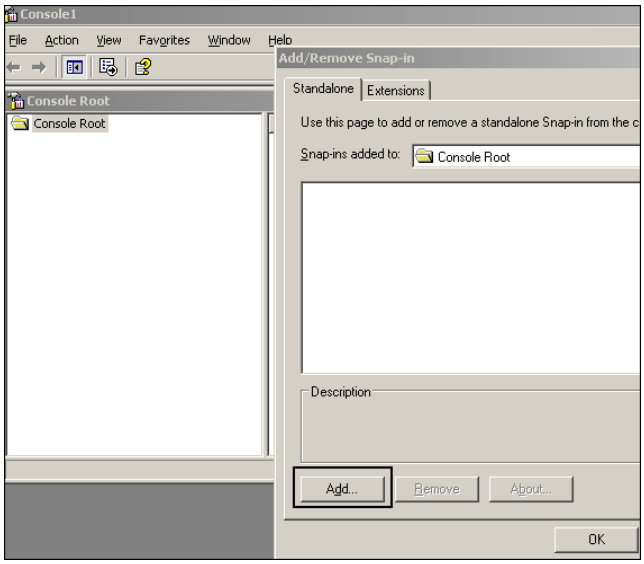

Figure 16:

Step 6. You should see an **"Add Standalone Snap-in"** screen, select **"ADSI Edit"**, and click on **"Add"**.

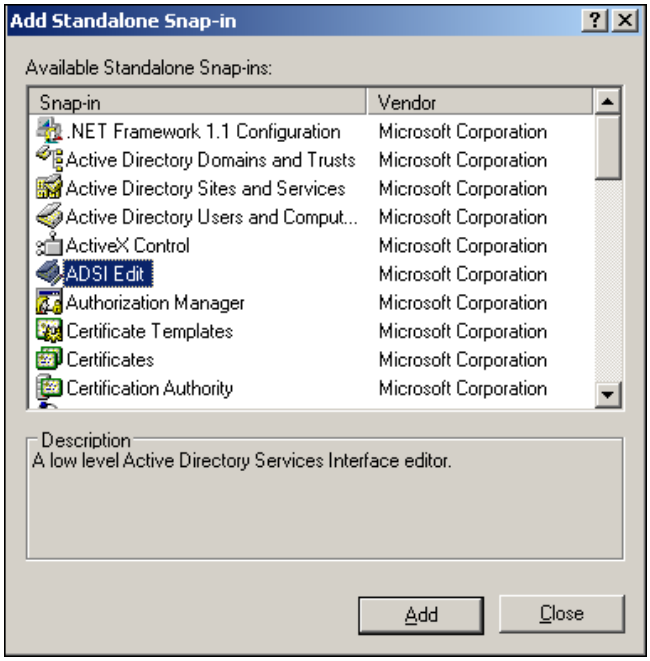

Figure 17:

Notes:

You need to install "ADSI Edit" before you add it in "Add Standalone Snap-in" (This is available in Windows Support Tools)

Step 7. You should be able to see **"Add/Remove Snap-in"** screen and click on **"OK"**.

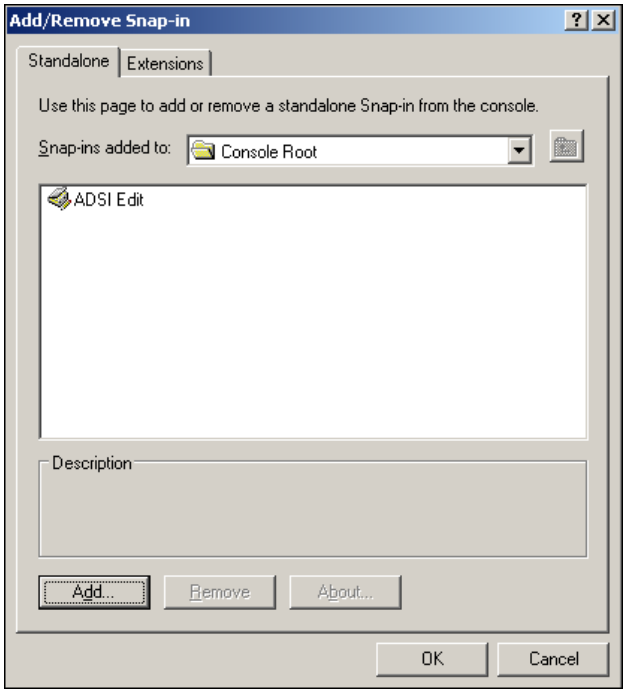

Figure 18:

Step 8. You should be able to see **"console"** screen. Select **"ADSI Edit"**, right click, and click on "**Connect To**".

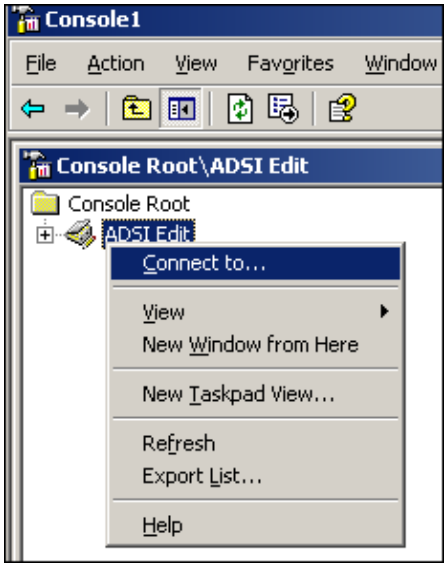

Figure 19:

Step 9. You should be able to see **"Connection Settings"** screen. Select domain from **"Select a well known Naming Context"** or **"Domain"** and click on **"OK"**.

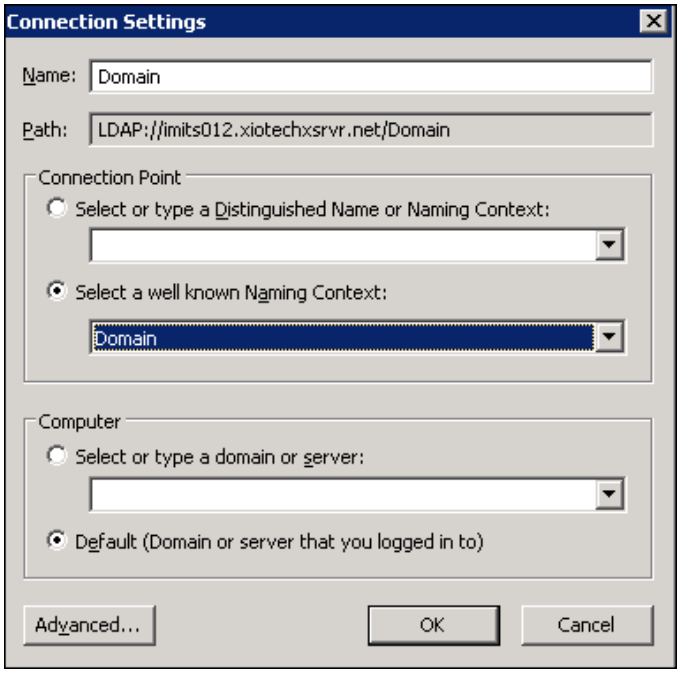

Figure 20:

Step 10. Select the domain user name (InMageUser) under **"Domain"** in the console root screen.

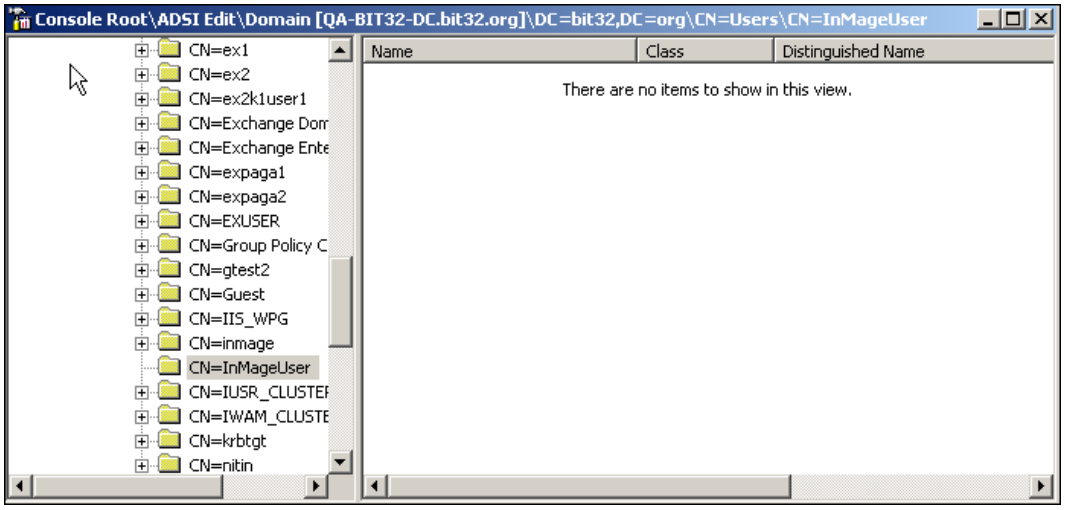

Figure 21:

Step 11. Right click and click on the **"Properties"**. You should be able to see the **"Properties"** screen and click on **"Security Tab"**.

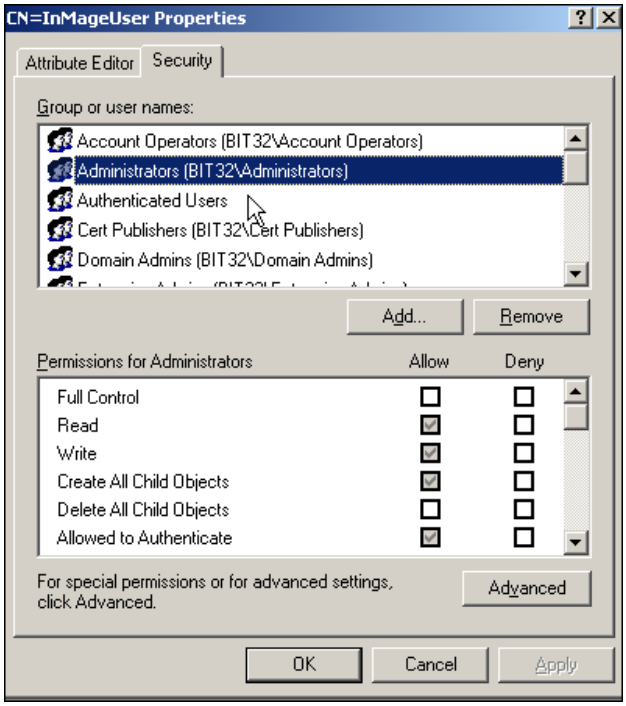

Figure 22:

Step 12. You should see the **"Select Users, Computers, or Groups"** screen. Select the domain user (InMageUser) created in the previous steps and check if this username is available or not by clicking on the **"Check Names"**. Click on "**OK**".

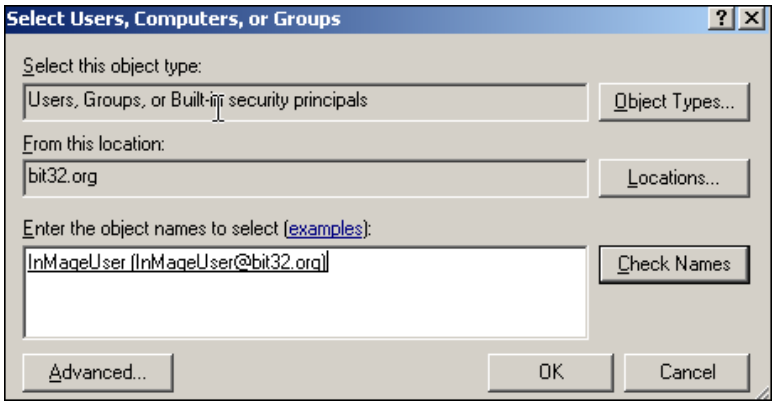

Figure 23:

Step 13. You should see the previous screen. Click on **"Full Control"** check box and click on **"OK"**.

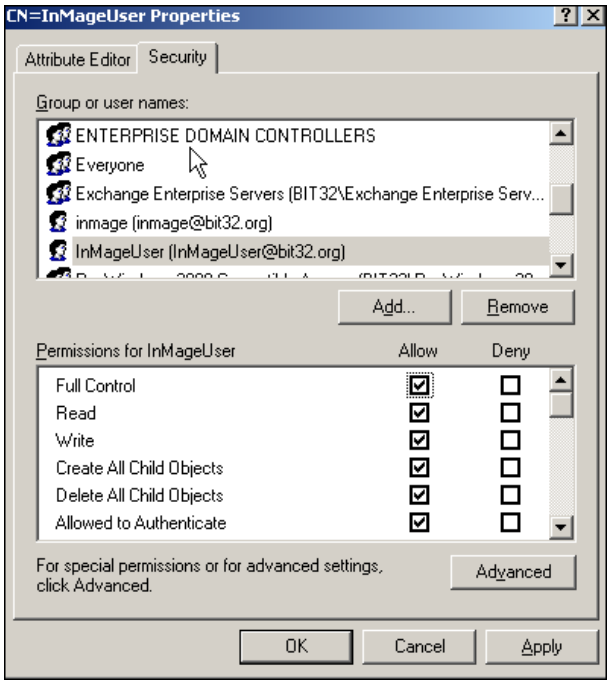

Figure 24:

Step 14. You should see the console screen, select the **"Production Server"**, right click, and click on the **"Properties"**.

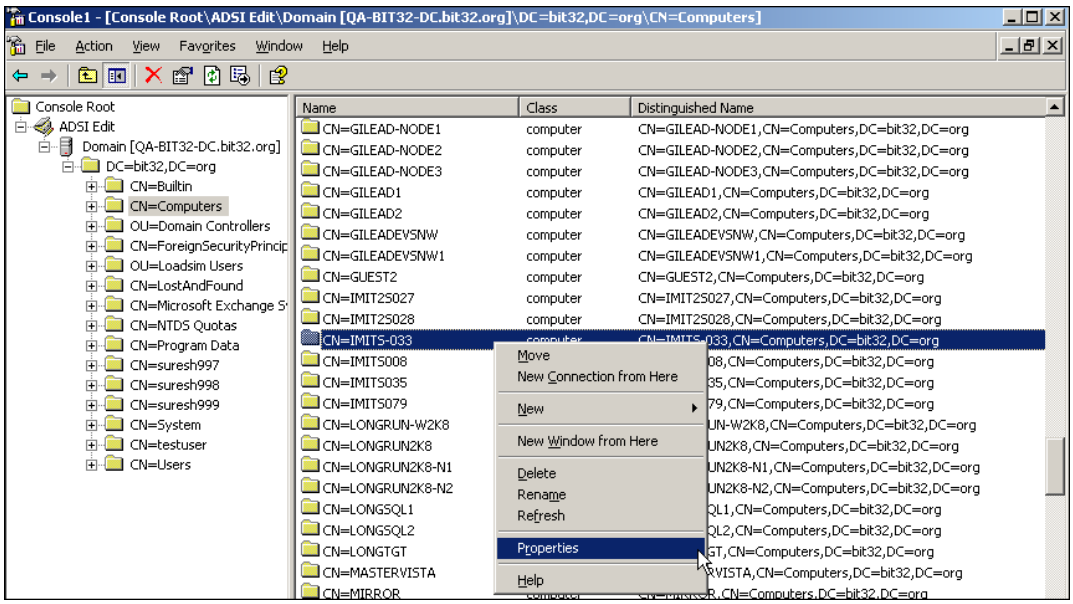

Figure 25:

Step 15. You should see the "**Properties**" screen. Select the "**Domain User**" and click on "**Add**".

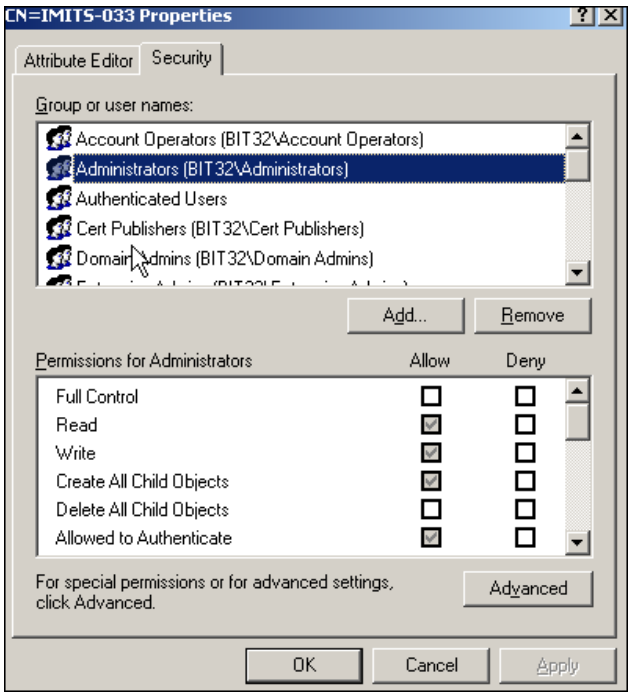

Figure 26:

Step 16. You should see the **"Select Users, Computers, or Groups"**. Select the domain user name (InMageUser) created in the previous steps and check if this username is available or not by clicking on the **"Check Names"**. Click on "**OK**"

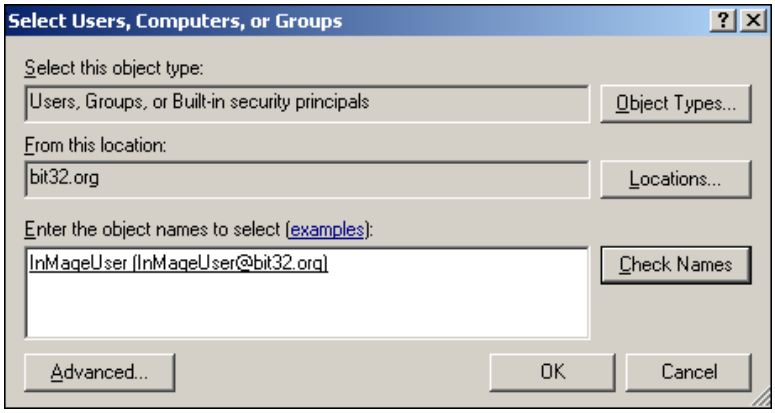

Figure 27:

Step 17. Click on **"Full Control"** check box under permission for test and click on **"OK"**. Repeat the same process for the DR server.

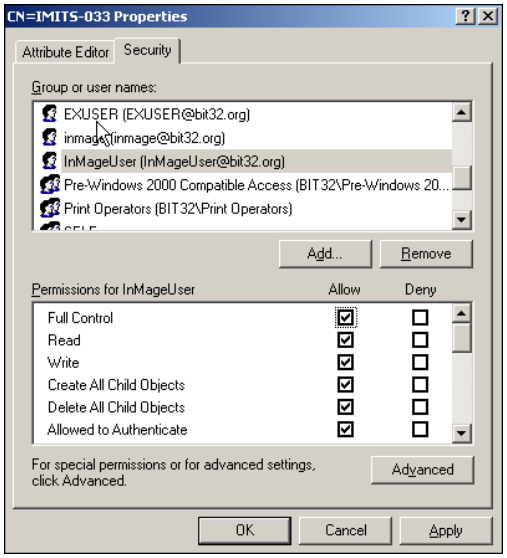

Figure 28:

Notes:

In Cluster case, you need to add domain user to each node. Repeat the steps from 10 to 13.

2.3.5 Adding User to Host Machines

Step 18. Logon to **"Production Server"** with the domain administrator. Open Computer management console, click "**Groups**" under **"Local Users and Groups"**, and click on "**Administrators**".

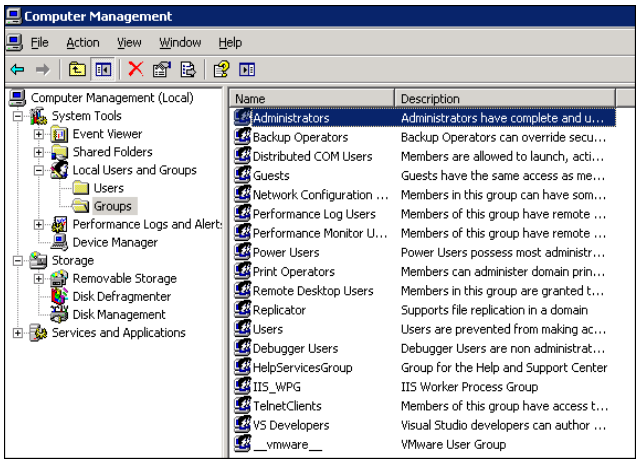

Figure 29:

Step 19. You should be able to see administrator's properties screen and click on **"Add"**.

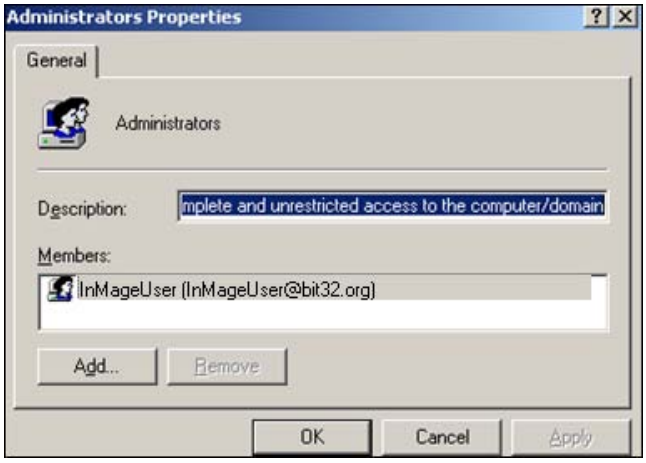

Figure 30:

Step 20. You should be able to see **"Select Users, Computers, or Groups"**, Select the domain user name (InMageUser) created in the previous steps and check if this username is available or not by clicking on the **"Check Names"**. Click on "**OK**".

Figure 31:

Step 21. Click "**Start->Control Settings->Administrative Tools**". You should be able to see **"Administrator's Properties"** screen. Now, click on **"Apply"** and then on **"OK"**.

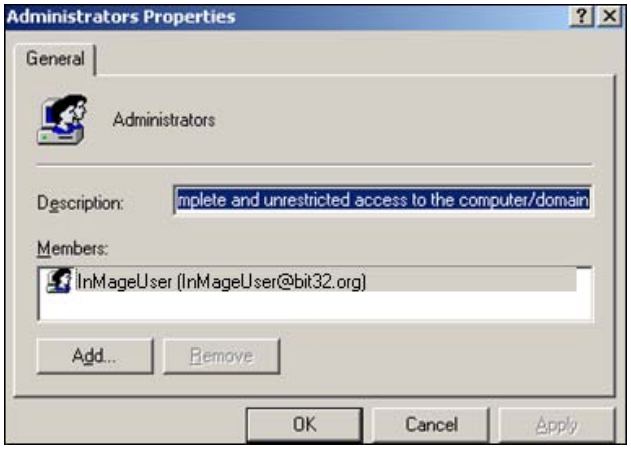

Figure 32:

2.3.6 Adding User to Logon services

Step 22. Click "**Start->Program Files->Administrative Tools->Local Security Policy**".

Figure 33:

Step 23. You should see **"Local Security Settings"** screen, select **"User Rights Assignment"**, and select **"Log on as a Service"**.

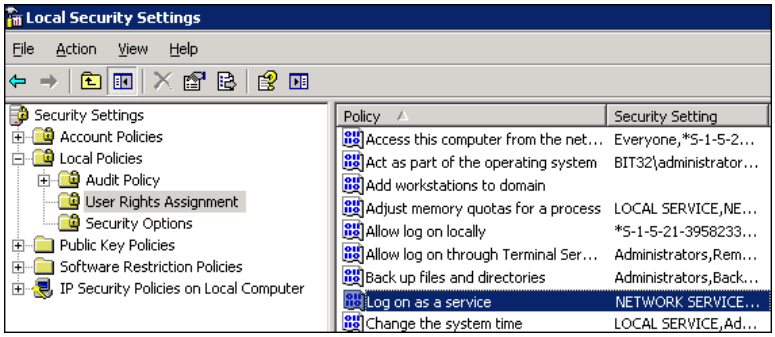

Figure 34:

Step 24. You should see **"Log on as a Service Properties"** screen, click on **"Add User or Group"**, and click on **"OK"**.

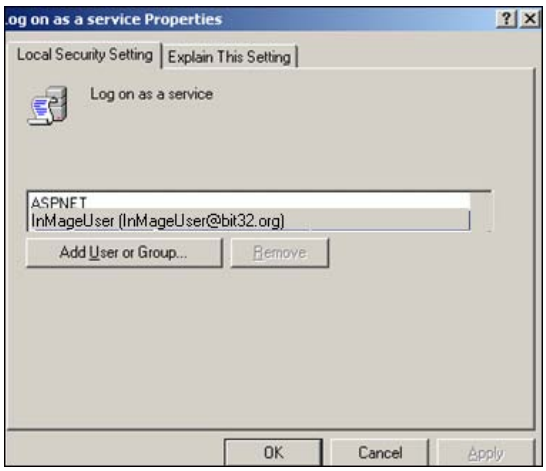

Figure 35:

Step 25. This should open **"Select Users, Computers, or Groups"** screen, select the domain user name created in the previous steps and check if this username is available or not by clicking on the **"Check Names"**. Click on "**OK**".

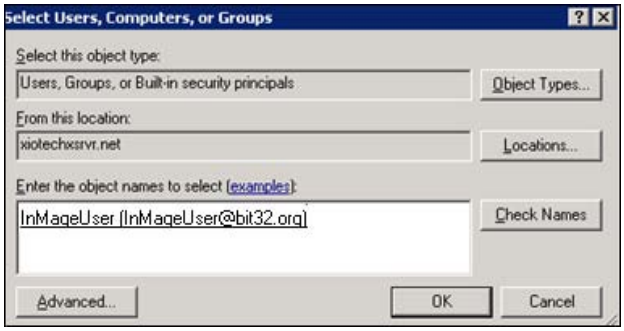

Figure 36:

Step 26. You should see the previous screen. Now, click on **"Apply"**, and then on **"OK"**.

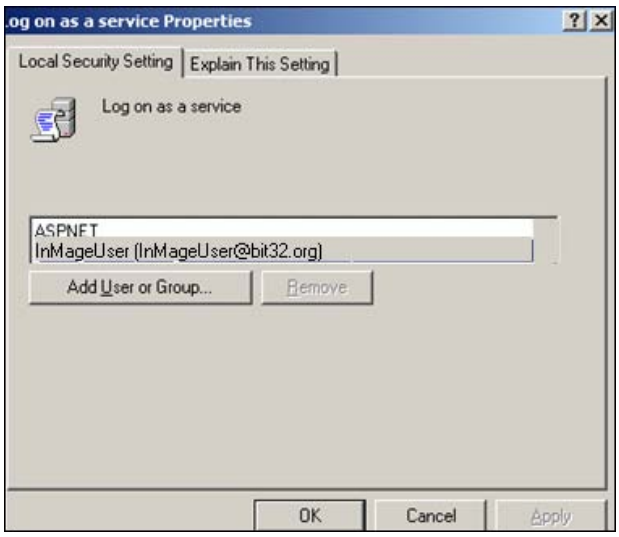

Figure 37:

Step 27. Log on to **"Production Server"** with the domain user created above. Click "**Start->Run->Services.msc"**, select the **"FX agent service"**, right click, and click on the **"Properties"**.

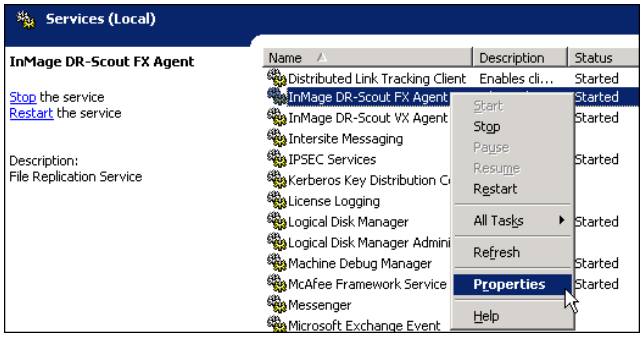

Figure 38:

Step 28. You should be able to see the **"FX agent Properties"** screen. Enter the **"Domain Username"** and password details. Then, click on **"Apply"** and then **"OK".** Restart the FX agent service and repeat the same process for the DR server.

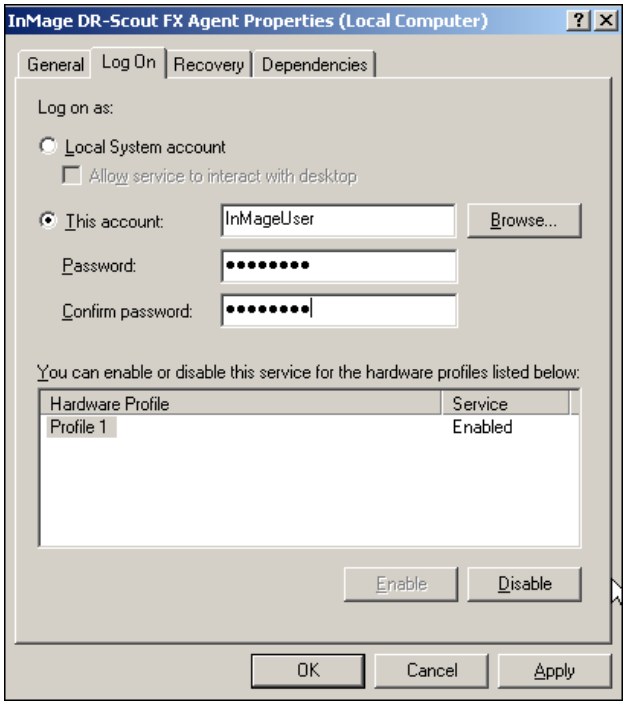

Figure 39:

Notes:

In Cluster case, you need to add domain user to each node. Repeat the steps from 1 to 8.

2.4 Verifying privileges

It is recommended that you check the privileges for failover and failback. This may be performed through the FX job.

Step 29. Access the CX UI and click on "**File Protection**" , Click on "**New Job Group Wizard**" to continue

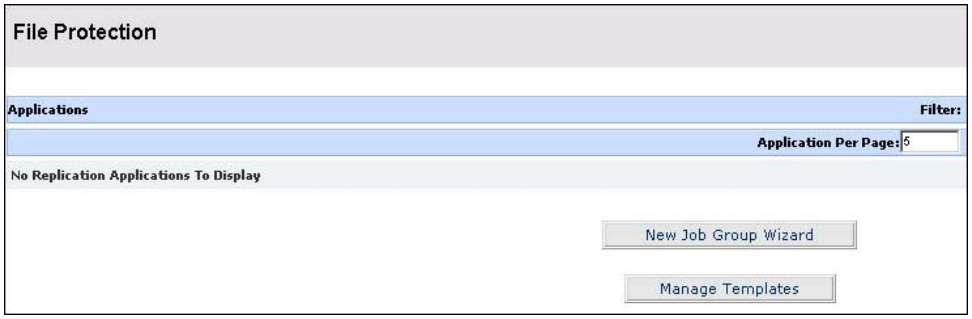

Figure 40

Step 30. Click on "**Add Job**"

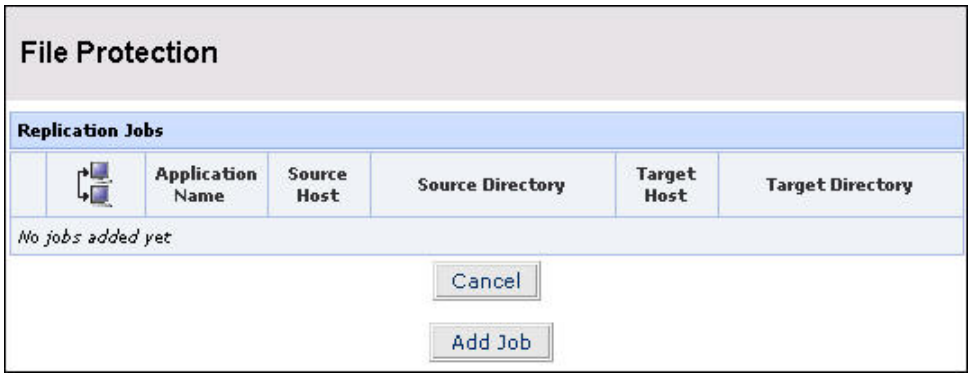

Figure 41

Step 31. Select the "**Source"** as the production file server and the "**Destination"** as the DR file server. Select the FX template as "**VerifyFileServerPermissions"** and click on "**Next"**

Figure 42

Step 32. The "**Job Options"** screen appears, scroll down and click on "**Finish"** without changing any settings

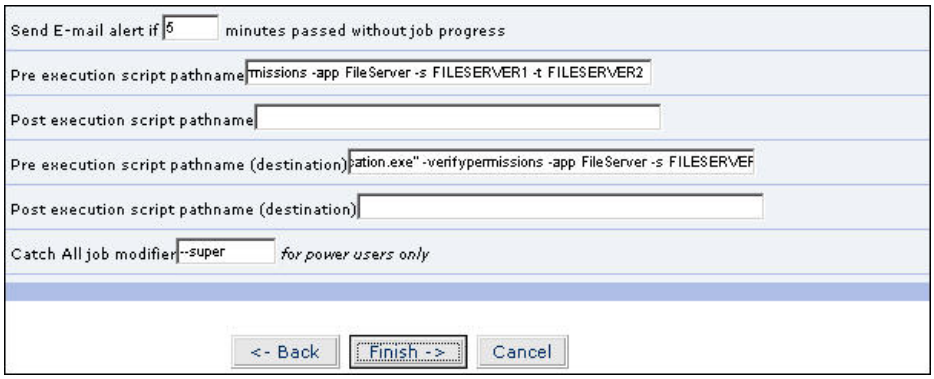

Figure 43

Step 33. The Job will be set to run "**On Demand",** click on "**Finish"** to save the job

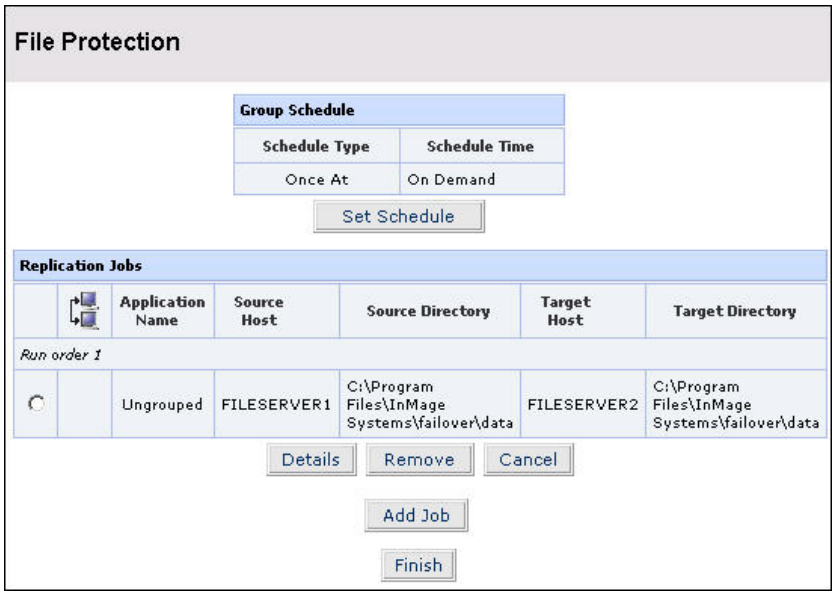

Figure 44

Step 34. Start the FX job through the File Protection screen and monitor the progress through the "**Protection Status"** screen. The result of this task will be found under the FX log.

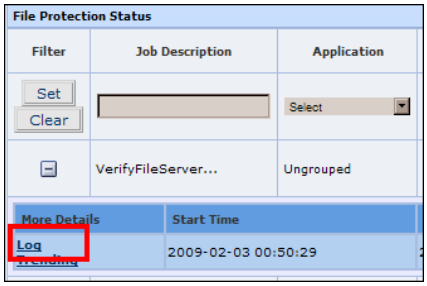

Figure 45

You should see the message "**[SUCCESS] The logon user has sufficient permissions to perform failover/failback of the Application**" if the FX agents have sufficient privileges or "**[ERROR] The service/logon account does NOT have sufficient privileges to update/modify Service Principal Name attribute in the Active Directory of the above failed server accounts"** if the FX agents do not have enough privileges

Part 1: Non-Clustered Environment

This part explains protecting File Server in non-clustered environment where production server and DR server both are standalone.

3 Introduction to Non-clustered Solution

This solution is divided into three major sections: Protect, Discovery, and Recovery. Each of these sections contains a set of steps.

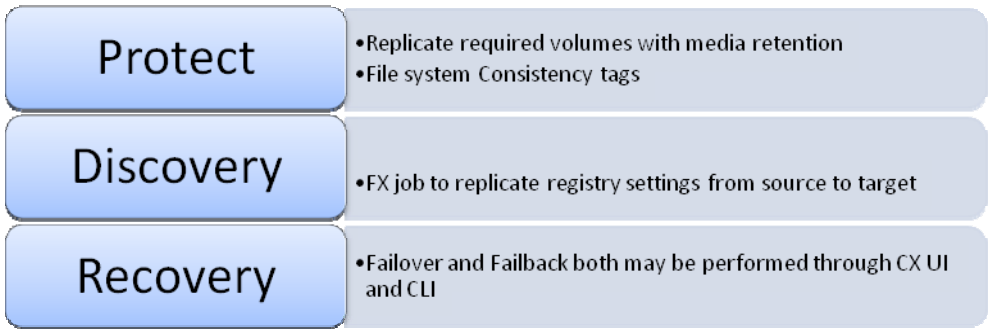

Figure 46:

Protect: Identify the volumes containing the shares or folders that are to be protected. Replicate the volumes to the target host with CDP retention enabled. Enabling CDP retention gives you a "roll back in time" capability. Only Shared folders residing on replicated volumes will be protected and recovered.

Discovery: A plain VX replication replicates all data on the source volume. Folders which are shared on the source volume will not be shared on the target volume by mere replication. Since all the "shared" information will be stored within the system registry. To overcome this, a discovery job is set to restore shared folders back to their respective shared state on the target volume. This information will be used during failover or failback.

Recovery: This section is divided into two parts, failover and failback.

Failover: This section explains planned and unplanned failovers both through CX UI and command line interface.

Failback: A failback is similar to that of a planned failover. Failback is performed in a set of three steps.

Caution:

After setting the replication pair, again run the discovery job as discovery job gather the file share information specific to the protected volume.

4 Protect

Identify and replicate the volumes on the Production File Server (source host) to the DR File Server (Target host).

In the figure below, the "**Production File Server**" has a volume E: containing four shared folders. The objective of this solution is to maintain backup of the production volume along with its shareable properties.

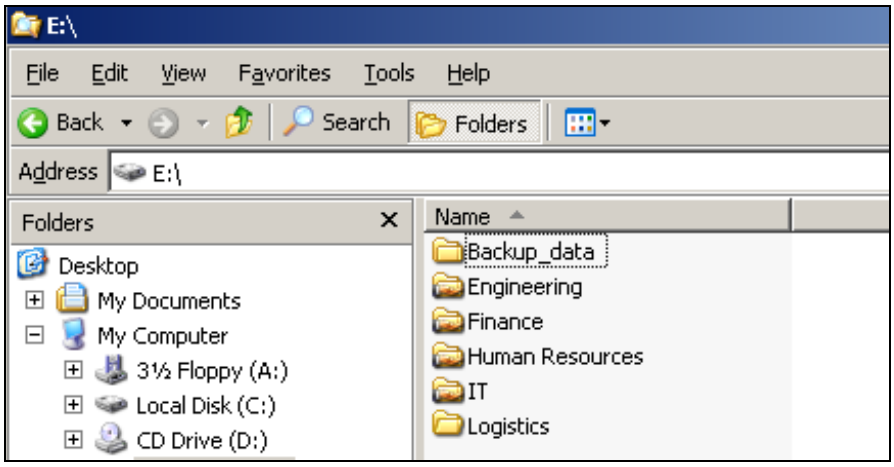

Figure 47: Source host before failover

4.1 Discovery

You can discover the File Share folder by setting File Server Discovery job.

Step 35. Navigate to "**File Protection**" on the CX user interface. Then click on "**New Job Group -> Add Job**". Enter the name of the "**Application"** and the "**Job description"**.

Step 36. Select the production file server for source and DR file server for destination. Then select the FX template as "**File Server Discovery**" and click on "**Next**".

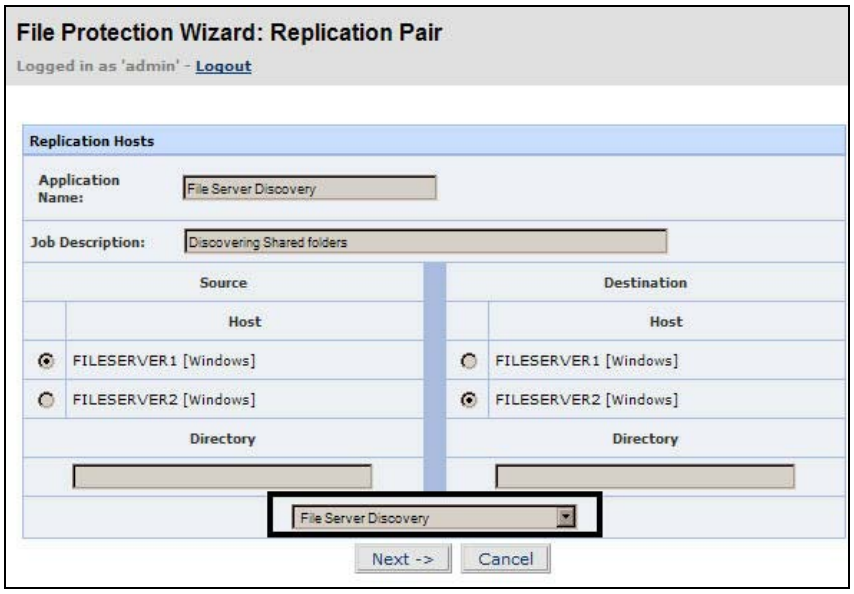

Figure 48: Setting FX replication

Caution:

It is strongly recommended that FX and VX agents is installed in the same folder (FX agent will be installed under the folder "**FileRep**" under the VX installation folder)
Discovery is to be executed at least once if an unplanned failover is to be performed at a later stage.

Notes:

Any changes in file share will require the Discovery job to run again to update the target host accordingly. By default the Discovery job will run once a day

Step 37. Scroll down to "**Miscellaneous Options**" to observe the source pre script and target post script are filled up automatically. Do not change any settings then click on "**Finish**"

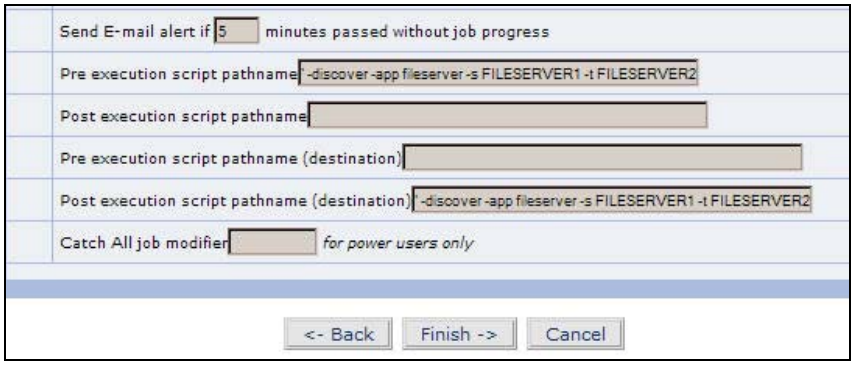

Figure 49:

Step 38. Schedule the job To "**Run on Demand**". And click on "**Finish**" to save the job.

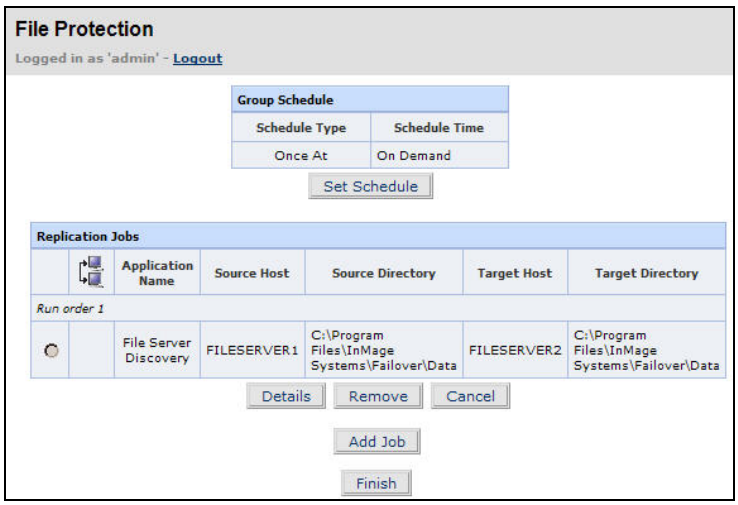

Figure 50: FX job about to be saved.

Step 39. You may start this job through "**File Protection"** on the CX UI and monitor its status on the "**Protection Status**". The status of the job shows as "completed" once the job is successful.

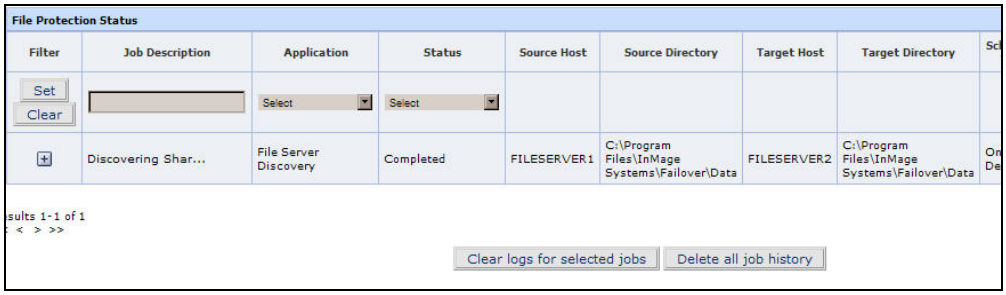

Figure 51:

4.2 VX Replication

Step 40. Open the CX user interface, click on "**Volume Protection**", select the required volume and then click on "**Start Replication**"

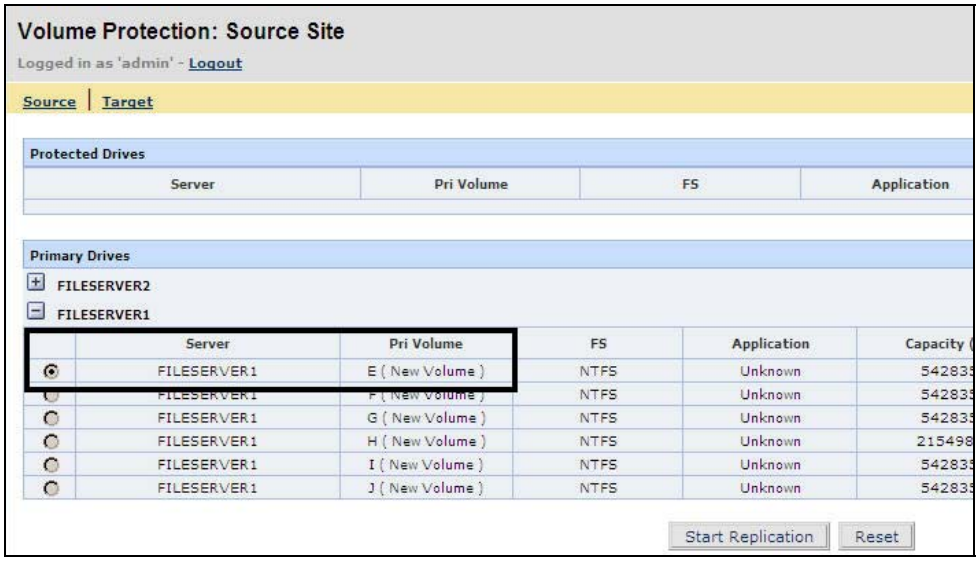

Figure 52: Selecting source volume for replicating

Step 41. This will open up the target volume page. Select the exact same drive letter on the target host and scroll down to set "**Replication Options**"

Figure 53: Selecting corresponding target volume

Step 42. Select a desired "**Process Server**" and scroll down.

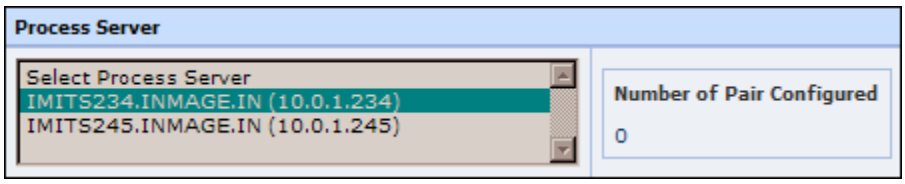

Figure 54

Step 43. Check the "**CDP retention option**". The rest of the options are optional. Then click on "**Submit**"

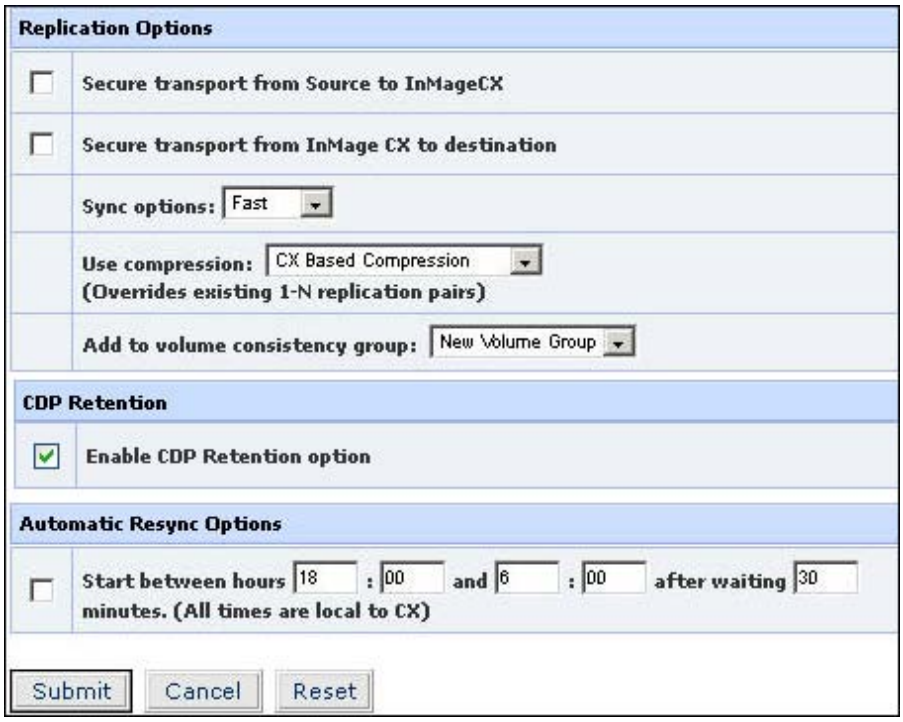

Figure 55: Setting Replication Options

Caution:

You will need to enable CDP retention for all VX replication pairs

Step 44. The final screen opens where you could choose the type of retention policy for this replication pair. Enter the required inputs and then click on "**Submit**". This starts the replication pair.

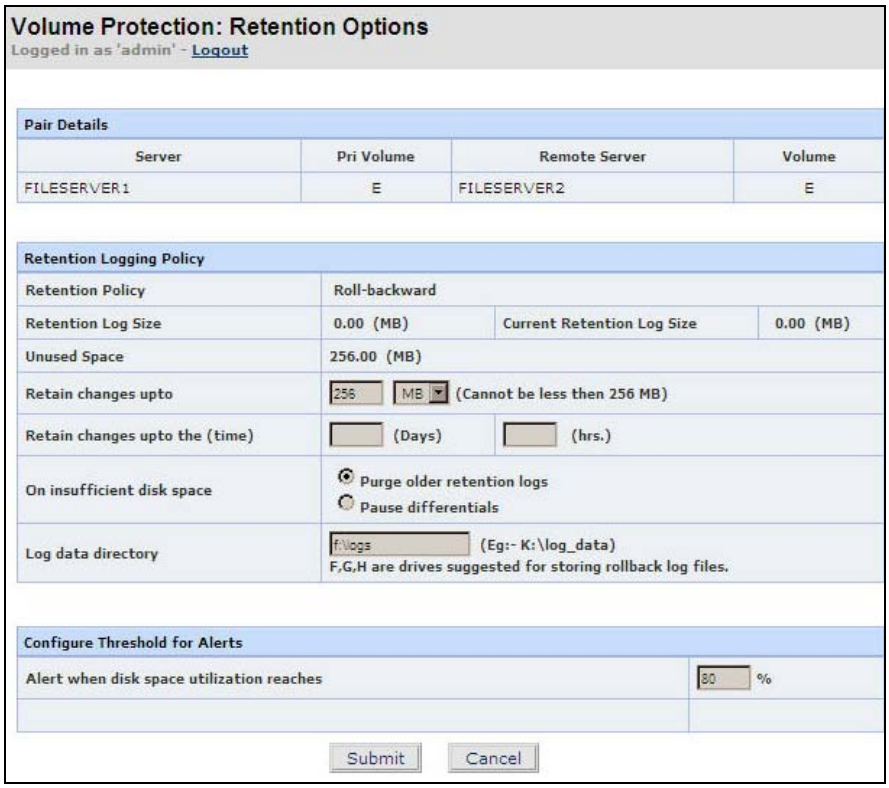

Figure 56: Defining retention policy

Step 45. This starts the replication pair, repeat the same process for the other volume(s) that are to be replicated.

Step 46. Click on the "**Protection Status**", this will show the status of the replication pairs. The status changes from "**Resync Step1"** to "**Resync Step2"** and then finally reaches "**Differential Sync"**.

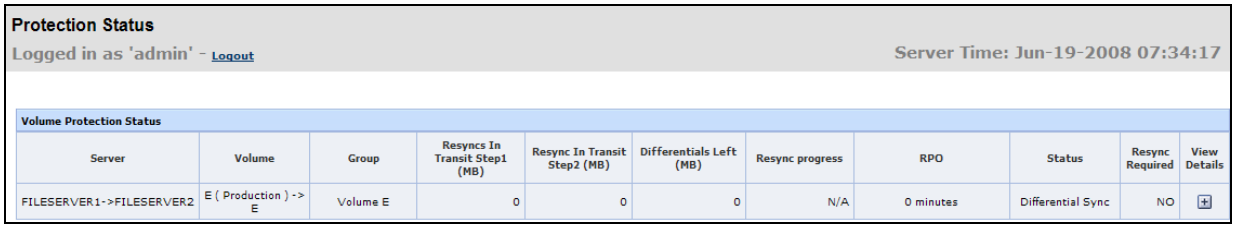

Figure 57: Monitoring replication pair(s) status

4.3 Consistency

Once the Discovery job is complete, proceed to setup a consistency job. This FX job will issue consistency tags on the source volume(s) at regular intervals. A rollback requires at least one consistency tag on the target volume.

Step 47. Click on "**File Protection -> New job Group Wizard -> Add Job".** Enter the "**Application Name", "Job Description"** then select the production server as "**source",** DR server as "**Destination**" and select the FX template as "**File Server Consistency"** then click on "**Next"**

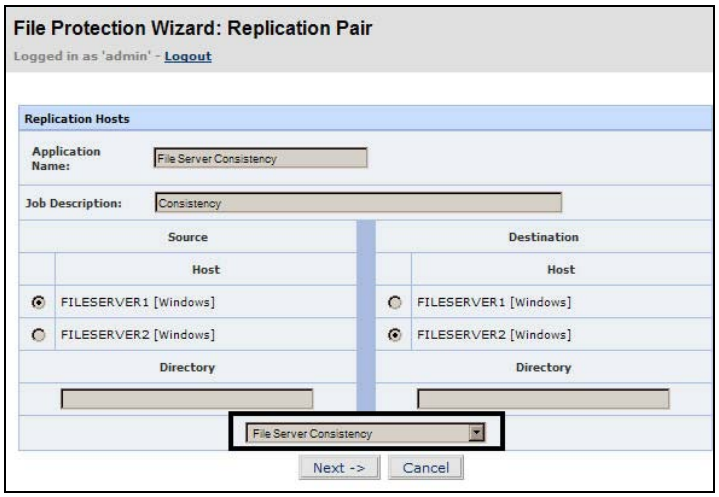

Figure 58

Step 48. The FX job Options page opens up, all the required fields are filled up automatically. Scroll down to observe the source pre script taken automatically. Do not change any settings, click on "**Finish"**

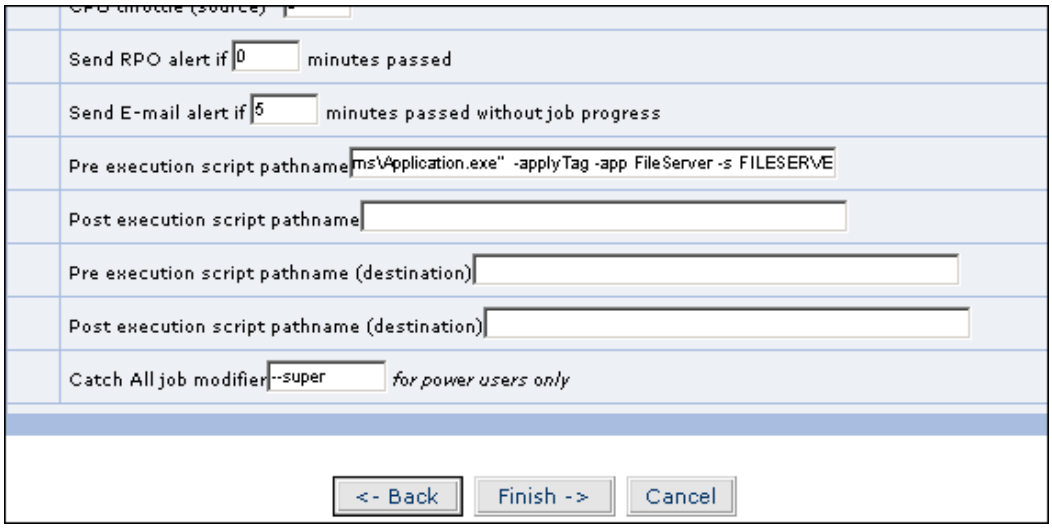

Figure 59:

Step 49. Click on "**Set Schedule"** to change the job execution frequency and then click on "**Finish"**

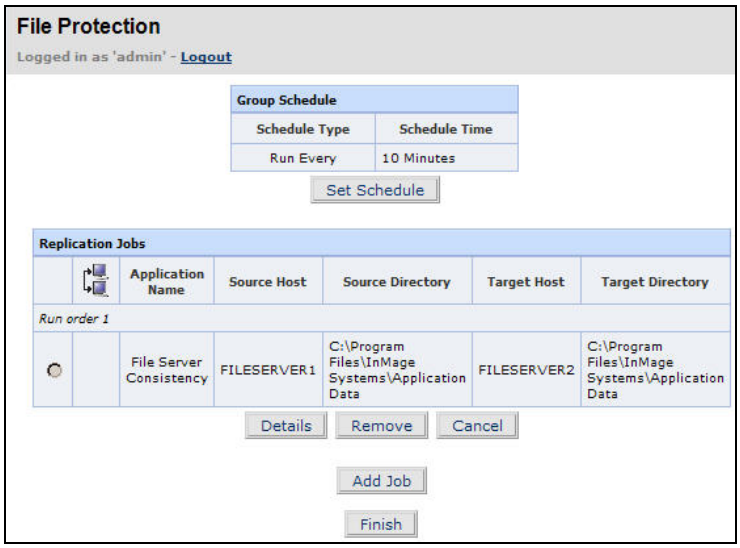

Figure 60:

Step 50. The job can be started manually if required through "**File Protection"**.

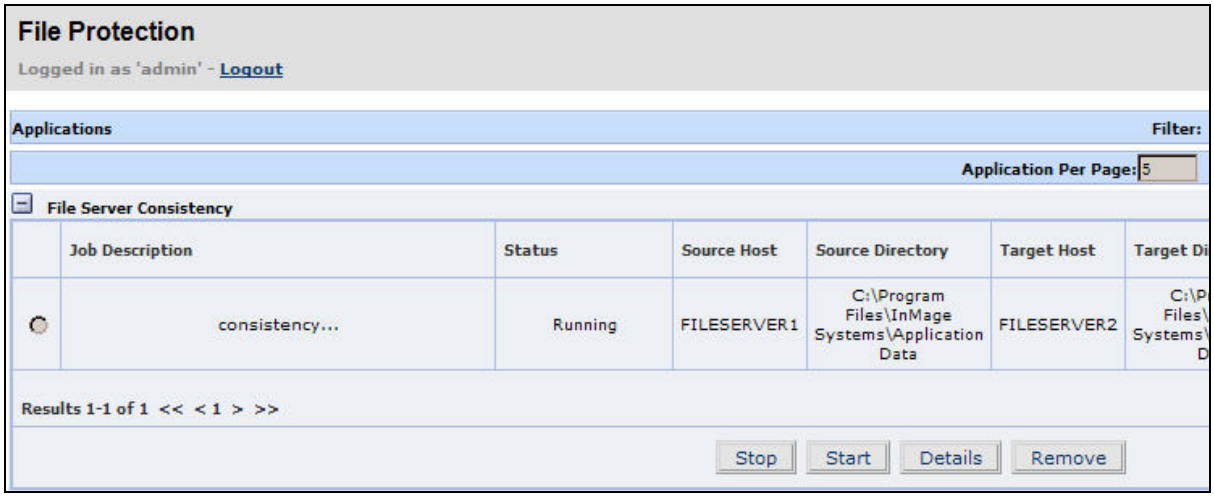

Figure 61:

5 Recovery

5.1 Failover

A failover is performed when there is an outage on the production site. If the outage is expected, such as a mock drill or to test the backup environment, then a planned failover is performed. A planned failover is performed either through CX UI or through CLI.

If the outages are unexpected, then an unplanned failover is performed. If the CX server is available then an unplanned failover is performed through the CX UI. If the CX server is down along with the production server then an unplanned failover is performed through the CLI.

	Unplanned failover	Planned failover
When to use	Real-time outages or unexpected outages	Mock drills, To test the setup. Any expected outages
Recovered to	To latest consistent tag common for all replication pairs	Issues a consistency tag on the protected volumes. Target is recovered to the same consistent tag.
Performed through CX UI	Yes, unless the CX is down.	Yes
Performed through CLI	Yes	Yes

5.2 Prerequisites for failover or failback

- Check the FX agent service privileges on the production and DR file servers.
- When FX is up with local system privileges, ensure that you store domain information through winop.exe on both the production and DR file servers.
- When the FX agent is up and running with local system privileges, you will need to edit the FX job's pre script and post script for failover or failback with the "**–useuseraccount"** switch.
- When the FX agent is up and running with domain administrator privileges, there is no need to edit the FX failover or failback job settings
- Ensure that target volume drive letter or mountpoint is same as that of source drive letter or mountpoint when setting replication pair.
- Disable "**Register this connection's addresses in DNS**" check box located on DNS tab of each network interface's TCP/IP advanced properties. If it is set, after failover if Source machine is restarted then, it will re-register it's IP at DNS server.

Notes:

File server failover does not support web sharing

To restore folder icons after a failover, the respective icons need to be replicated to the path on DR file server that is identical to the path on production file server

Cluster File server failover is supported only for single network name. Failover of file shares having multiple network name dependencies is not supported.

For Windows Vista and Windows Server 2008, if MS Shadow copy provider is not properly installed, VACP will hang as VSS will take time to send the response to VACP. When VACP fails, look at the Application event log for more information

If source has more than 1 NIC, then either uncheck "Register this connection's addresses in DNS" check box for all NICs OR add the "DisableDynamicUpdate" of type DWORD to the following registry key with value set to 1 "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Tcpip\Parameters" This key disables DNS update registration for all adaptors on that computer.

5.3 Planned Failover through CX UI

Step 51. To perform a planned failover through CX UI, setup an FX job with source as the production file server and destination as the DR file server, Select the FX template as "**FileServer Planned Failover**", then click on "**Next"** to proceed.

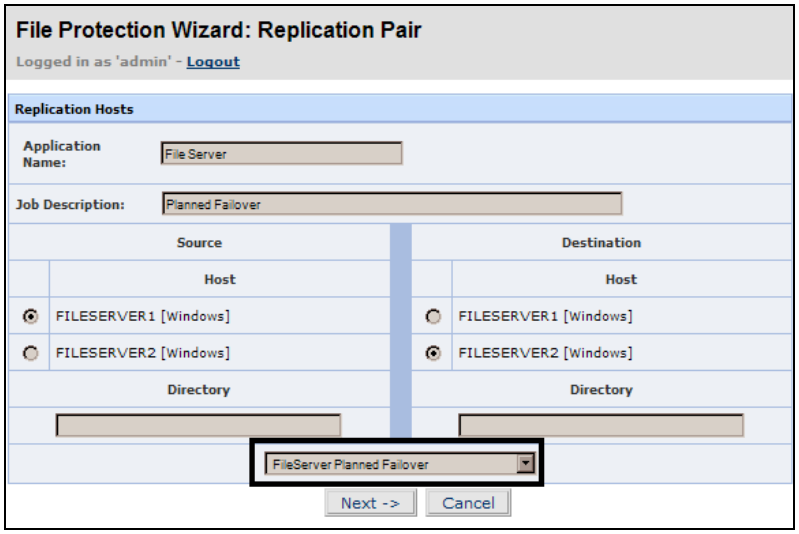

Figure 62:

Step 52. The FX job options screen opens up with all the required fields filled up, scroll down to observe that the source prescript and target post script are already filled up. Do not change any settings, click on "**Finish"**

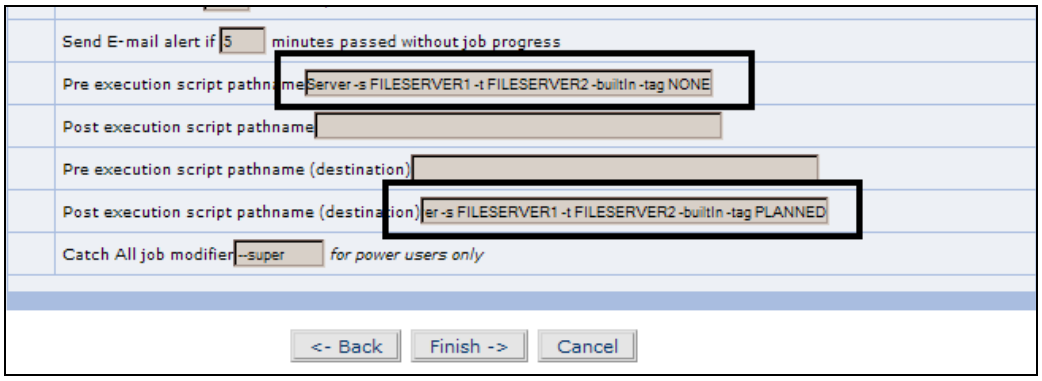

Figure 63:

Caution:

When FX service is running with local System account, ensure to edit the source pre script and target post script with the additional "**–useuseraccount"** switch.

Step 53. The next screen appears, the job is set to execute "**On Demand"** by default. Click on "**Finish"** to save the job.

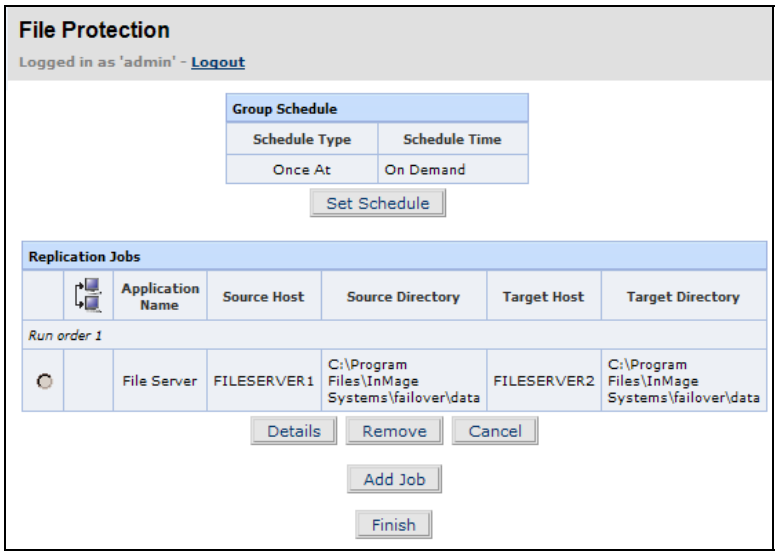

Figure 64:

Step 54. To perform a planned failover, click on "**File Protection"** and start the corresponding job

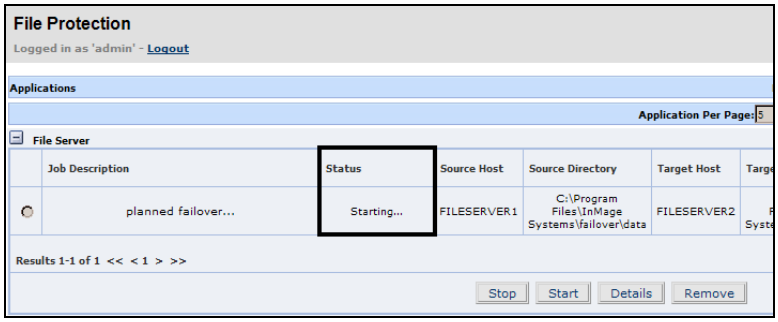

Figure 65:

Notes:

After failover
VX Replication pairs are no longer active
Shares will be active on the target as well.
Discovery and Consistency jobs will be set to "On demand"

5.4 Planned failover through CLI

Step 55.A planned failover can also be performed through the CLI. This requires the CX server and the production server to be up and running. Access the production machine's command interface as domain administrator to issue the following command under the VX installation folder

`Application –failover –planned –app fileserver –s <`*production file server name***`> -t <`** ***DR file server name*****`> -builtin –tag NONE`**

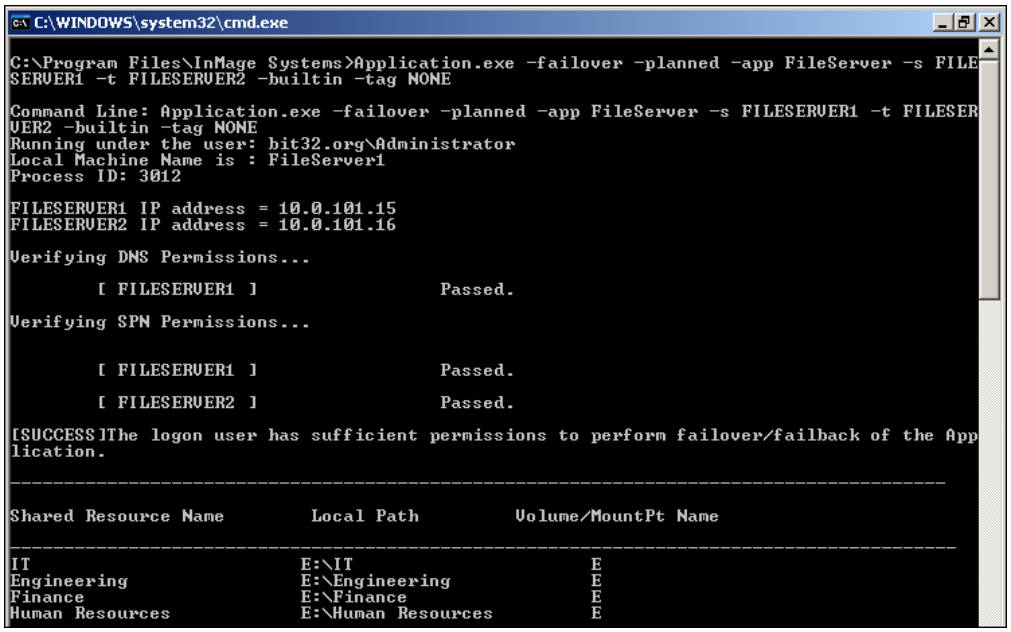

Figure 66:

Step 56. At the end of the output a command is displayed within "important information" as shown in the picture below. This command is to be executed on the DR File server to complete planned failover.

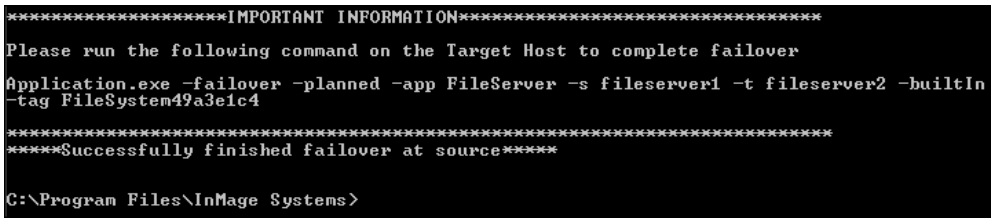

Figure 67:

Step 57. Ensure that you copy the "<VX installation folder>/failover/data" folder from production file server to DR file server's same location. This folder contains a list of five files as shown below

- <Production file server name>_<DR file server name>.txt
- <Production File server name>_FileServer_FILESERVER2.reg
- FailoverServices.conf
- consistency_tag.txt
- <Production File server name>_fileserver_config.dat

Step 58. Access the DR file server's command prompt then navigate to the VX installation folder to execute the above command.

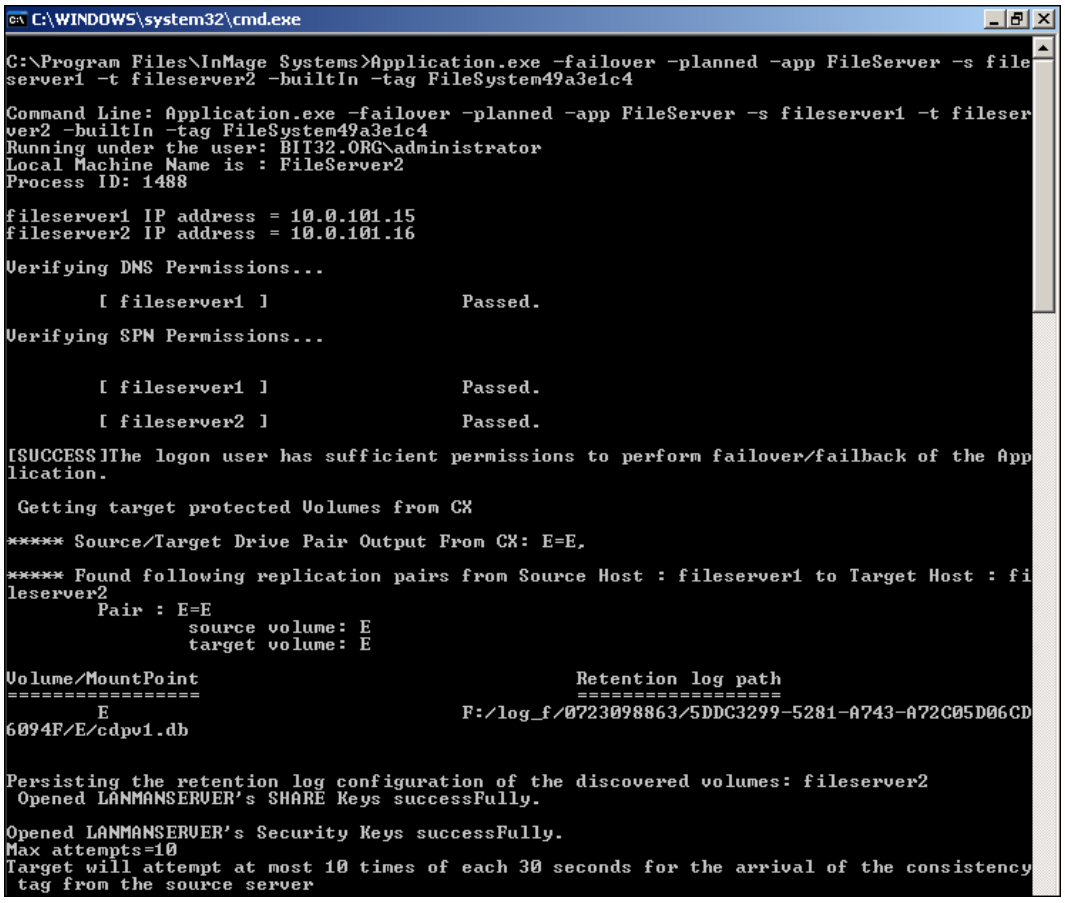

Figure 68:

Notes:

When there are more than one domain controller in the domain you may want to perform AD replication to update the other domain controller with the SPN and DNS entries in the AD/DNS Server

By default AD will not be replicated during File server failover. However if you need AD replication as part of File Server failover edit the command line/pre and post script with the "–doadreplication" switch.
OR
You may run "WinOp.exe" from command line to perform AD replication and DNS Update

5.5 Unplanned failover through UI

Step 59. Unplanned failover through the CX UI is preferred when the production File Server is down but the CX server is up and running.

Step 60. Unplanned failover can be performed through the FX job. Setup the FX job with source and destination as the DR file server then select the FX template as "**File Server Unplanned Failover"**, click on "**Next"** to continue.

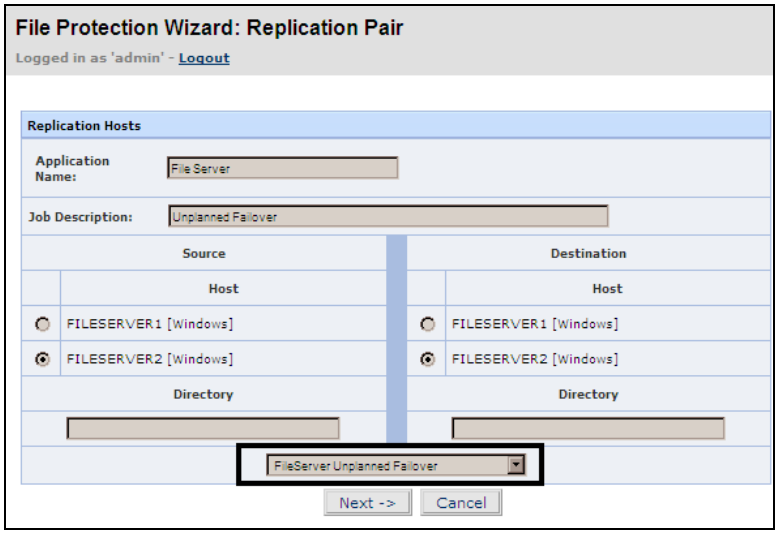

Figure 69:

Step 61. The job options page opens up with all the required fields filled up including the target post script. Change the "**–s"** switch to the production server name

```
"C:\Program Files\InMage Systems1\Application.exe" -failover -unplanned -app
FileServer -s <production server name> -t <DR server name> -builtIn -tag
LATEST
```

Step 62. Click on "**Finish"** to continue.

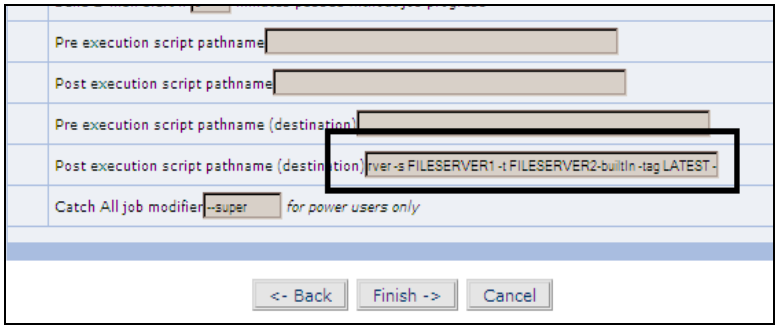

Figure 70:

Caution:

When FX service is running with local System account, ensure to append the additional "**–useuseraccount"** switch to the target post script.

Step 63. The job is set to execute "**On Demand"**, click on "**Finish"** to save the job.

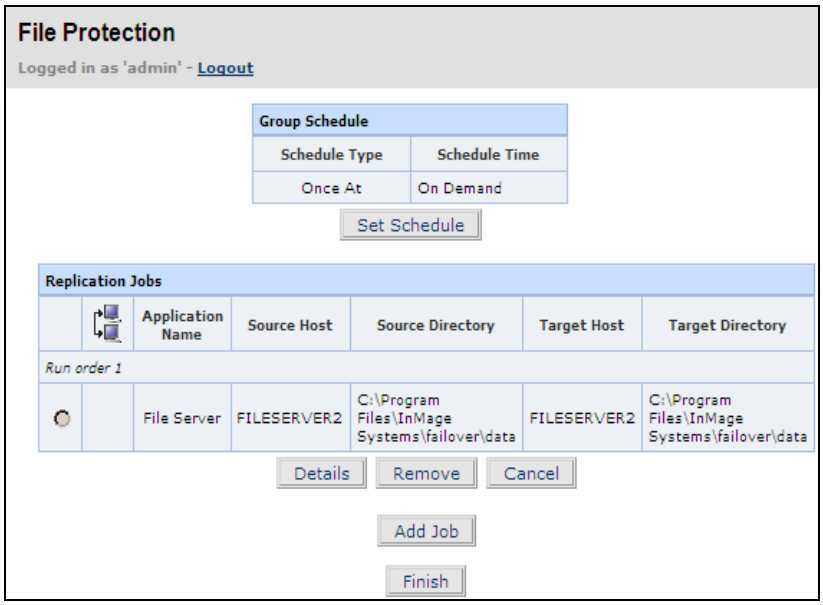

Figure 71:

Step 64. Click on "**File Protection"**, then select the job and click on Start to perform an unplanned failover

5.6 Unplanned failover through CLI

Unplanned failover is performed when both the production server and CX servers are down. To perform an unplanned failover through command prompt, access the DR File server's command prompt then navigate to the VX installation path to issue the following command

Application.exe –failover –unplanned –app fileserver –s <*production file server***> -t <***DR file server***> -builtin -tag latest**

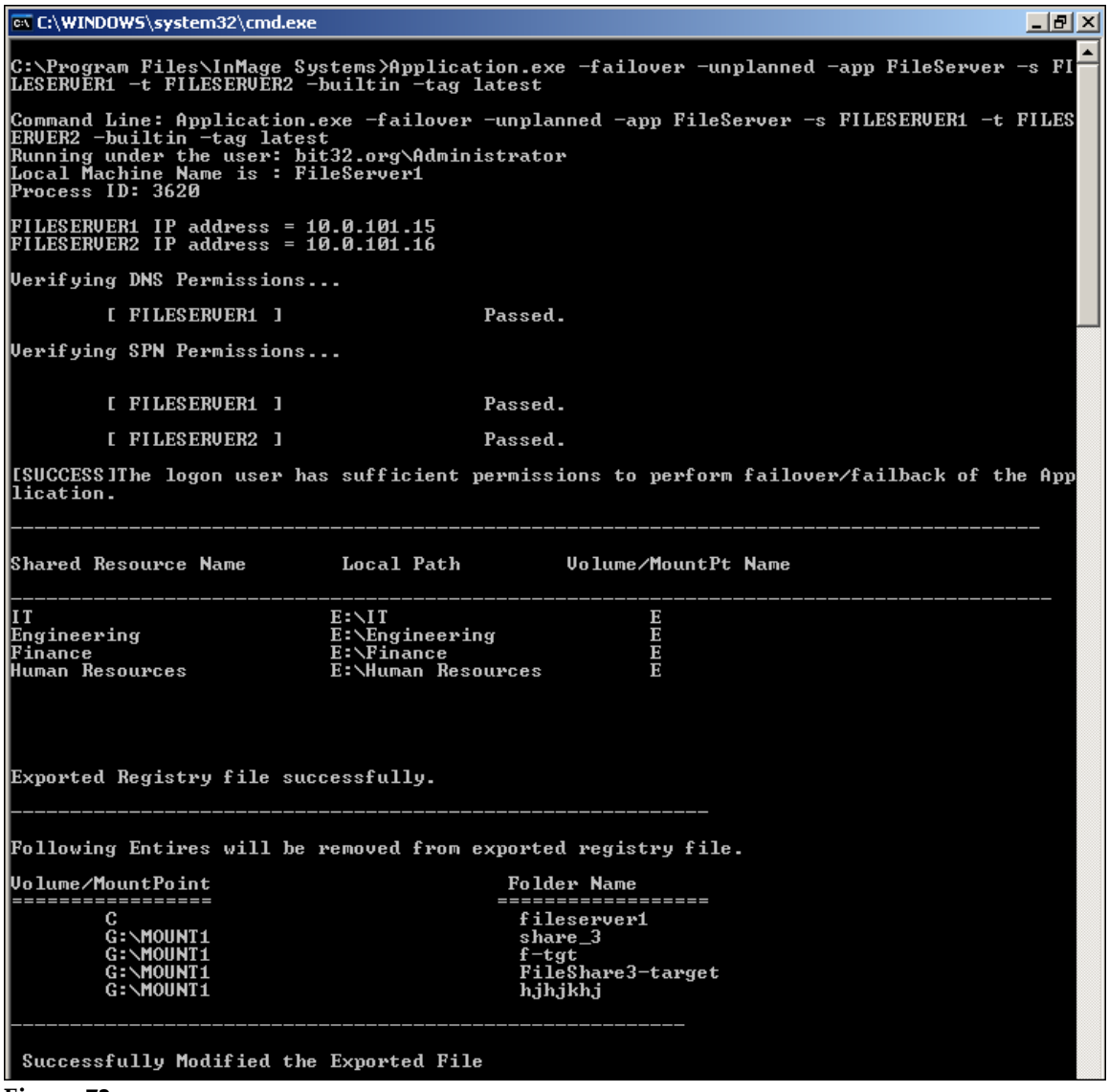

Figure 72:

Caution:

When FX job is running with local System account, ensure to append the additional "**–useuseraccount"** switch to the end of the command.

5.7 Failback

A failback is performed when the production server recovers from the outage. The process is similar to that of a planned failover.

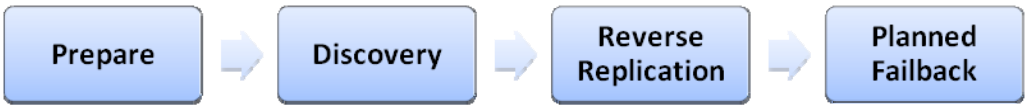

Figure 73:

5.7.1 Prepare

When the FX agent service is configured to run at the domain user it will not start after failover due to explained SPN changes. If the production machine is restarted after failover the user cannot logon to the domain. To overcome this issue run the following command from DR server to add the host SPN entries back to the production server.

`WinOp.exe SPN -addhost` **<***production server name***>**

Logon to production server and run the FX agent service. Now proceed with setting the FX job.

Notes:

This preparation is not applicable when FX agent is already configured with local system privileges.

5.7.2 Discovery

A discovery job is executed to maintain shared folder information specific to the replication pair. A reverse discovery is performed here to replicate all the shared folder information from DR file server to Production file server.

Step 65. Open the CX UI, click on "**File Protection"** to setup the Discovery job.

Step 66. Select the "**Source"** and "**Destination"** as DR File server and Production File server respectively. Select the FX template as "**FileServer Discovery"** then click on "**Next"** to continue.

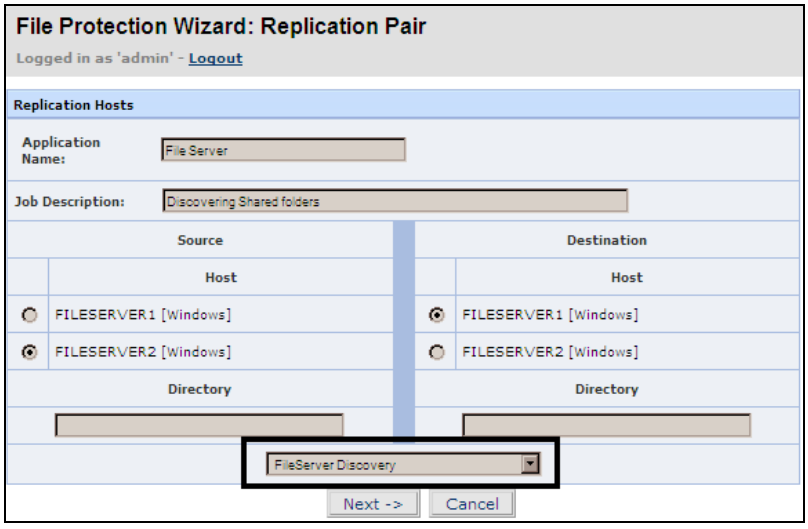

Figure 74:

Step 67. The job options page opens up with all the required fields filled up, scroll down to observe the source pre script and target post script is taken automatically. Do not change any settings, click on "**Finish"**

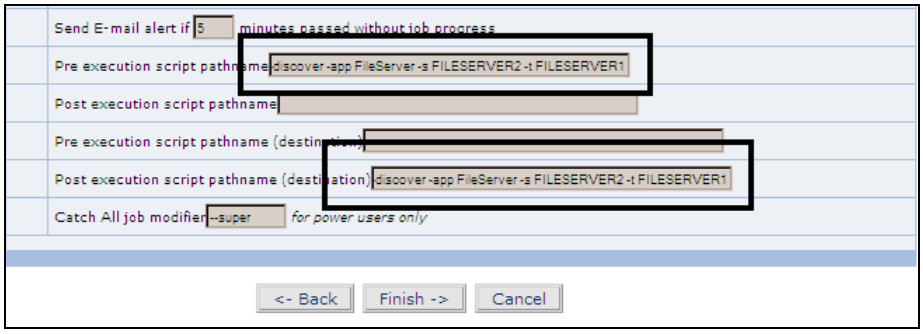

Figure 75:

Step 68. The next screen appears, click on "**Set Schedule**" to change the execution frequency. Click on **Finish"** to save the job

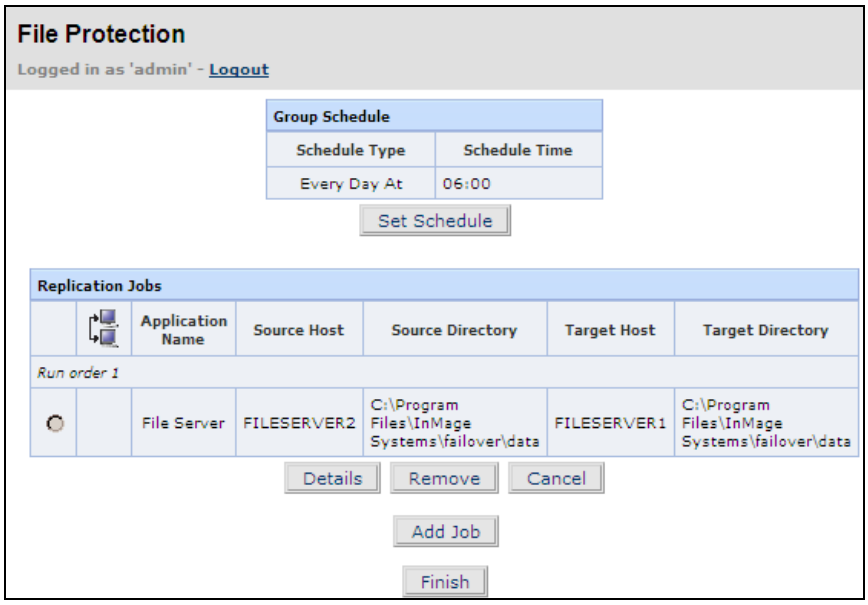

Figure 76:

Step 69. Then start the discovery job, through "**File Protection"**

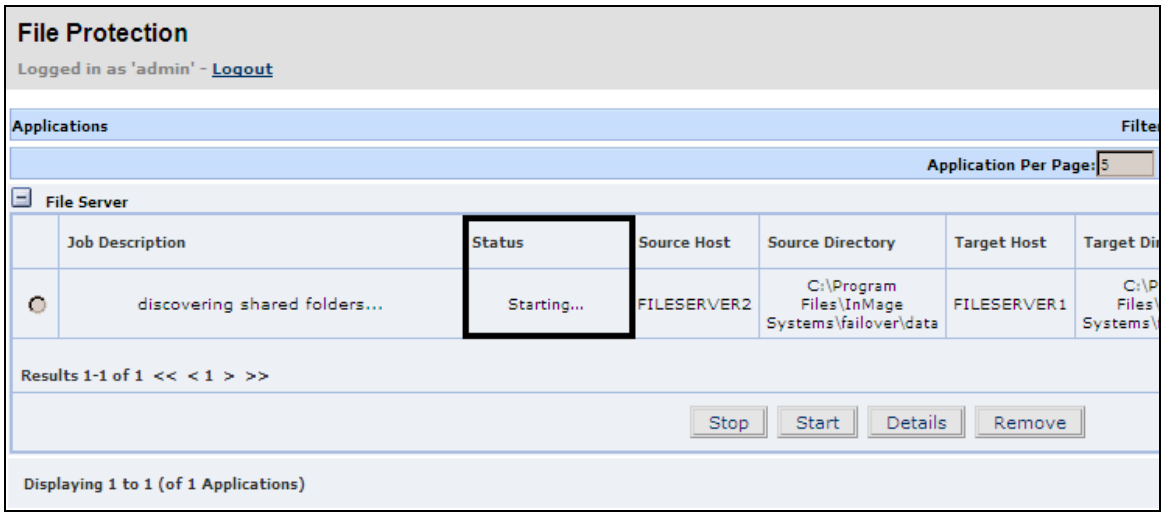

Figure 77

Notes:

Issuing consistency tags after discovery is optional while failback because consistency tag will be issued internally by the planned failover script to minimize data loss

5.7.3 Reverse replication

A reverse replication is performed to update the production file server with all the data changes occurred during the outage.

Step 70. Access the CX UI, click on "**Volume Protection"** then expand the DR file server to select the source volume (the same volume was used as a target earlier) and click on "**Start Replication"**

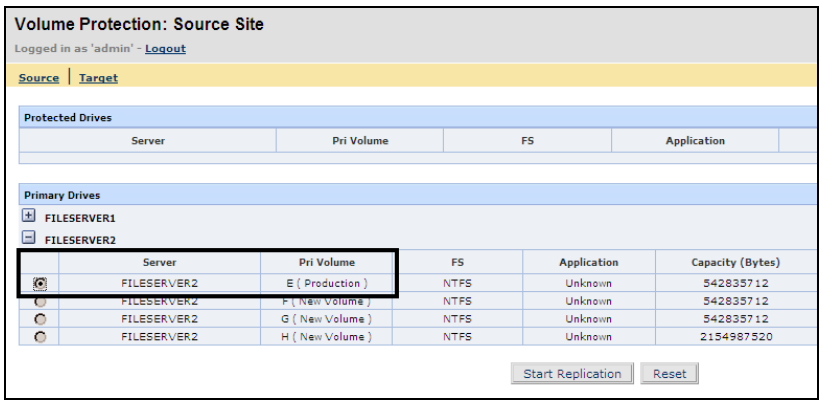

Figure 78:

Step 71. The target screen opens up, expand the production file server to select the target volume (production volume) and scroll down to set the replication options.

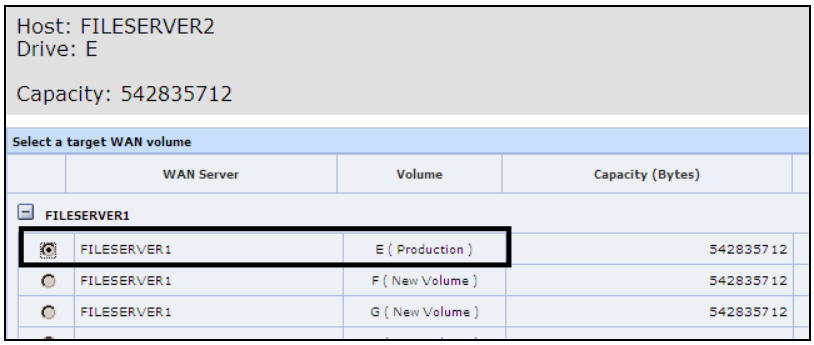

Figure 79:

Step 72. Select the desired "**Process Server**" and scroll down

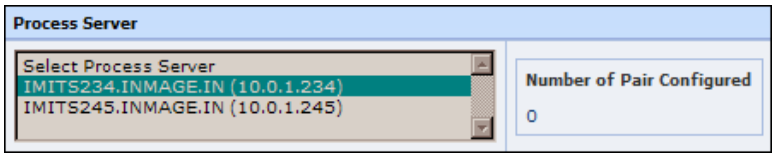

Figure 80

Step 73. Ensure that the "**CDP retention"** is enabled. Click on "**Submit"** to continue**.**

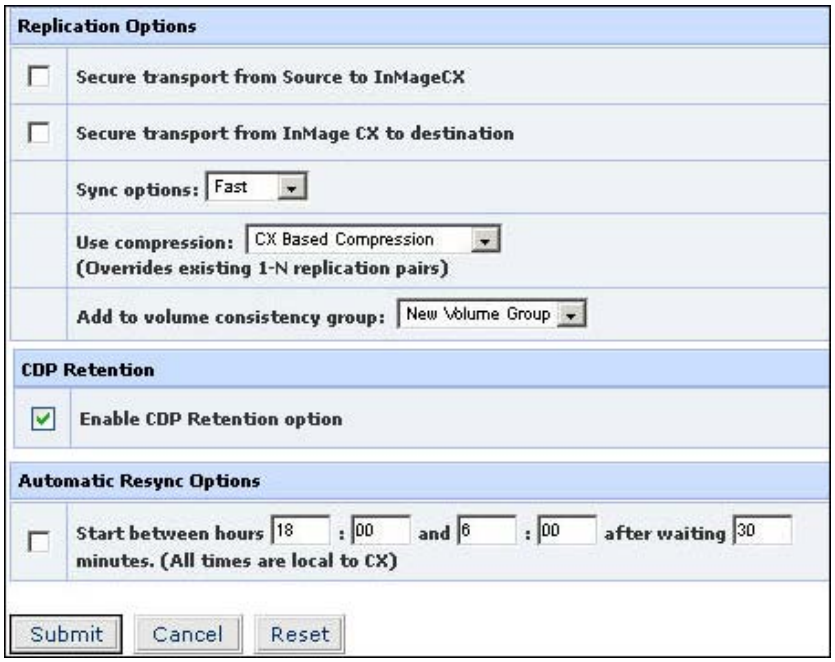

Figure 81:

Step 74. The next screen opens up, define the type of retention policy and click on "**Submit"** to start the replication pair.

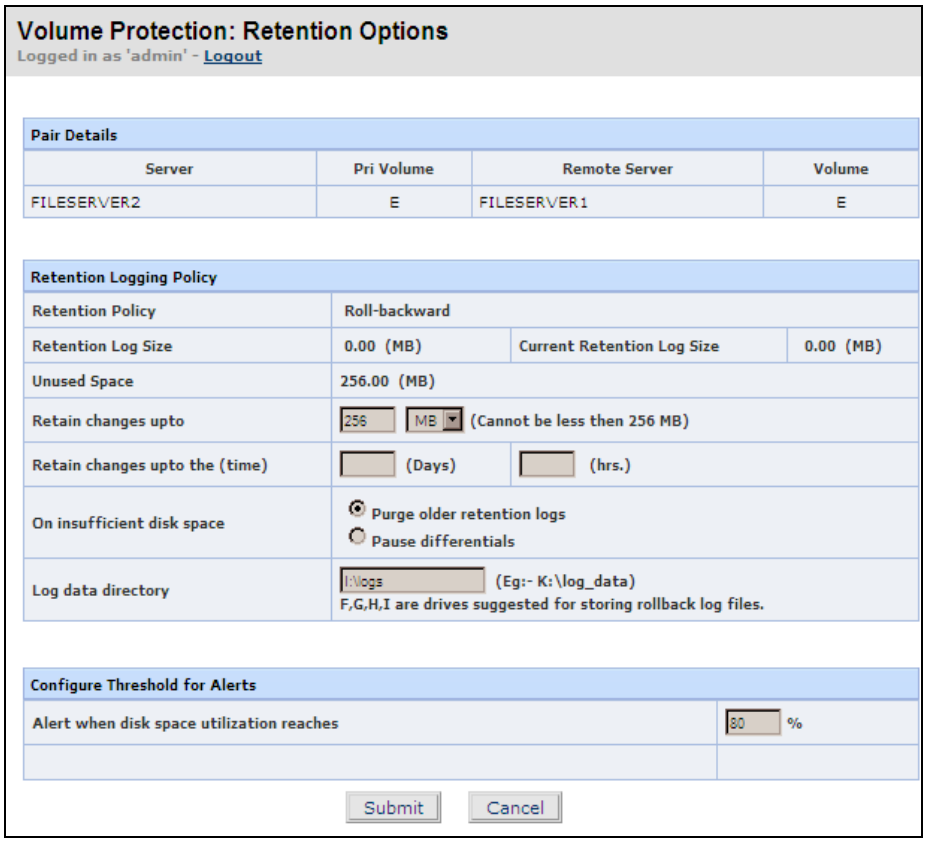

Figure 82:

Step 75. Once the replication pair reaches "**Differential Sync**" proceed to the next step

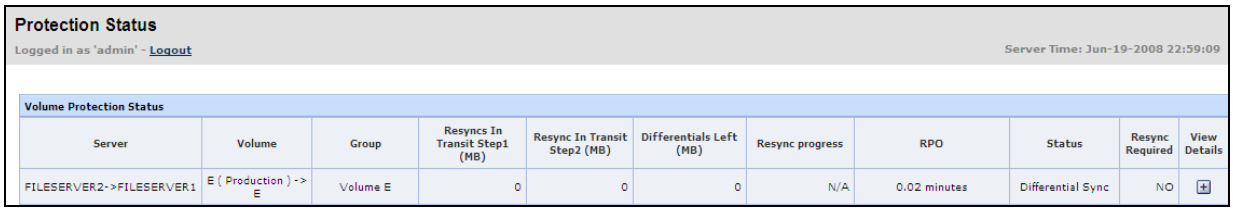

Figure 83:

5.7.4 Failback

Step 76. After the Discovery job is complete, proceed to perform a failback. Open the CX UI and setup the FX job with source and destination as DR file server and Production File server respectively. Select the FX template as "**File Server Planned Failover"** and click on "**Next"** to proceed

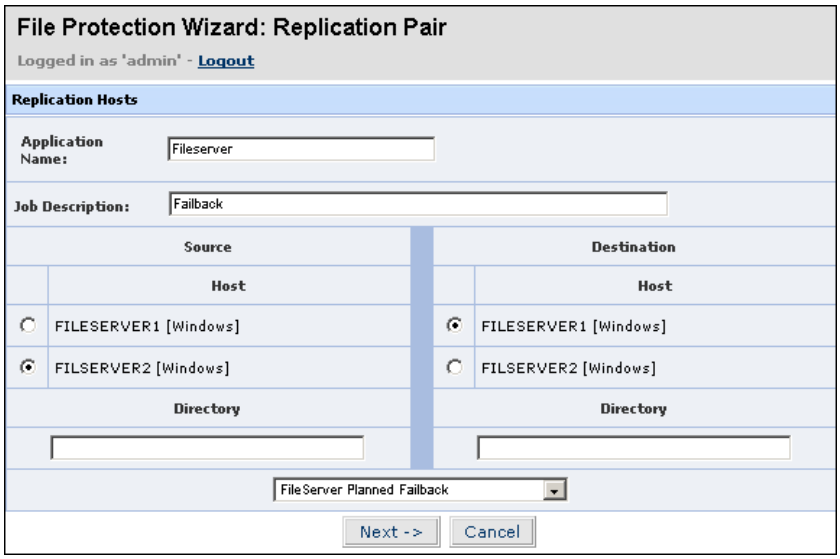

Figure 84:

Step 77. In The **"Job Options"** UI, uncheck the **"update only (do not overwrite files)"** under **"Inclusion/Exclusion Options".**

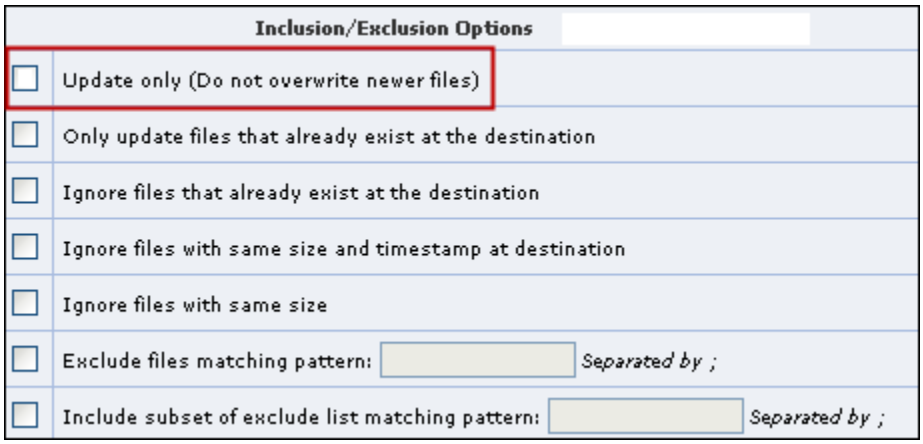

Figure 85

Step 78. Leave other default selections as it is and scroll down to click "**Finish**".

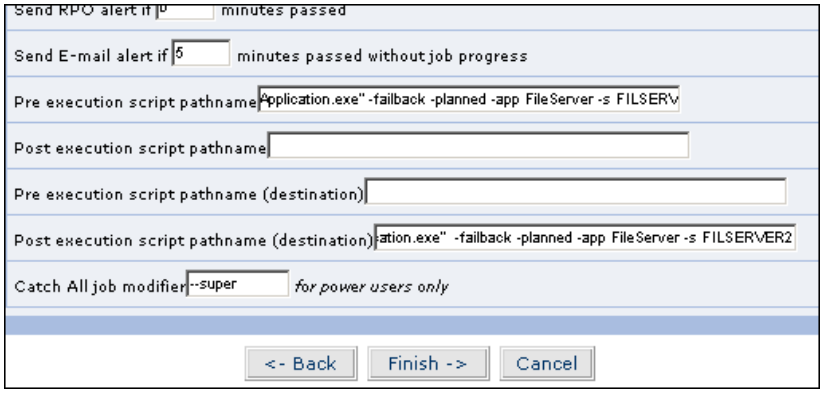

Figure 86:

Caution:

Although the source pre script and target post script have changed for the failback, the older commands involving "**–failover"** and "**–ip"** switches work as well.

When FX job is running with local System account, ensure to append the additional "**–useuseraccount"** switch.

Step 79. The next screen appears, click on "**Finish"** to save the job. By default the job is set to execute "**On Demand".** Start the job to perform a failback (planned failover).

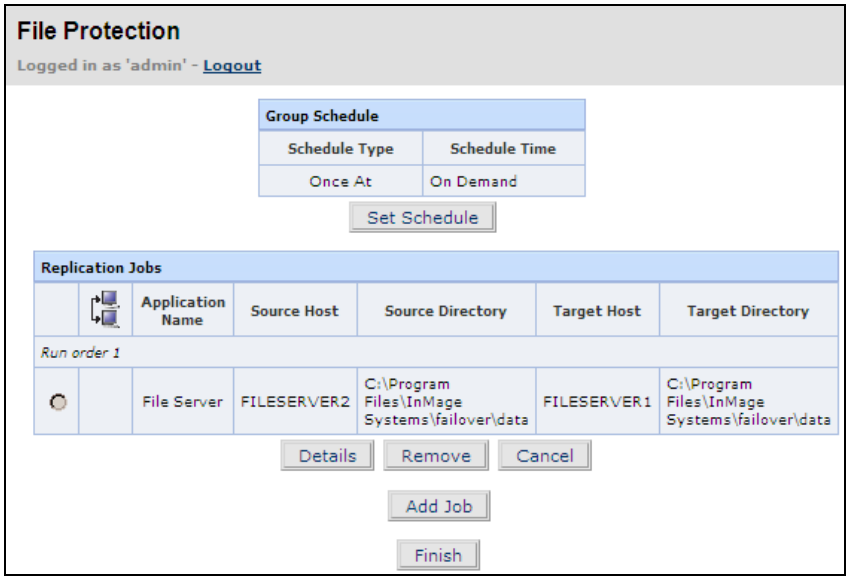

Figure 87:

6 Failover and failback using crash consistency tag

In normal setup, DR scout uses VSS snapshot to issue application or consistency tag but in a setup it is not possible to issue VSS consistency tag. In this case, crash consistency tag can be used and the same can be used for failover and failback. When crash consistency tag is used it always generates USERDEFINED tag. It will not generate any filesystem or application consistency tag.

6.1 Discovery

Use the application discovery template as used in planned failover. No changes are required.

6.2 Consistency

To set crash consistency FX job use the ***Fileserver_consistency_fstag.bat*** file and pass the required argument as given below.

Syntax:

```
Fileserver_consistency_fstag.bat "List of volumes separated by semicolon" -
CrashConsistency
```

For example, following volumes G, H, K:\Mnt1, J:\Mnt2 have shared folders. Use the following command in prescript to set the crashconsistency job or run it through CLI.

```
"C:\Program Files (x86)\InMage Systems\consistency\ Fileserver
_consistency_fstag.bat" "G:;H:;K:\Mnt1;J:\Mnt2" –CrashConsistency
```

Notes:

List of volumes must be in double quotes else only first Drive or mount point is taken for issuing tag.

-Crashconsistency can be written with or without double quotes

Caution:

While protecting large number of databases, application consistency tags may fail. You can use the file system tag to overcome this error.

Additionally you can also write a batch script and automate this through the FX job.

6.3 Planned Failover

6.3.1 Planned failover through CX UI

When you set the planned failover job, in the planned failover template, add the prescript with "**–crashconsistency**" and postscript with-"**-tagtype USERDEFINED**"
For example,

Pre script: "C:\Program Files (x86)\InMage Systems\application.exe" -failover -planned -app Fileserver -s W2K3-SRC -t W2K3-TGT -builtIn -tag NONE **-CrashConsistency**

Post script: "C:\Program Files (x86)\InMage Systems\application.exe" -failover -planned -app Fileserver -s W2K3-SRC -t W2K3-TGT -builtIn -tag PLANNED **-tagtype USERDEFINED**

6.3.2 Planned Failover through CLI

When you run through CLI follow the same procedure as in section 8.2.
The only change is add "**–crashconsistency**" switch to the source command and target command with "**-tagtype USERDEFINED**".

Source Command:
"C:\Program Files (x86)\InMage Systems\application.exe" -failover -planned -app Fileserver -s W2K3-SRC -t W2K3-TGT -builtIn -tag NONE **-CrashConsistency**

Target command:
"C:\Program Files (x86)\InMage Systems\application.exe" -failover -planned -app Fileserver -s W2K3-SRC -t W2K3-TGT -builtIn -tag <User Defined Tag> **-tagtype USERDEFINED**

6.4 Failback

6.4.1 Failback through CX

Use the same failback template as in section 8.2.4. The only change is add "**–crashconsistency**" switch to the source command and target command with "**-tagtype USERDEFINED**".

For example,
Pre script: "C:\Program Files (x86)\InMage Systems\application.exe" -failback -planned -app Fileserver -s W2K3-TGT t W2K3-SRC -builtIn -tag NONE **-CrashConsistency**

Post script: "C:\Program Files (x86)\InMage Systems\application.exe" - failback -planned -app Fileserver -s W2K3-TGT -t W2K3-SRC -builtIn -tag PLANNED **-tagtype USERDEFINED**

6.4.2 Failback through CLI

When you run through CLI follow the same procedure as in section 8.2.4.
The only change is add "**–crashconsistency**" switch to the source command and target command with "**-tagtype USERDEFINED**".

Source command:
"C:\Program Files (x86)\InMage Systems\application.exe" - failback -planned -app Fileserver -s W2K3-TGT -t W2K3-SRC -builtIn -tag NONE **-CrashConsistency**

Target command:
"C:\Program Files (x86)\InMage Systems\application.exe" - failback -planned -app Fileserver -s W2K3-TGT -t W2K3-SRC -builtIn -tag <User Defined Tag> **-tagtype USERDEFINED**

6.5 Unplanned Failover

When you set the unplanned failover job, in the unplanned failover template, add the postscript with-"**-tagtype USERDEFINED**". The same can be used for the CLI

For example,
"C:\Program Files (x86)\InMage Systems>application.exe -failover -unplanned -app Fileserver -s W2K3-SRC –t W2K3-TGT -builtIn -tag LATEST **-tagtype USERDEFINED"**

Part 2: Clustered Production Server and Standalone DR Server

This part explains protecting File Server in a environment where production server is a cluster and DR server is standalone.

7 Introduction to Clustered solution

This solution is divided into three major sections: Protect, discover, failover and failback. Each of these sections contains a set of steps.

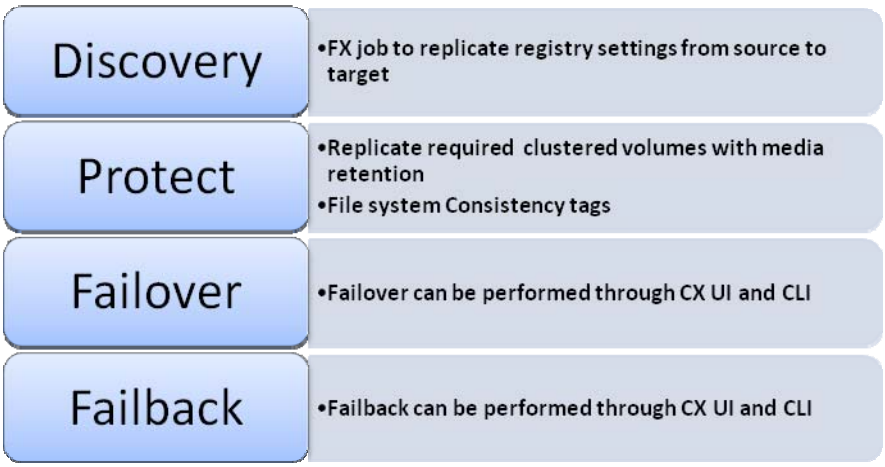

Figure 88:

Discovery: A plain VX replication replicates all data on the clustered source volume. Folders which are shared on the source volume will not be shared on the target volume after roll back. Since all the "shared" information will be stored within the system registry. To overcome this, a discovery job replicates all shared information (registry file) from the source host to the target host.

Protect: Replicate desired volumes on a clustered file server to a standalone target host with CDP retention enabled. Only Shared folders residing on replicated volumes will be protected and recovered.

Failover: This section explains planned and unplanned failovers both through CX UI and command line interface.

Failback: A failback is similar to that of a planned failover. Failback is performed in a set of three steps.

Caution:

After setting the replication pair, again run the discovery job as discovery job gather the file share information specific to the protected volume.

8 Protect

Refer to the Prerequisites section on page 11

8.1 Discovery

A discovery job is executed to discover file share volume available on the production server. Discovery can be performed through CX UI and CLI.

Through CX UI

Step 80. Login to the CX UI, click on "**File Protection -> New Job Group Wizard"**

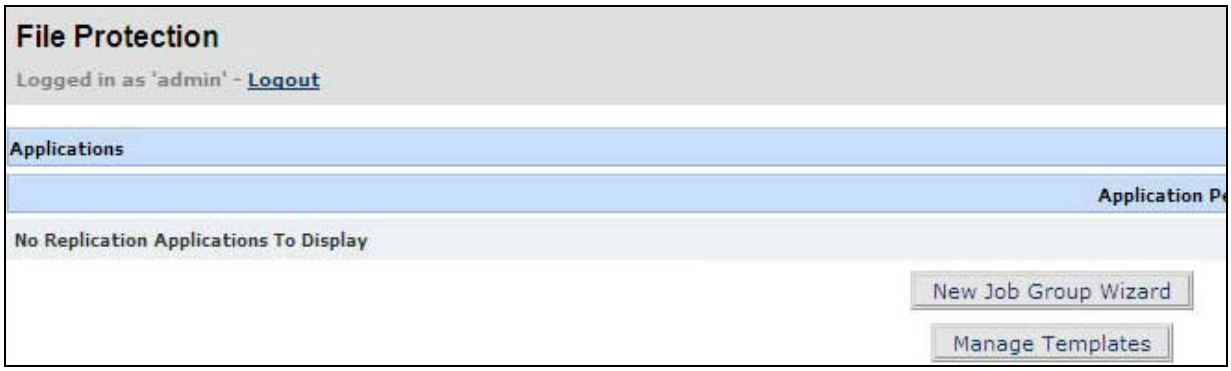

Figure 89:

Step 81. The next screen opens up, click on "**Add Job"** to continue.

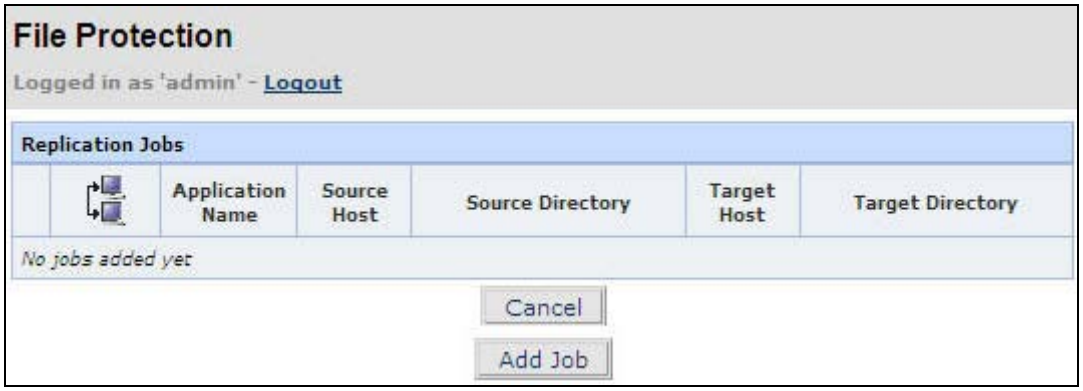

Figure 90:

Step 82. Select the active node as the "**Source"** and the standalone target host as "**Destination"**. Select the FX template as "**FileServer Discovery"** and click on "**Next"**

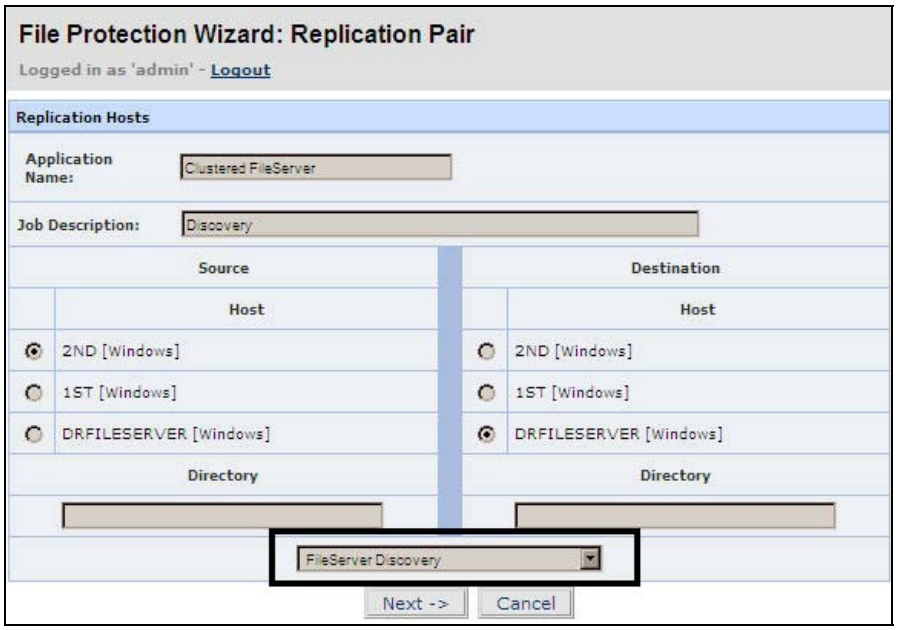

Figure 91:

Step 83. The FX job Options screen opens up with all the required fields filled up. Scroll down to "**Miscellaneous Options**" to append the switch **– `virtualserver` <*name of the virtual server*>** to the source Pre script. Then click on "**Finish"**

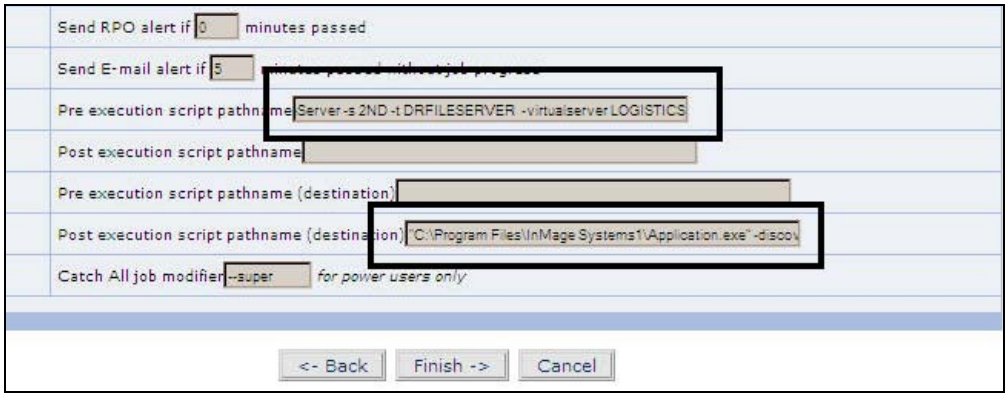

Figure 92:

Step 84. The job is set to execute "**On Demand",** you may change this by clicking on "**Set Schedule"** button. Click on "**Finish"** to save the job.

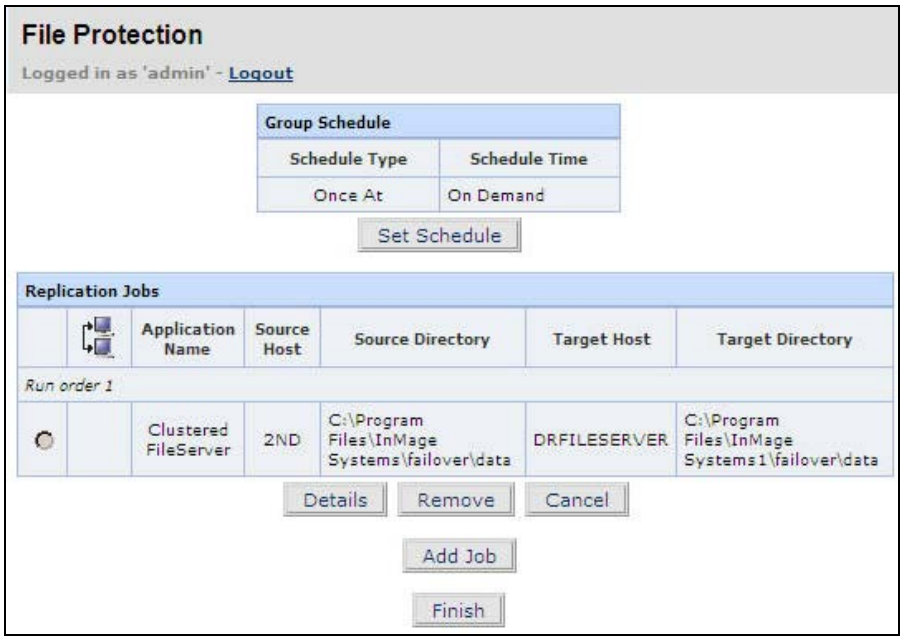

Figure 93:

Step 85. Click on "**File Protection"** then select the Discovery job and click on "**Start**"

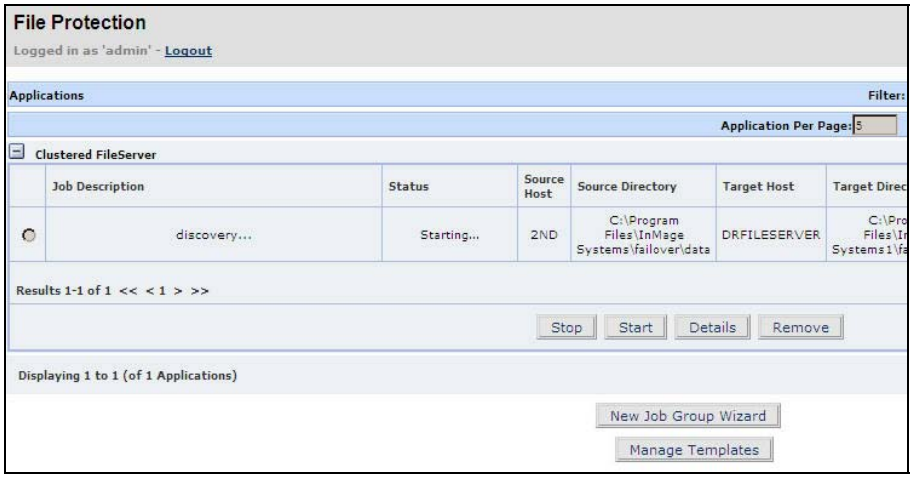

Figure 94:

You may monitor the job's progress through the "**Protection Status"** screen

Through CLI

Discovery can also be performed through command prompt.

Step 86. Switch to the active node's command prompt and navigate to the VX agent installation path to issue the following command

`Application –discover –s <name of the source host> -t <name of the target host> -app fileserver –virtualserver <name of the virtual server>`

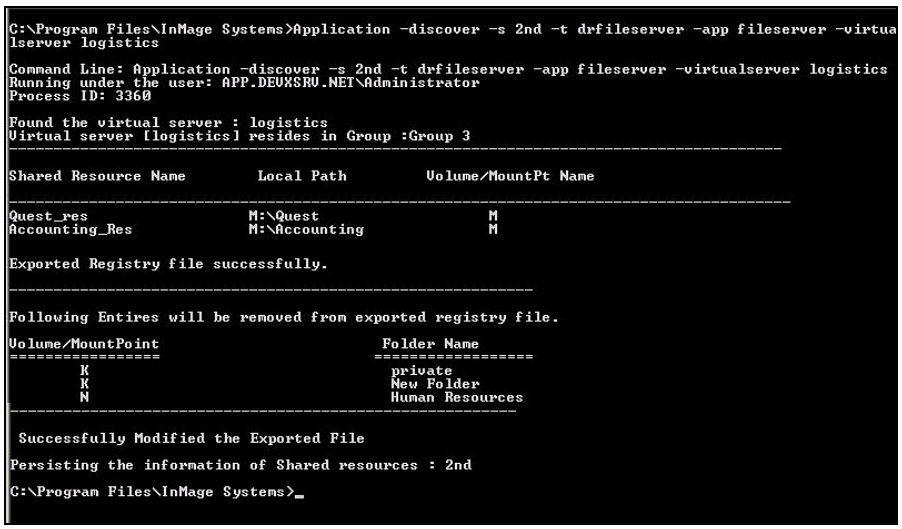

Figure 95:

Step 87. Then copy the folder "**<VX install path>\Failover\Data**" folder to the same location on the target host. Switch to the target command prompt to issue the following command

`Application –discover –s <`*`name of the active node`***`> -t <`***`name of the target host`***`> -app fileserver`**

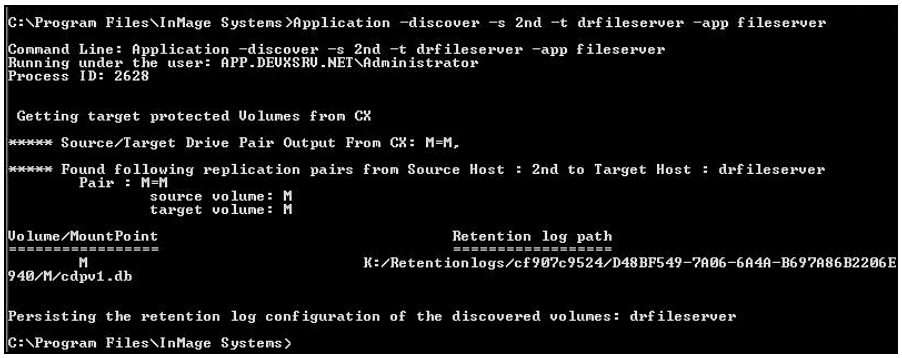

Figure 96:

8.2 VX replication

Step 88. Open the CX UI and click on "**Volume Protection"** expand the "**Cluster Group(s) Volumes**" to select the clustered source volume and click on "**Start Replication"**

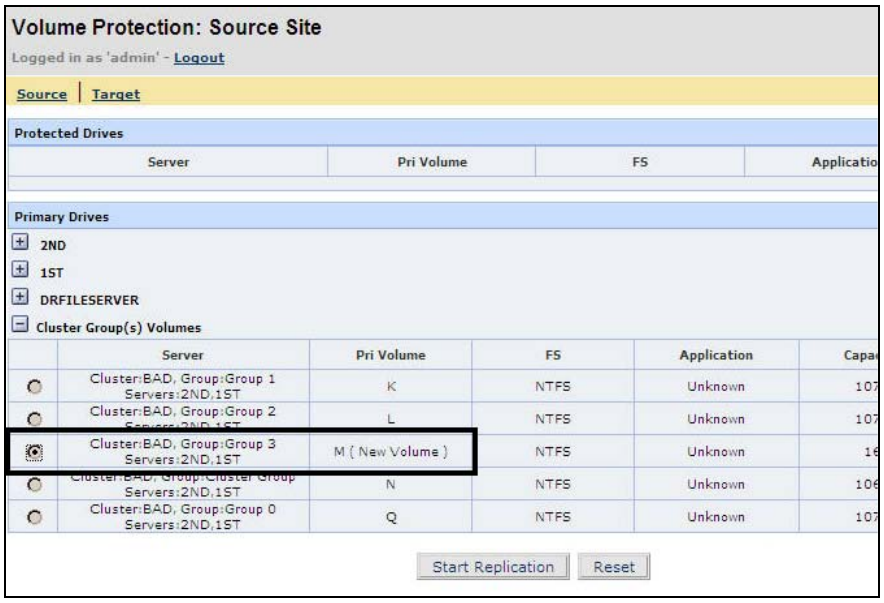

Figure 97:

Step 89. This will open up the next screen, select the clustered volume and click on "**Next"** to continue

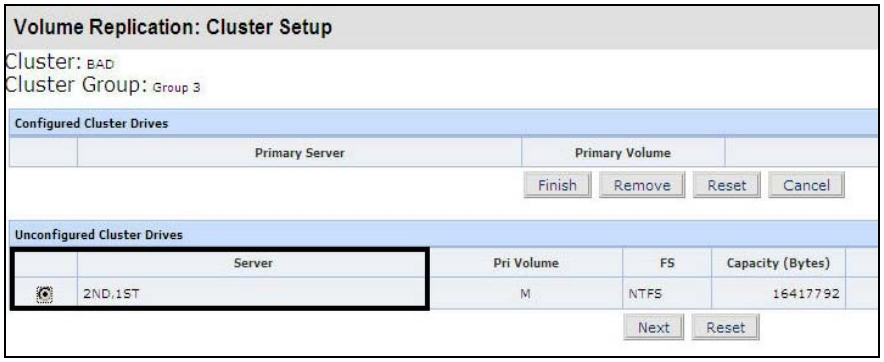

Figure 98:

Step 90. The target screen opens up, expand the standalone target host to select the target volume with save drive mapping and scroll down to set the "**Replication options"**

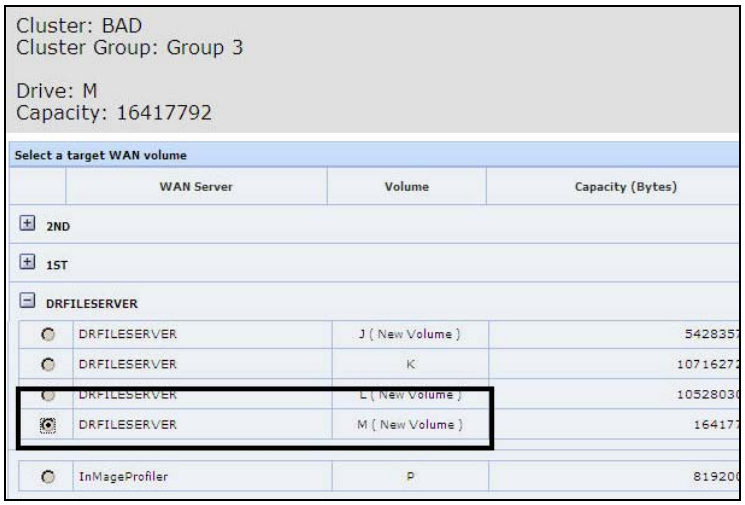

Figure 99:

Step 91. Select a desired "**Process Server**" and scroll down.

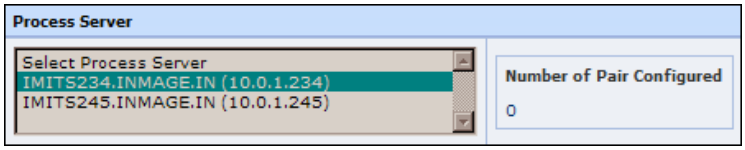

Figure 100

Step 92. Enable the "**CDP Retention**" option, the rest are optional.

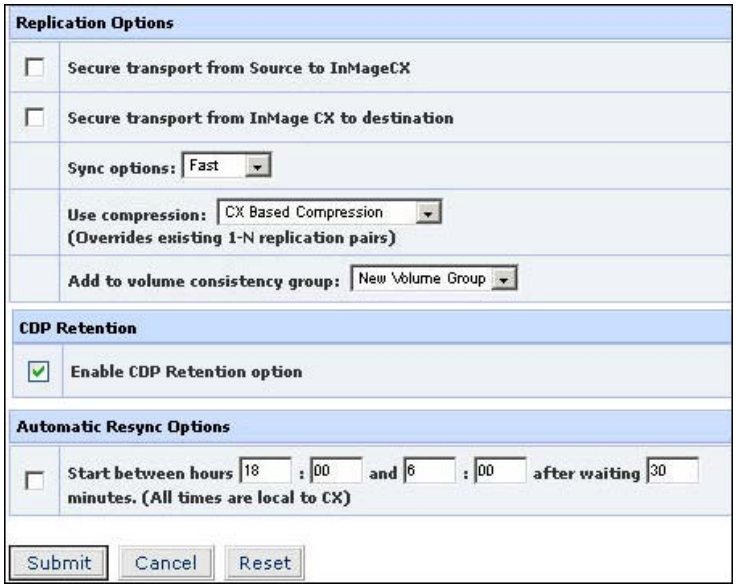

Figure 101:

Step 93. Define the retention policy (time based, space based or a combination) then click on "**Submit"** to proceed to the last screen.

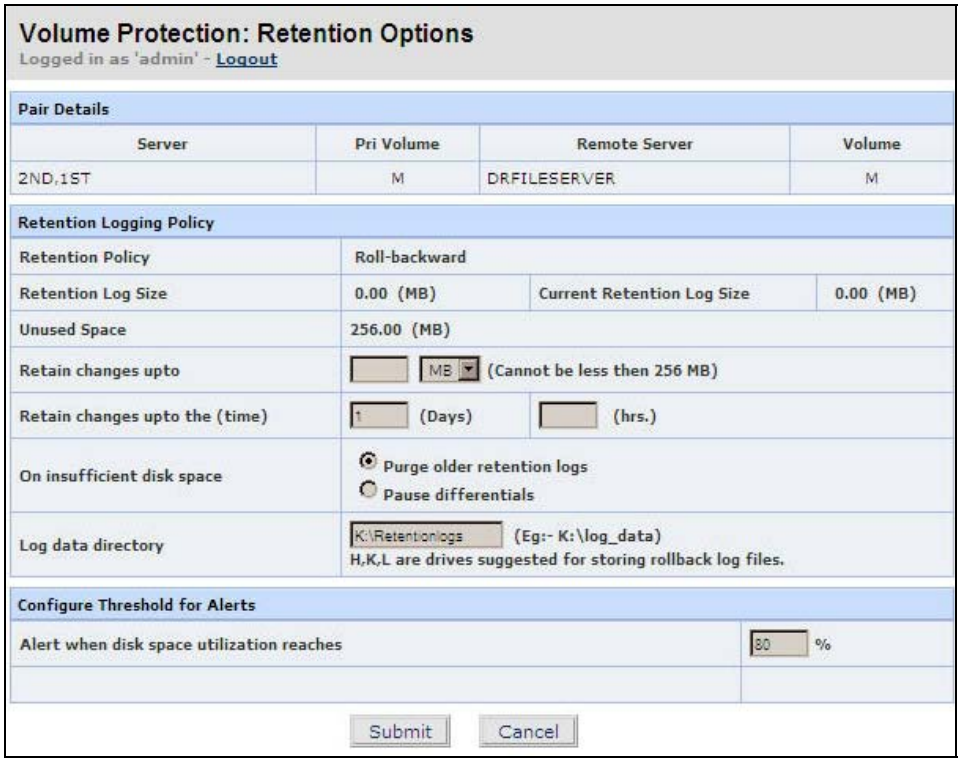

Figure 102:

Step 94. Select the clustered volume and click on "**Finish"** to start the replication pair

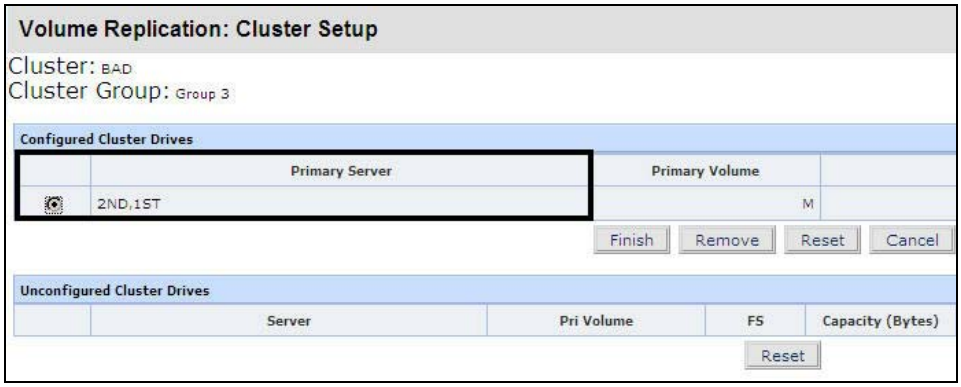

Figure 103:

Step 95. Click on "**Protection Status**" to monitor the replication pair. The replication pair starts from Resyncing (step 1) then move to Resyncing (Step 2) and finally reaches "**Differential Sync**"

Protection Status

Logged in as 'admin' - Logout

Server Time: Jul-11-2008 08:01:48

Volume Protection Status

Server	Volume	Group	Resyncs In Transit Step1 (MB)	Resync In Transit Step2 (MB)	Differentials Left (MB)	Resync progress	RPO	Status	Resync Required	View Details
Cluster:BAD, Group:Group 3 Servers: 1ST,2ND->DRFILESERVER	M (New Volume) -> M (New Volume)	Volume M	0	0	0	0 %	0	Resyncing (Step 1)	YES	⊞

Figure 104:

Caution:

You will need to enable CDP retention for all VX replication pairs

8.3 Consistency

Consistency tags can be issued either through CX UI or through CLI.

Through CX UI

Step 96. Set a new FX job with active node as "**Source**" and standalone target host as the "**Destination"** then select the FX template as "**FileServer Consistency**", then click on "**Next"** to continue

Figure 105:

Step 97. The Job Options screen opens up with all the required fields filled up; scroll down to observe the source pre script filled up. Do not change any settings, click on "**Finish"** to continue

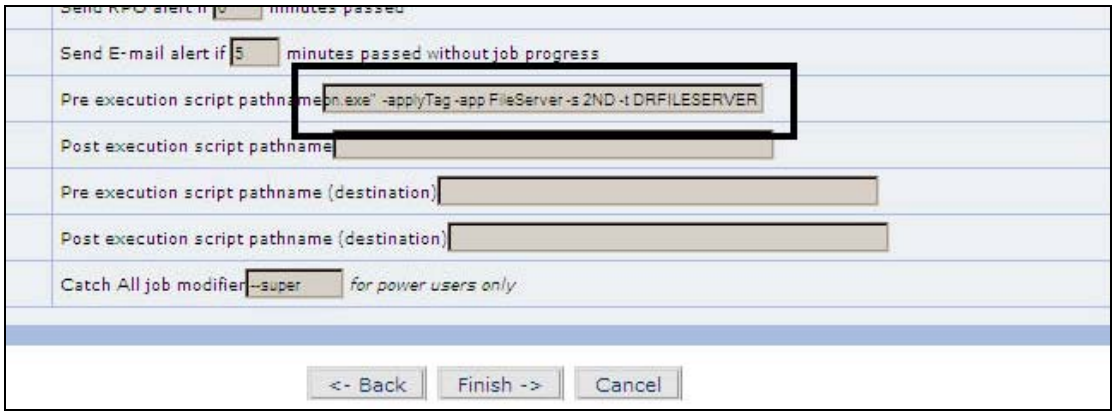

Figure 106:

Step 98. Consistency job is set to execute every six hours by default, you may choose to change this through the "**Group Schedule**". Click on "**Finish"** to save the job

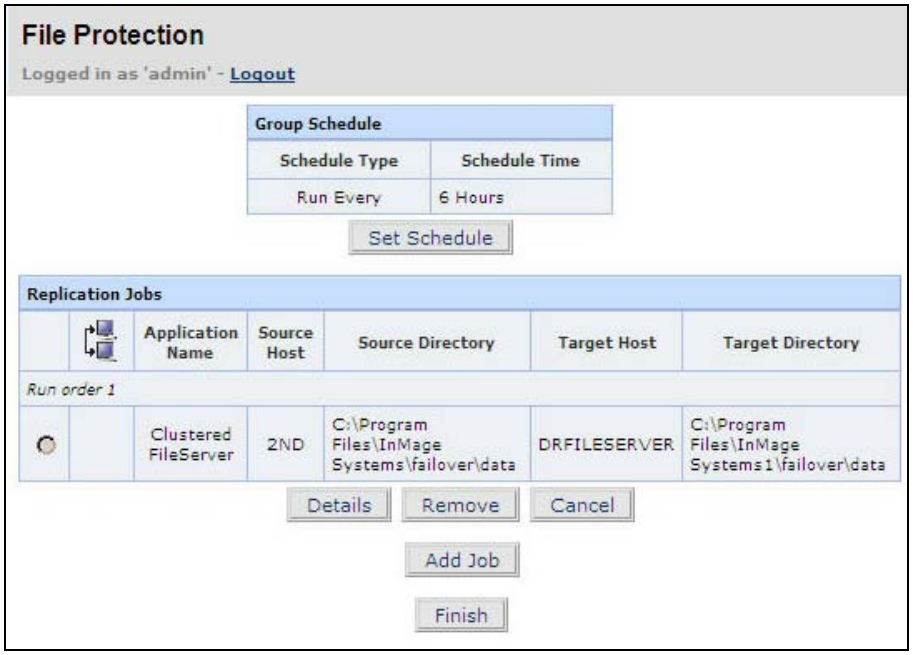

Figure 107:

Step 99. Click on the "**Protection Status**" to monitor the VX replication pair, discovery and consistency jobs.

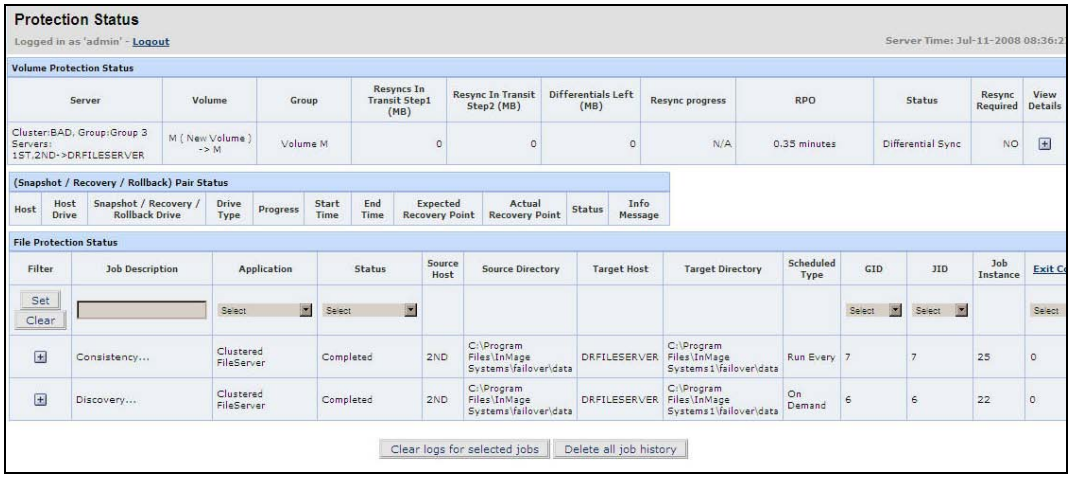

Figure 108:

Through CLI

Consistency can also be executed through the source (active node) command prompt. Access the command prompt and navigate to the VX agent installation folder to issue the following command

Application –app fileserver –applytag –s <*name of the source host***> -t <***name of the target host***> -Bookmark "<***Name of the event***>"**

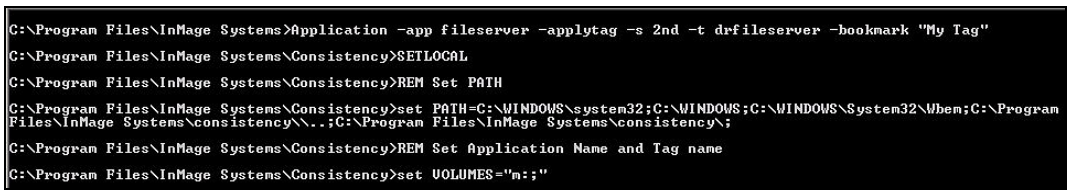

Figure 109:

9 Failover

9.1 Pre-requisites for failover or failback

- Ensure target volume drive letter or mountpoint is same as that of Source drive letter or mountpoint when setting the replication pair.
- For cluster File Server, when performing failover through CX UI, it is required that FX agent service of production server or target DR server must be running under domain administrator or domain user that was created for failover job.
- For clustered File Server, ensure that the network name resource of the production file server is online else failover might not be successful.

 **Notes:**

"-useuseraccount" option is not applicable for CLUSTER. If user specifies "–useuseraccount", it will be ignored.

File server failover does not support web sharing

To restore folder icons after a failover, the respective icons need to be replicated to the path on DR file server that is identical to the path on production file server

Cluster File server failover is supported only for single network name. Failover of file shares having multiple network name dependencies is not supported.

For Windows Vista and Windows Server 2008, if MS Shadow copy provider is not properly installed, VACP will hang as VSS will take time to send the response to VACP. When VACP fails, look at the Application event log for more information

9.2 Planned through CX UI

Step 100. To perform a planned failover through CX UI, click on "**File Protection-> New Job Group Wizard"** to set the FX job

Figure 110:

Step 101. Click on "**Add Job"** on the next screen

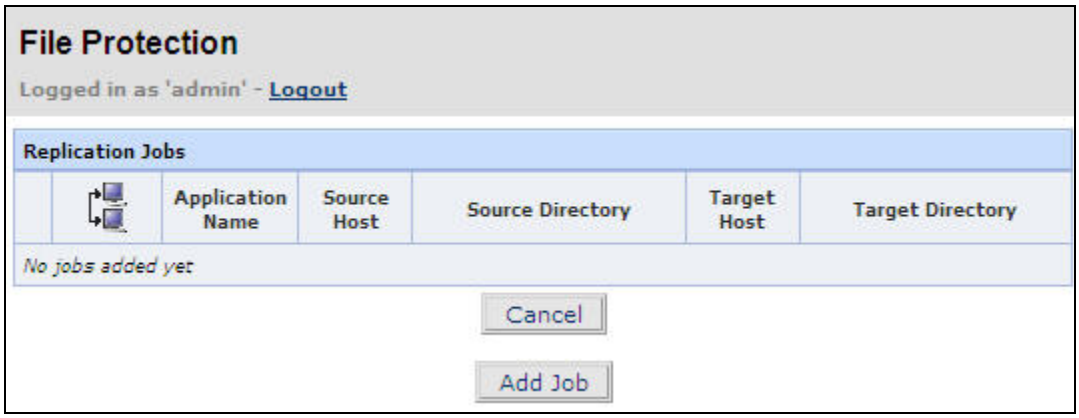

Figure 111:

Step 102. Select the active node (clustered source host) as the "Source" and standalone target host as the "**Destination",** Select the FX template as "**FileServer Planned Failover**" and click on "**Next"** to proceed

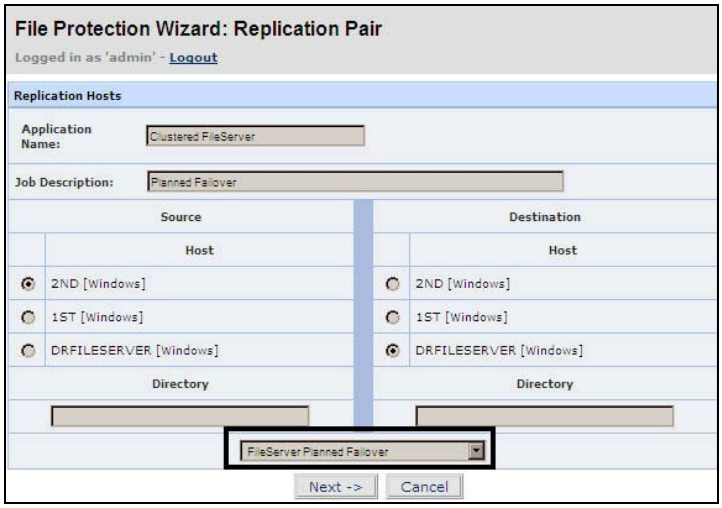

Figure 112:

Step 103. The "**Job Options"** screen opens up, scroll down to "**miscellaneous options"** to add the **`–virtualserver <`*`name of the virtual server`*`>`** switch to the end of the source pre script and target post script as given in the picture below. Click on "**Finish"** to continue

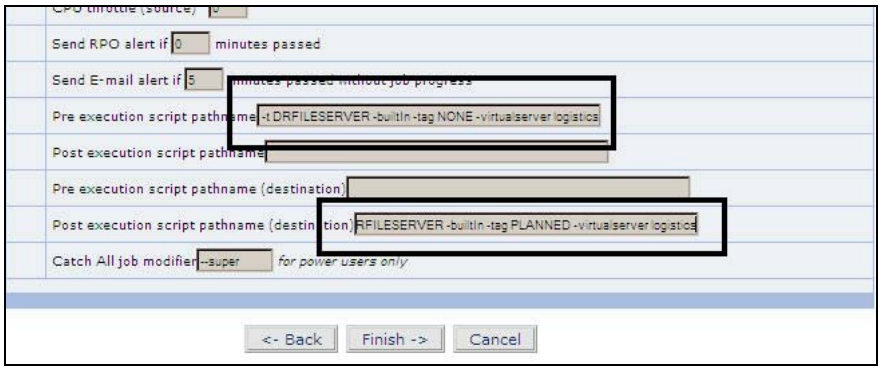

Figure 113:

Notes:

Adding the –virtualserver switch is specific to clustered file server.

Step 104. The job is set to execute "**On Demand"**, click on "**Finish"** to save the job.

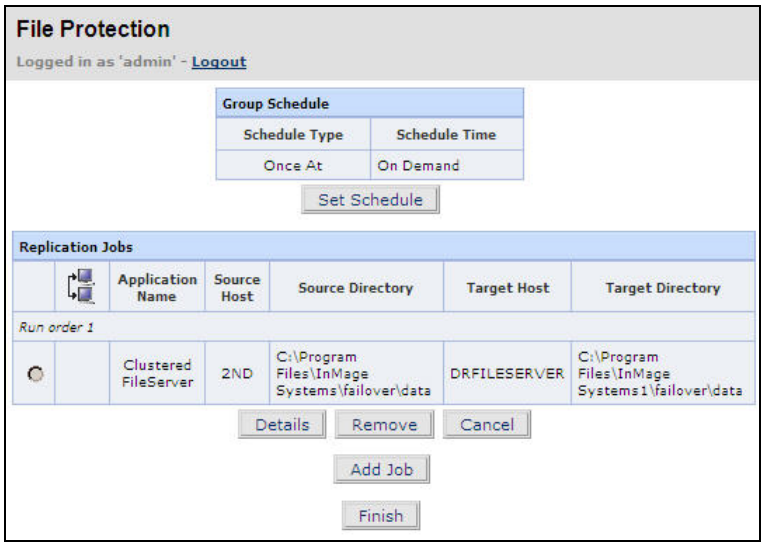

Figure 114:

Step 105. Start the job through "**File Protection"** screen to perform a planned failover from clustered file server to a standalone file server. You may monitor the failover progress through the "**Protection Status"** screen.

9.3 Planned through CLI

Planned failover can also be performed through CLI. Access the active node's command prompt and then navigate to the VX agent installation path to issue the following command

Application –failover –planned –s <*name of the clustered source host***> -f <***name of the standalone target host***> -app fileserver –builtin –virtualserver <***name of the virtual server***> -tag none**

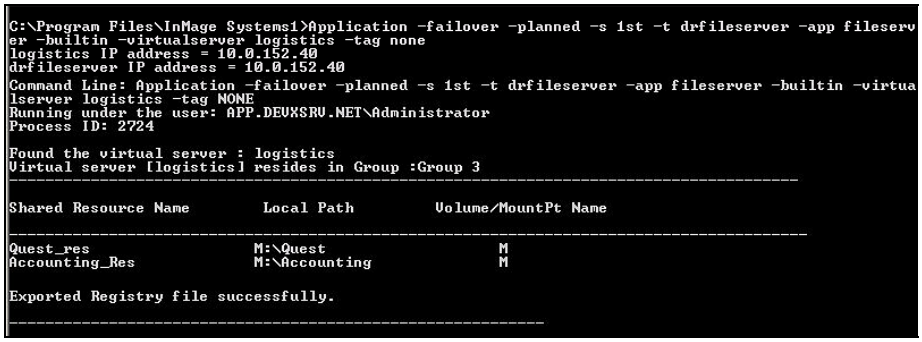

Figure 115:

At the end of the command the output is displayed enclosed within "**Important Information**". This is the command that has to be executed on the target console to complete the planned failover.

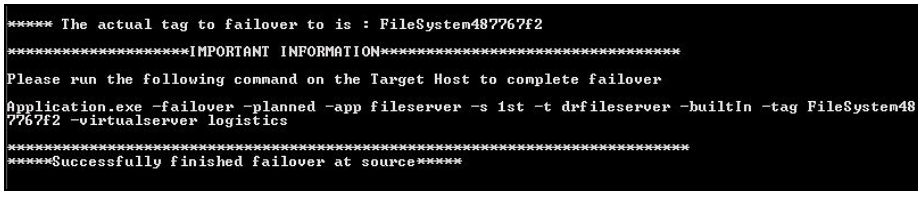

Figure 116:

Then copy the folder "**<VX install path>\Failover\Data**" folder to the same location on the target host. Switch to the target command prompt to issue the command.

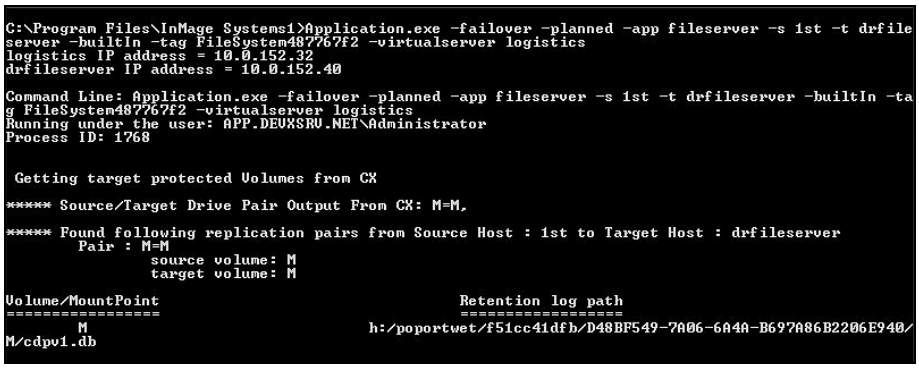

Figure 117:

9.4 Unplanned through CX UI

Caution:

Ensure that the Discovery and Consistency jobs have successfully completed at least once after any change in the configuration to ensure that target node has latest information.

Step 106. Setup an FX job with "**Source"** and "**Destination"** as the standalone file server (since the production server is down). Select the FX template as "**FileServer Unplanned Failover"**

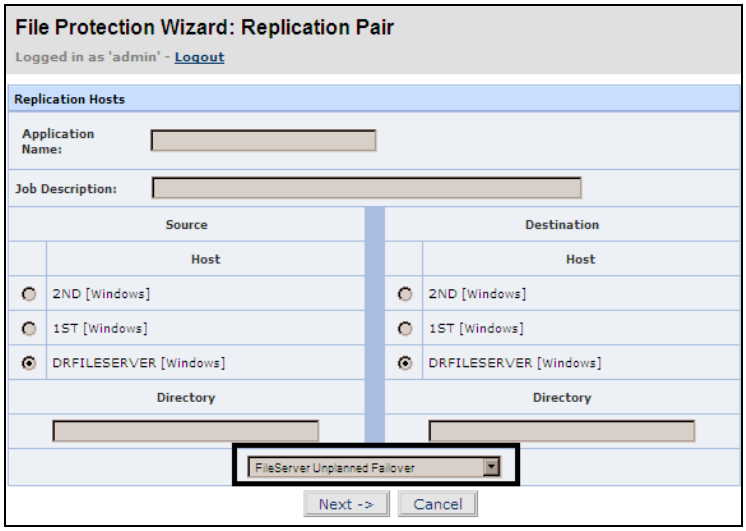

Figure 118:

Step 107. The Job Options screen opens up, scroll down to miscellaneous options to append the switch **`-virtualserver <`*`name of the virtual server name`*`>`**. Click on "**Finish"** to proceed

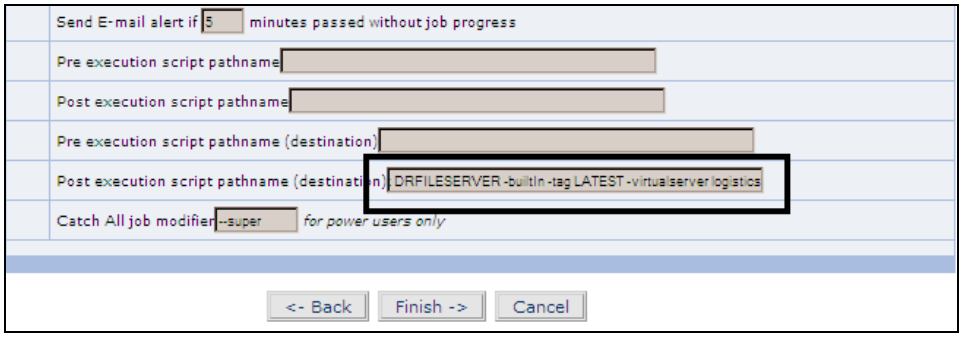

Figure 119:

Step 108. The job will be set to execute "**On Demand**". Click on "**Finish**" to save the job. You may start the job through the "**File Protection**" screen to perform an unplanned failover.

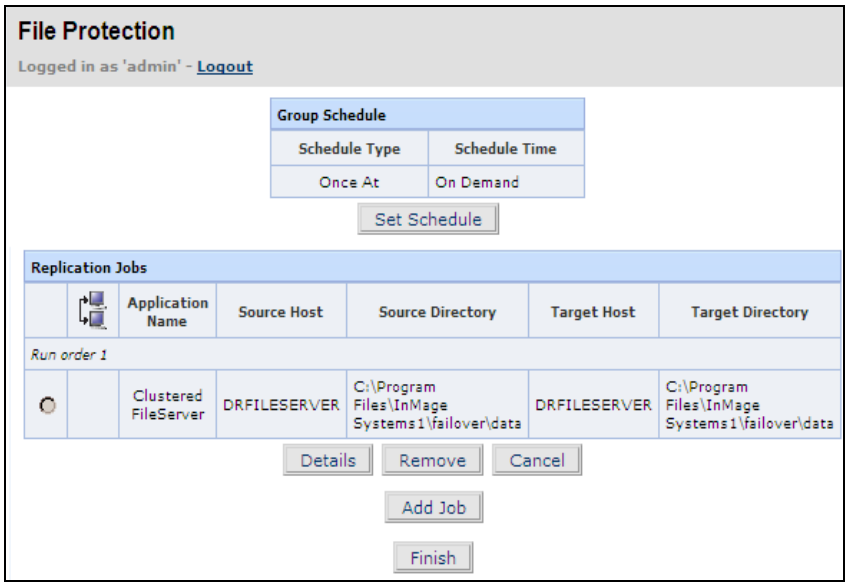

Figure 120:

You may monitor the status through the "**Protection Status**" screen on the CX UI.

9.5 Unplanned through CLI

To perform an unplanned failover through CLI, access the target host's command prompt to issue the following command

Application –failover –unplanned –s <*name of the clustered source file server***> -t <***name of the standalone target server***> -app fileserver –tag LATEST –builtin –virtualserver <***name of the virtual server***>**

```
C:\Program Files\InMage Systems1>Application -failover -unplanned -s 1st -t drfileserver -app filese
rver -tag LATEST -builtin -virtualserver logistics
logistics IP address = 10.0.152.32
drfileserver IP address = 10.0.152.40

Command Line: Application -failover -unplanned -s 1st -t drfileserver -app fileserver -tag LATEST -b
uiltin -virtualserver logistics
Running under the user: APP.DEVXSRV.NET\Administrator
Process ID: 2160


 Getting target protected Volumes from CX

***** Source/Target Drive Pair Output From CX: M=M,

***** Found following replication pairs from Source Host : 1st to Target Host : drfileserver
        Pair : M=M
                source volume: M
                target volume: M

Volume/MountPoint                                   Retention log path
=================                                   ==================
        M                                   h:/poportwet/f51cc41dfb/D48BF549-7A06-6A4A-B697A86B2206E940/
M/cdpv1.db
```

Figure 121:

10 Failback

A failback is the reverse of a failover. Failover can only be performed to a standalone server. However, to perform a failback to a clustered server, it will be turned into a standalone server during the failback process. Once the failback is complete it will be turned back into a clustered server.

Figure 122:

10.1 Cluster to standalone

Step 109. Access the active node's command prompt, and then navigate to the VX agent installation path to issue the following command

`Clusutil –prepare clustertostandalone:` **<***name of the active node***>** **`-shutdown`** **<***name of the passive node***>**

Figure 123:

After the command is execute the active node will turn into a standalone server while the rest of the nodes are shutdown.

Notes:

For Windows Server 2008 cluster, you will need to perform onlinedisk operation after the node restarted as the result of the above step.

In Windows Server 2008 cluster, after server restarts, cluster disk will be offline and cannot be used until it becomes online. You may use the "ClusUtil.exe –onlinedisk" command to bring all the disks online.

When you need only selected clustered disks online, you may access the cluster management interface and take the other disks offline

10.2 Reverse replication

Step 110. Proceed to set a reverse replication from standalone file server to the active node which is turned into another standalone server (original source host).

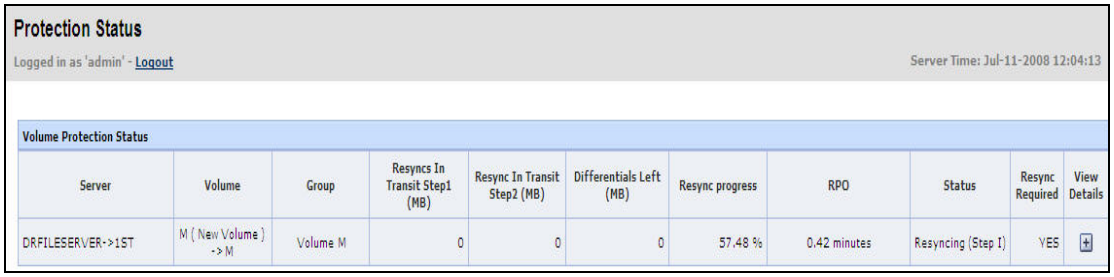

Figure 124:

10.3 Discovery

Step 111. Set the FX job to replicate shared information specific to the VX replication pair from the DR file server to the production file server. Select the "**Source"** as original target and "**Destination"** as the production file server (now a standalone server). Select the FX template as "**FileServer Discovery"**

Figure 125:

Step 112. The Job Options screen opens up with all the required fields filled up automatically, scroll down and click on "**Finish"** to continue.

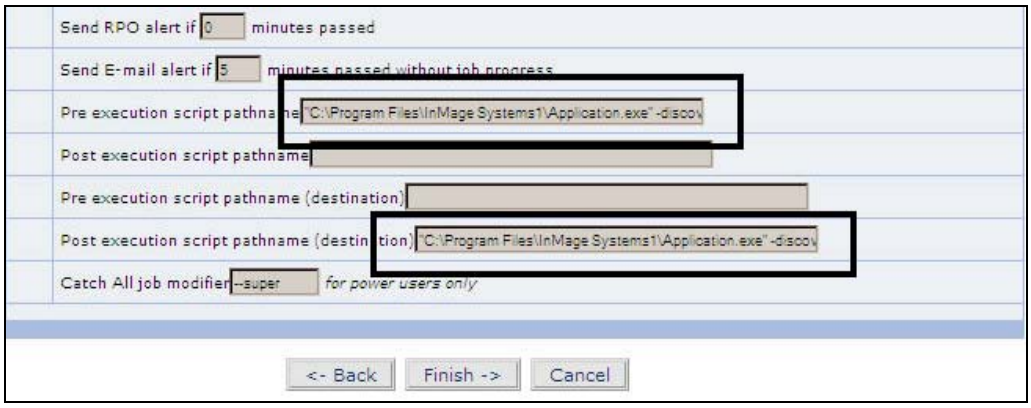

Figure 126:

Step 113. The next screen opens up, the job is set to execute "**On Demand"**. Click on "**Finish"** to save the job. You can start the job through the "**File Protection"** screen.

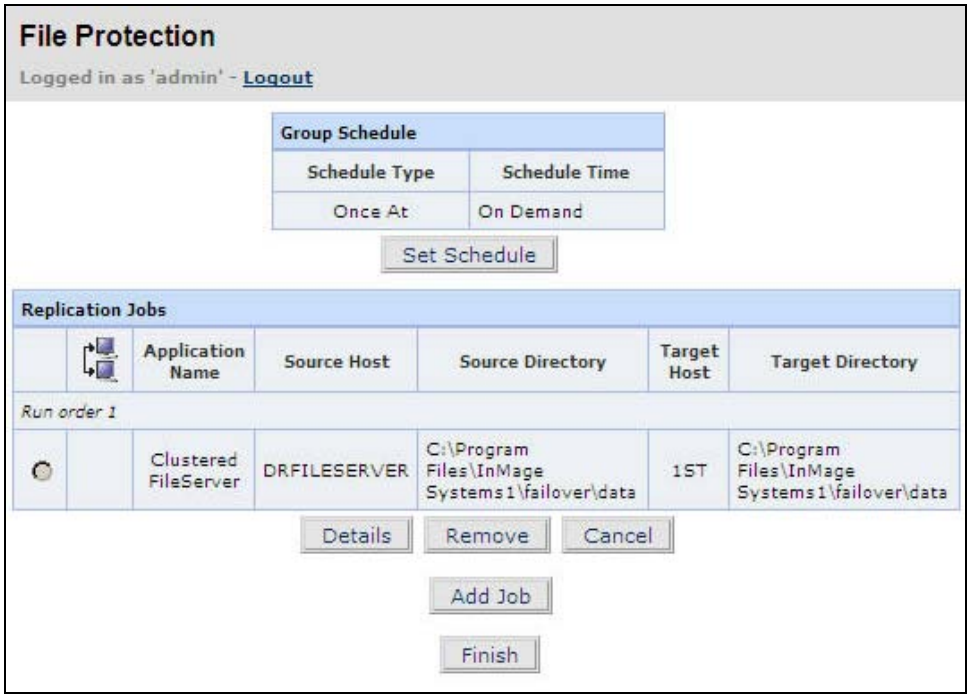

Figure 127:

10.4 Failback

Step 114. Once the Discovery job is completed, proceed to setup another FX job for the failback. Select the source as the DR file server (original target) and Destination as the newly created standalone server (once clustered file server). Select the FX template as "**FileServer Planned Failover"** and click on "**Next"** to continue.

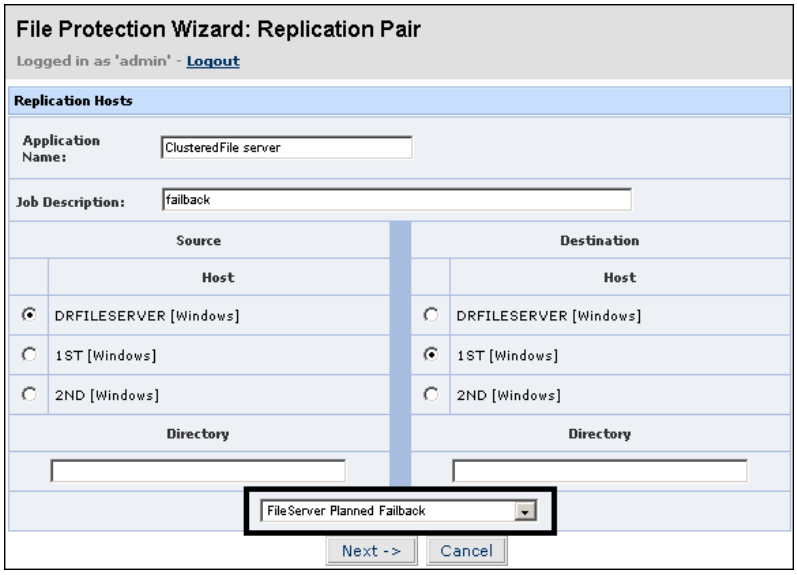

Figure 128:

Step 115. The "**Job Options"** screen opens up, scroll down to "**miscellaneous options**" to add the **`-virtualserver <name of the virtual server>`** to both source prescript and target post script. Then click on "**Finish"** to continue

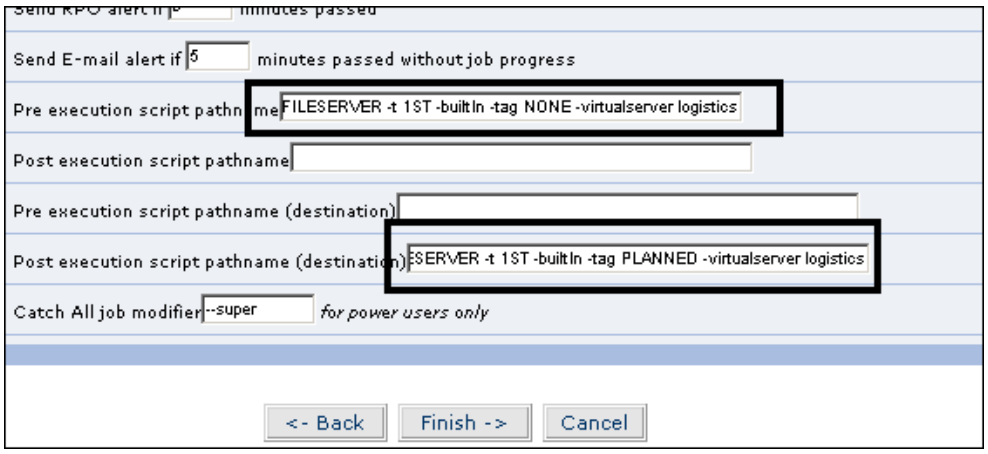

Figure 129:

Step 116. The job is set to execute "**On Demand"**. Click on "**Finish**" to save the job and start the job through "**File Protection"** to perform a failback.

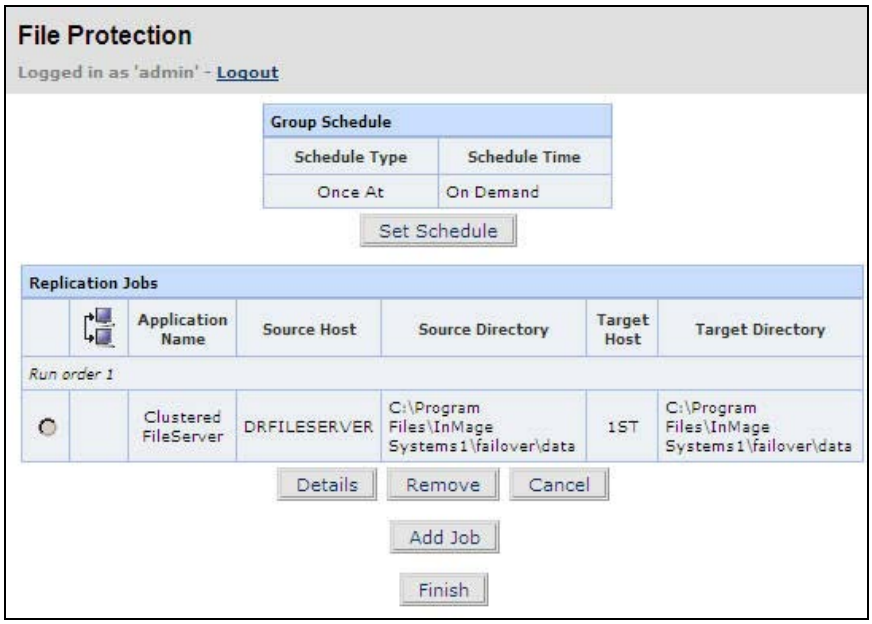

Figure 130:

You may monitor the progress on the "**protection status"** screen on the CX UI

10.5 Standalone to cluster

Step 117. After failback, access the standalone production server to convert it back to a clustered server. Access the command prompt, and then navigate to the VX agent installation path to issue the following command

```
ClusUtil.exe -prepare StandalonetoCluster <standalone name>
```

```
C:\Program Files\InMage Systems>clusutil.exe -prepare -StandalonetoCluster 1st
```

Figure 131:

This will restart the machine and restore it to its former clustered state. Then start all passive nodes that were shutdown earlier. Access the cluster administrator interface to bring the fileserver group online. Verify that all the cluster resources are coming online and client can access the cluster.

Part 3: Clustered Production Server and Clustered DR Server

This part explains protecting File Server in an environment where production server and DR server both are in clustered environment.

11 Cluster to Cluster Environment

This part of the document explains protecting a clustered file server to another clustered server. The DR cluster needs to be prepared to act as a target for the replication pairs.

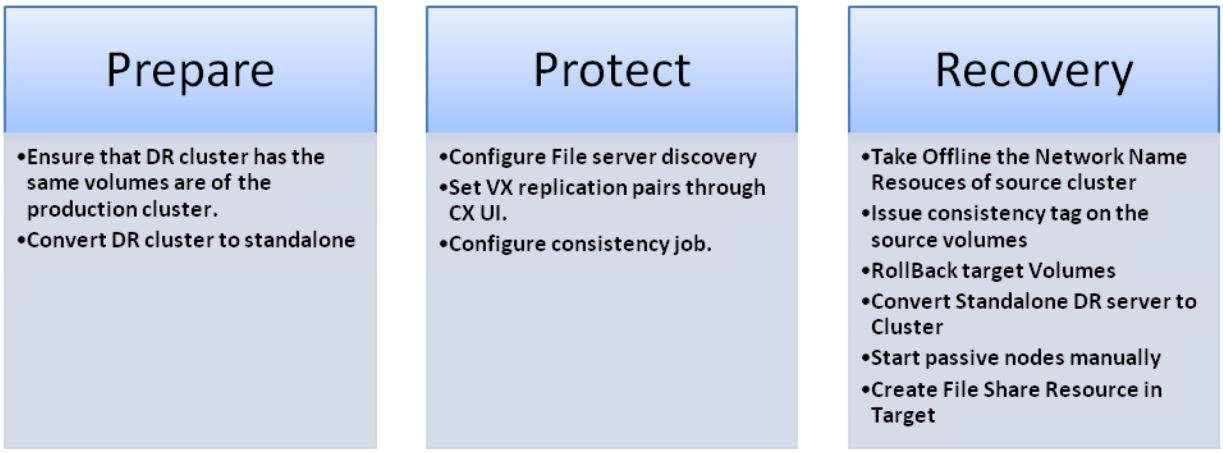

Figure 132:

Caution:

After setting the replication pair, again run the discovery job as discovery job gather the file share information specific to the protected volume.

11.1 Prepare:

The prepare step describes steps to prepare the DR cluster before setting VX replication pairs.

You will first need to offline the Network Name Resources of the DR cluster to restrict any further changes to the volume on the DR cluster.

Convert DR cluster to standalone DR server using the clusutil.exe command under the Vx agent install directory. All passive nodes on the DR server will be shut down and the active node goes down for a reboot and comes back as a standalone DR server. This enables you to set VX replication pairs.

```
clusutil.exe -prepare clustertostandalone:<active node> -shutdown <Passive node>
```

Notes:

For Windows Server 2008 cluster, you will need to perform onlinedisk operation after the node restarted as the result of the above step.

In Windows Server 2008 cluster, after server restarts, cluster disk will be offline and cannot be used until it becomes online. You may use the "ClusUtil.exe –onlinedisk" command to bring all the disks online.

When you need only selected clustered disks online, you may access the cluster management interface and take the other disks offline

11.2 Protect

Step 118. Configure a file server discovery job through the CX UI. After the FX job is successful, proceed to set the VX replication.

Step 119. Set volume replication from production cluster to standalone DR server with CDP retention enabled. Ensure that you replicate between same drive letters.

Step 120. Once the replication pair reaches "Differential Sync", configure the file server consistency job. This consistency job issues vacp tags on the source volumes at regular intervals. These tags act as markers while performing a recovery operation.

Caution:

You will need to enable CDP retention for all VX replication pairs

11.3 Recovery

Step 121. Offline the "Network Name Resources" of production cluster to avoid further changes on the clustered volumes.

Step 122. Issue consistency tag on the production cluster

```
vacp –V K:; H:  -t "<name of the tag>"
```

Step 123. Rollback target volumes through the CX UI.

Step 124. Convert the standalone DR server back to its clustered form using the clusutil.exe command

```
clusutil.exe -prepare standalonetocluster:<Active node name>
```

You will then need to start the passive nodes manually

Step 125. Create File share resource on the DR cluster

Hitachi Data Systems

Corporate Headquarters
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
www.hds.com
info@hds.com

Asia Pacific and Americas
750 Central Expressway
Santa Clara, California 95050-2627
U.S.A.
Phone: 1 408 970 1000
info@hds.com

Europe Headquarters
Sefton Park
Stoke Poges
Buckinghamshire SL2 4HD
United Kingdom
Phone: + 44 (0)1753 618000
info.eu@hds.com

Hitachi Data Systems

MK-98DF8225-00