Setting up the DR Series System as a Backup Target on ASG-TimeNavigator

Technical White Paper

Quest Engineering

October 2017

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal .

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Zmanda is a trademark of Zmanda Incorporated in the USA.All other trademarks and registered trademarks are property of their respective owners.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Contents

Revisions

Date	Description
January 2014	Initial release
November 2016	Updated with new DR Series system GUI screenshots (version 4.0)
October 2017	Updated with new DR Series system GUI screenshots post-rebranding (version 4.0.3)

Executive Summary

This white paper provides guidelines about how to set up the DR Series system as a backup to disk target for ASG-Time Navigator over CIFS and NFS. This paper is a quick reference guide and does not include all DR Series system deployment best practices.

For additional information, see the DR Series system documentation and other data management application best practices whitepapers for your specific DR Series system at:

http://support.quest.com/DR-Series

NOTE: The DR Series system and ASG-Time Navigator build version and screenshots used for this document may vary slightly, depending on the version of the software you are using.

1

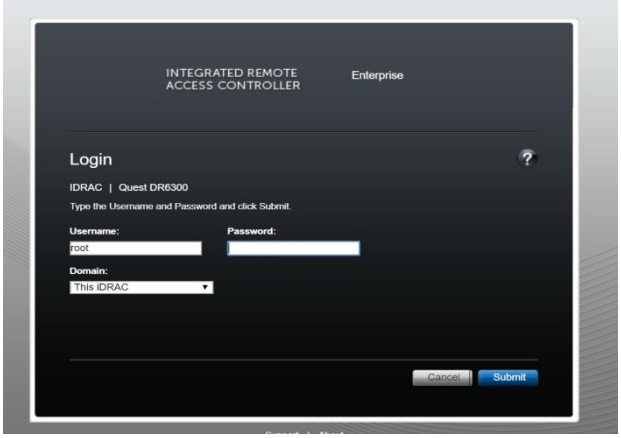
Installing and configuring the DR Series system

Complete the following steps to install and configure the DR Series system.

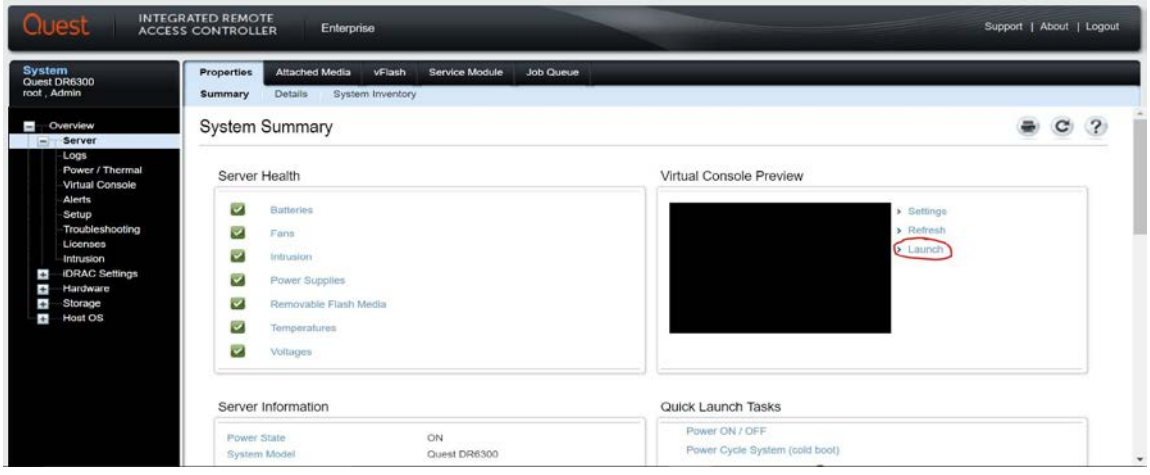
1 Rack and cable the DR Series system, and power it on.

2 Initialize the DR Series system. Refer to the *DR Series System Administrator Guide* topics: “iDRAC Connection”, “Logging in and Initializing the DR Series System,” and “Accessing IDRAC6/Idrac7 Using RACADM” for more information.

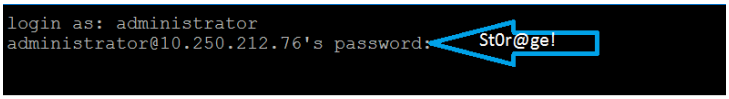
3 Log on to iDRAC using the default address 192.168.0.120, or the IP address that is assigned to the iDRAC interface. Use the user name and password: “root/calvin”.



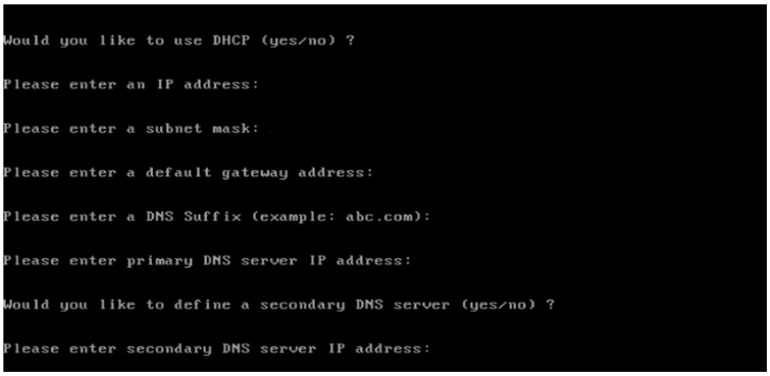
4 Launch the virtual console.



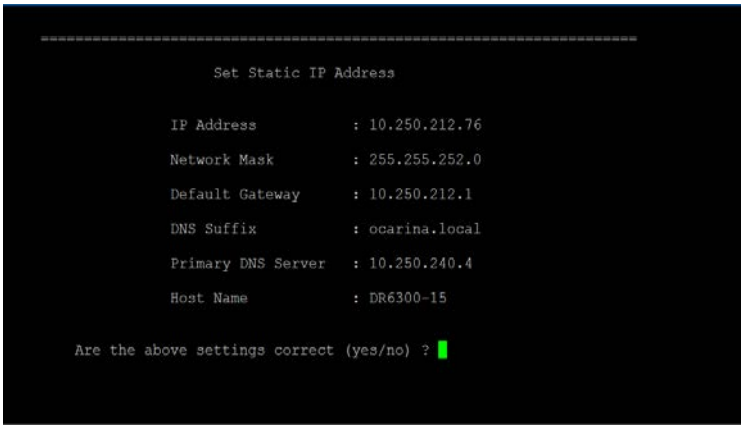
5 When the virtual console is open, log on to the system as user administrator with the password St0r@ge! (The “0” in the password is the numeral zero).



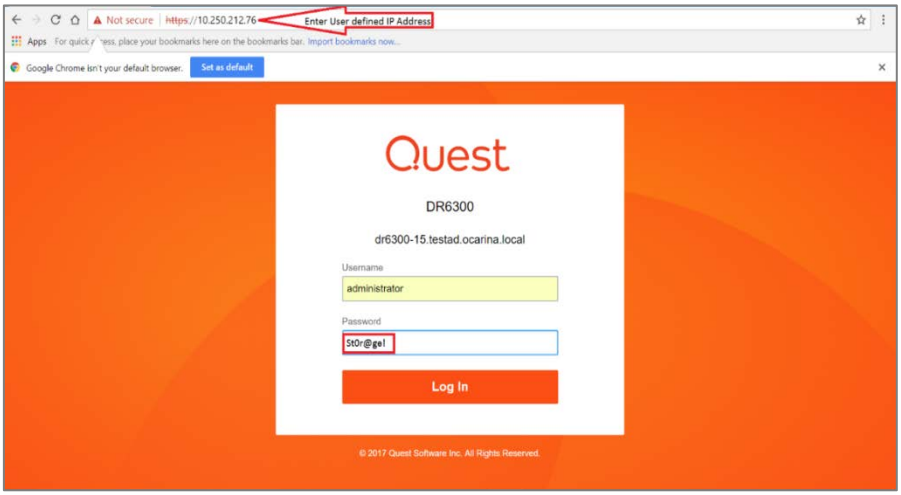
6 Set the user-defined networking preferences.



7 View the summary of preferences and confirm that it is correct.



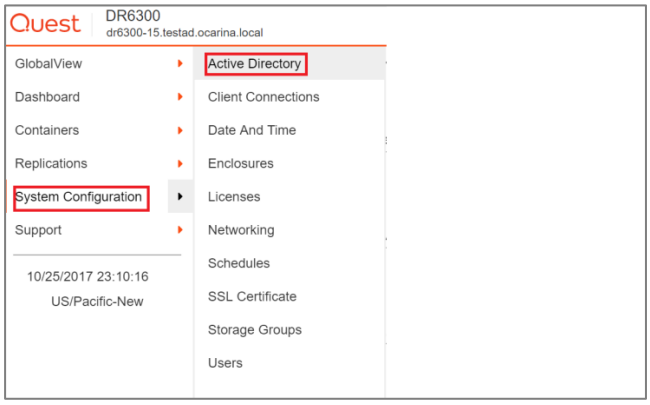
8 Log on to DR Series System administrator console at the IP address you just provided for the DR Series system with the following credentials, username: administrator and password: St0r@ge!



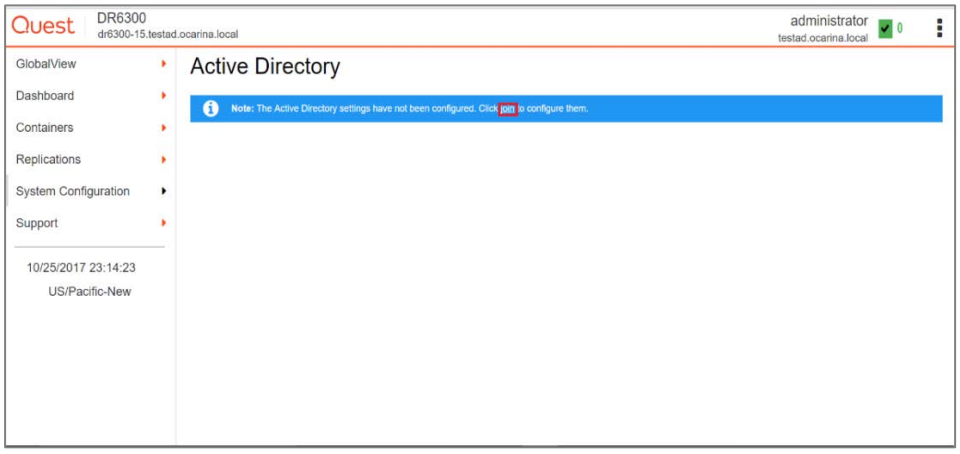
9 Join the DR Series system to Active Directory.

NOTE: If you do not want to add the DR Series system to Active Directory, see the *DR Series System Owner's Manual* for guest logon instructions.

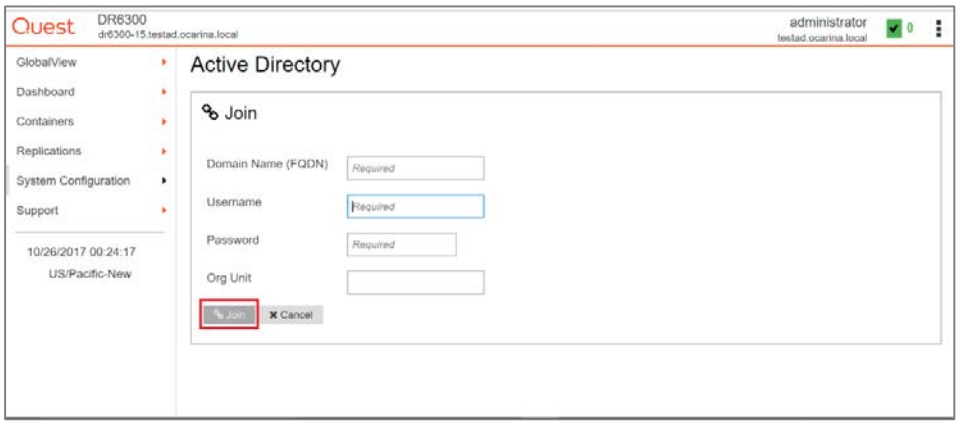
a In the left navigation area of the DR Series system GUI, select **System Configuration >Active Directory**.



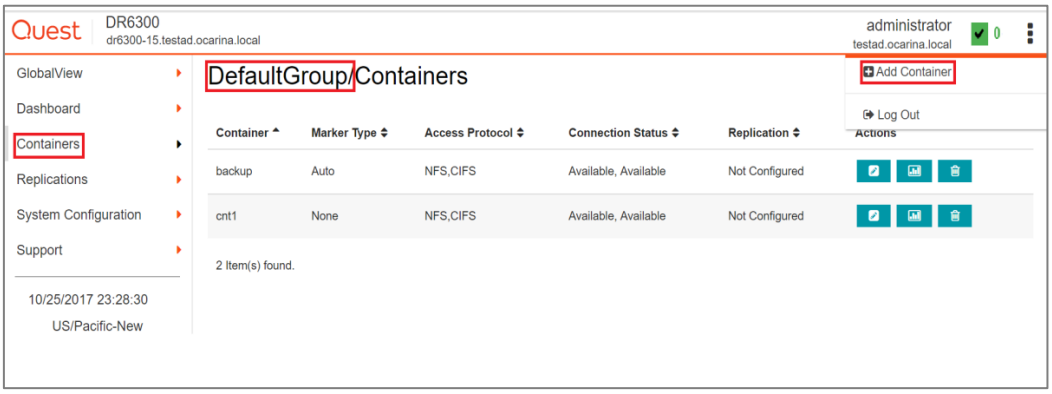
b Click the **Join** link.



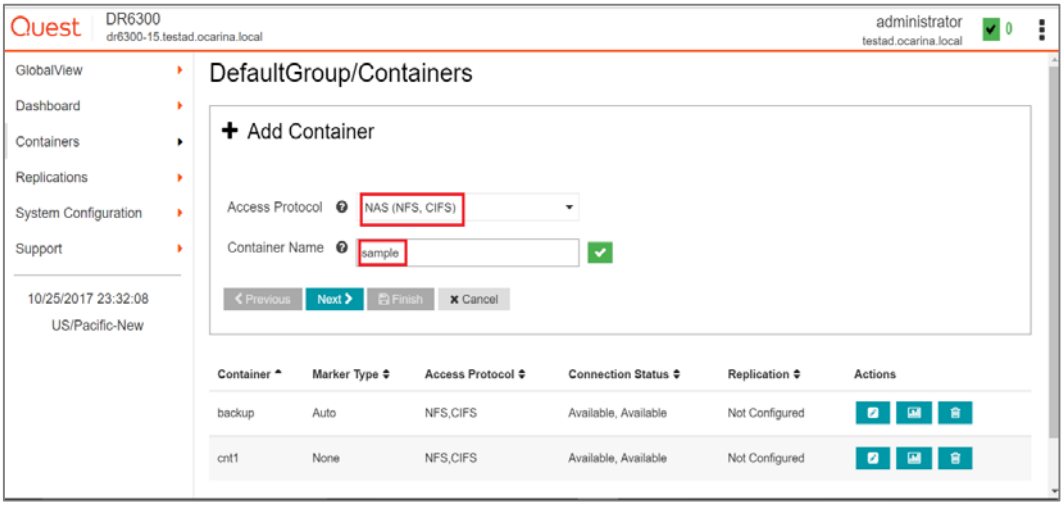
c Enter your Active Directory credentials, and click the **Join** button.



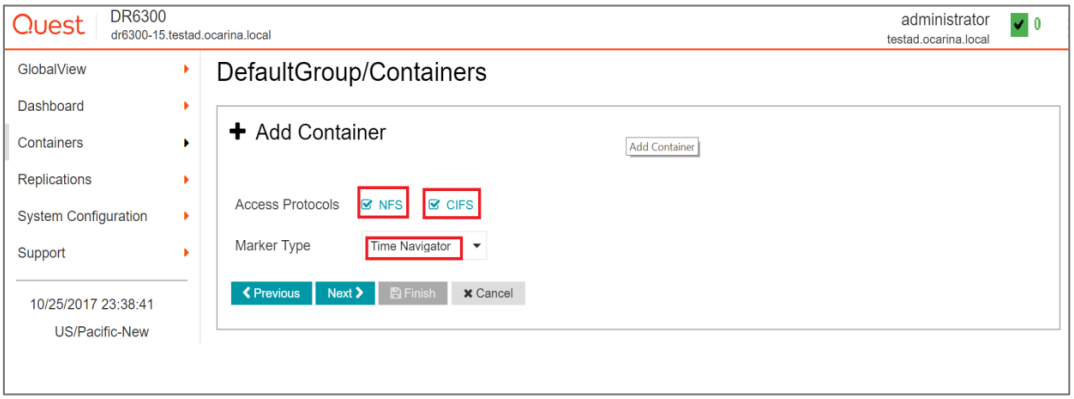
10 Select **Containers** in the left navigation area of the DR Series system GUI, and then, in the Action Menu in the upper right corner, click **Add Container**.



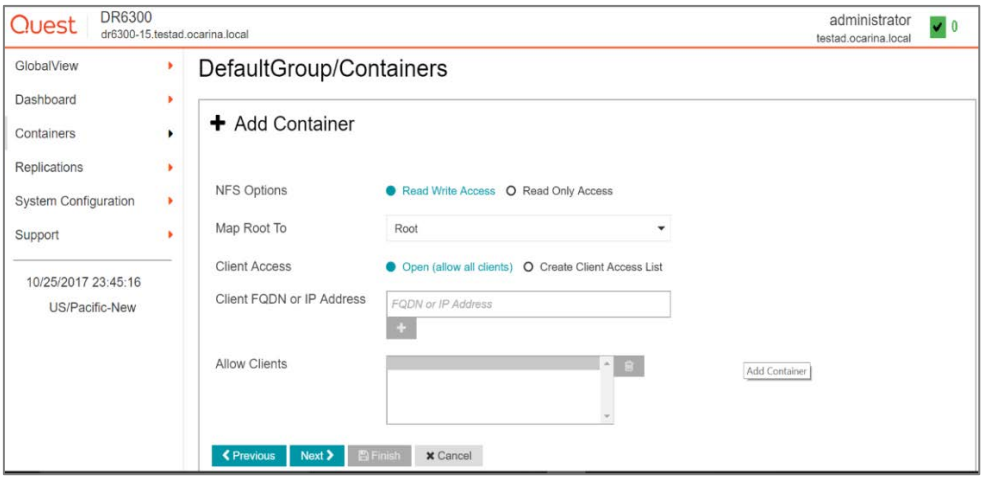
11 Enter a Container Name, select **NAS (NFS, CIFS)** for the Access Protocol, and then click **Next**.



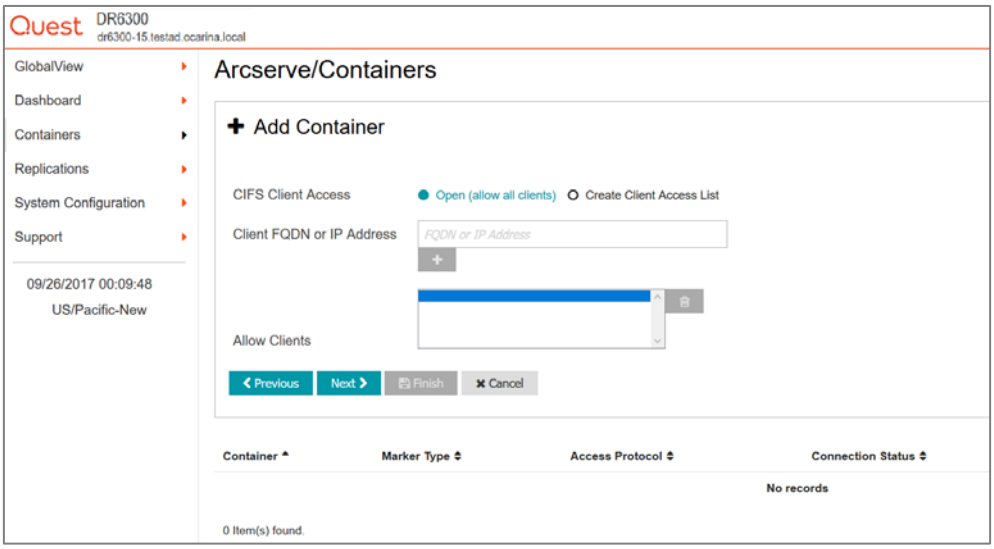
12 Select the **NFS** and **CIFS** check mark for access to the container, as appropriate, and then select **Time Navigator** for the Marker type. Click **Next**.



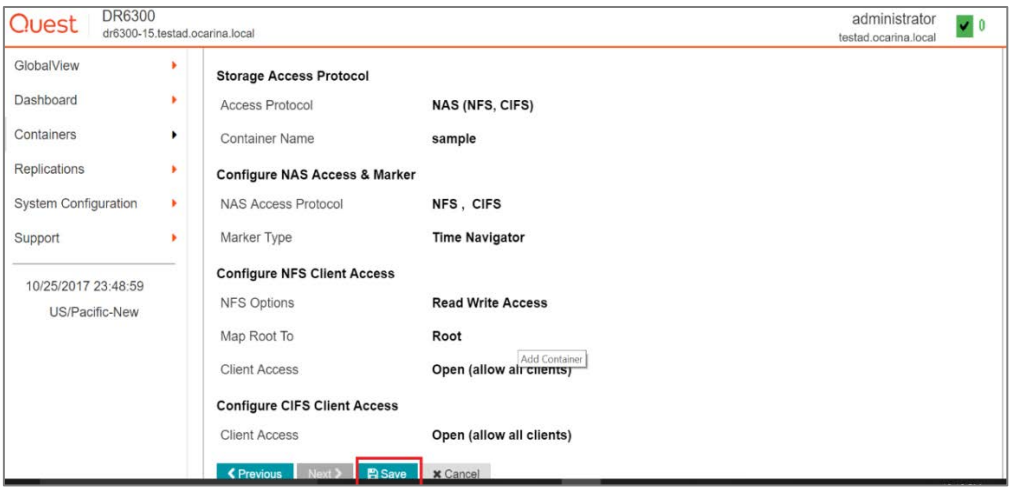
13 For NFS: Enter the required access control list details and click **Next**.



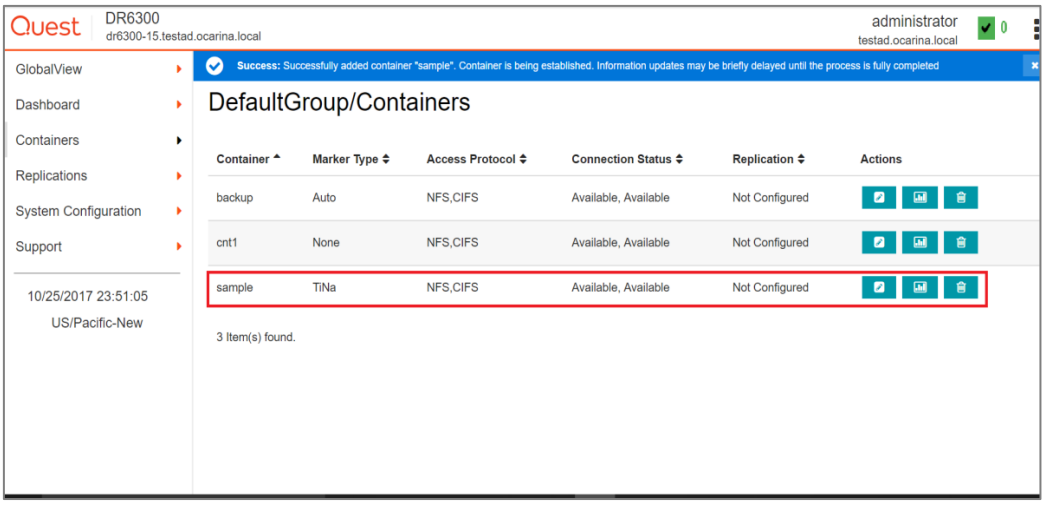
14 For CIFS, enter the required access control list details and click **Next**.



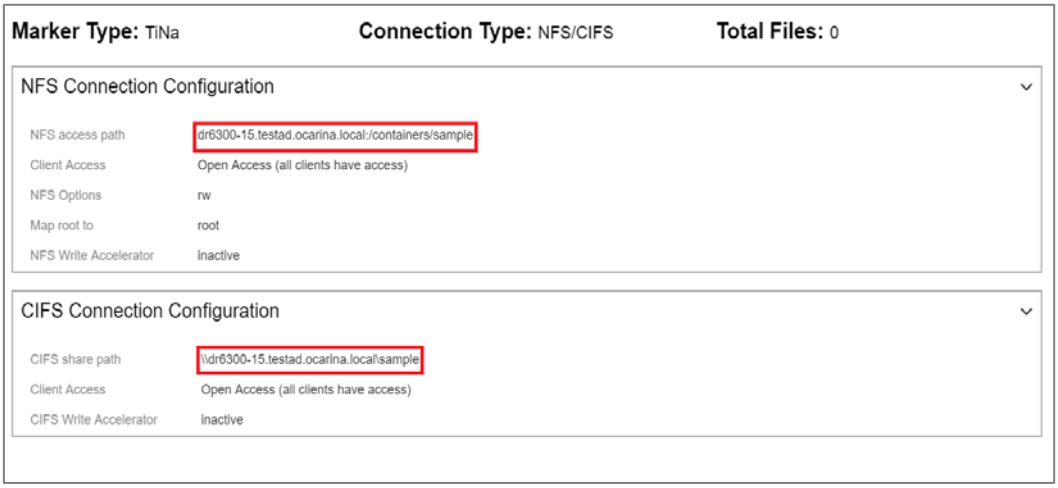
15 Confirm the settings and click **Save**.



16 Verify that the container is created.



17 Select the container that you just created, and click the Graphs icon. Note the container share/export path, which you will use later to target the DR Series system.



NOTE: For improved security, Quest recommends adding IP addresses for the Backup console (ASG-Time Navigator). Not all environments will have all components.

Configuring a backup job on ASG-Time Navigator for a CIFS target

This procedure describes how to initiate and configure a backup job using ASG-Time Navigator with the DR Series system. The high level steps are as follows:

1 Configure CIFS container as a TiNa-library (i.e., backup device).

2 Create a media pool and attach the TiNa library to this media pool.

3 Configure the TiNa backup strategy.

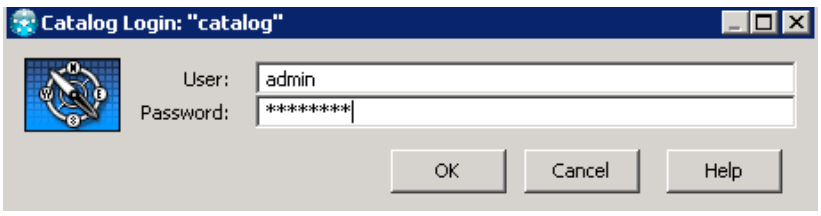
4 Select source data and start a backup job.

1
2

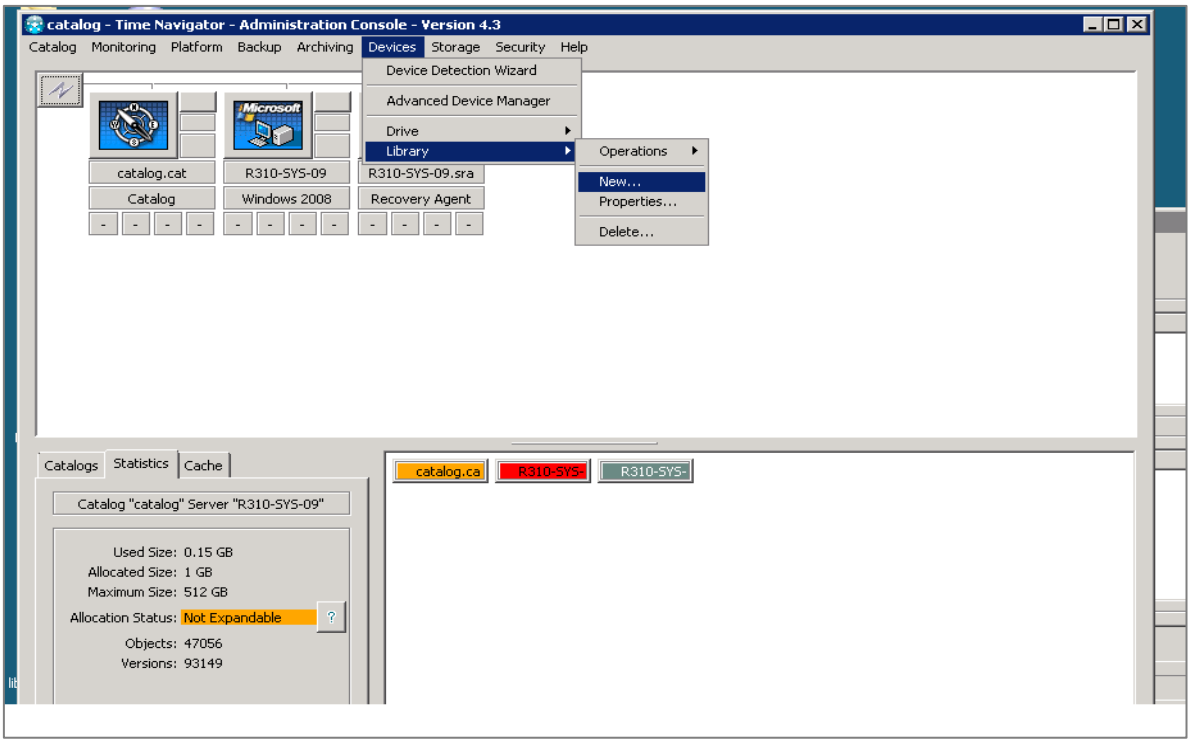
Configuring a CIFS container as a TiNa-library

1 Open the Time Navigator Administration Console by going to **Start** > **All Programs** > **TimeNavigator** > **Administration**. Configure the CIFS container as a TiNa-library (backup device) in the form of a virtual library system.

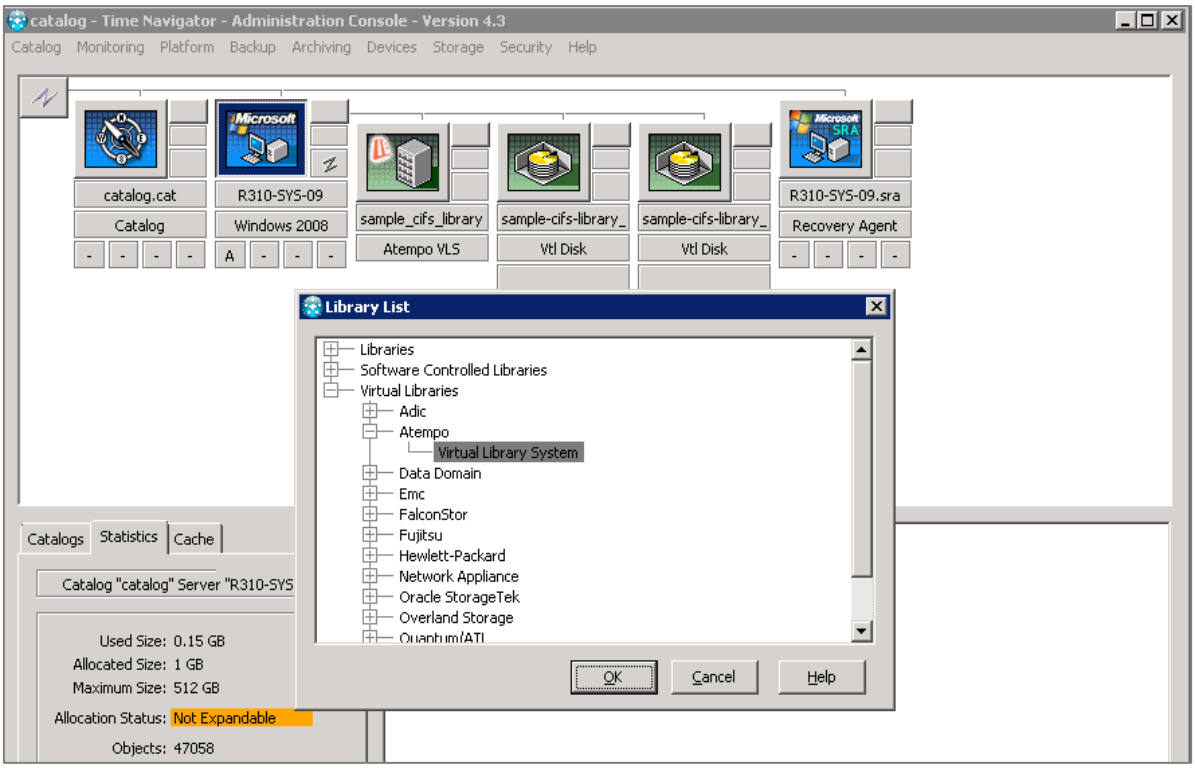
2 Log on to catalog.



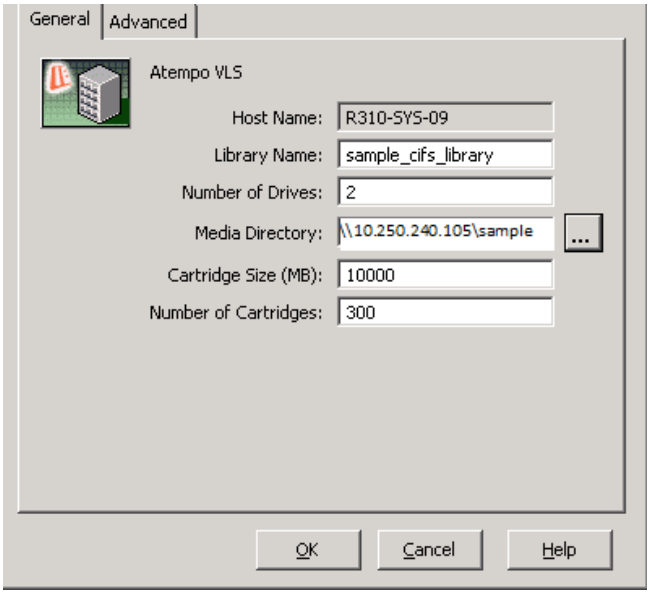
3 Go to **Devices > Library > New**.



4 Select **Virtual Libraries**, and expand the Atempo section. Click **Virtual Library System**.



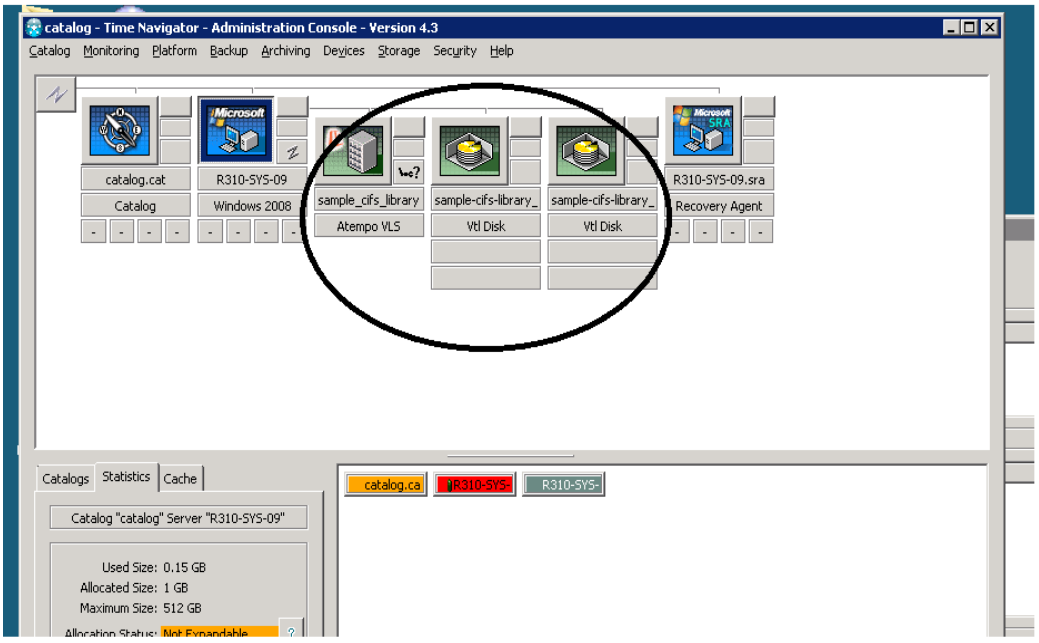
5 Enter a library name (for example, sample_cifs_library) in the New Atempo VLS screen and provide the CIFS share path in the **Media Directory** field. Click **OK**.



6 Confirm the library has been properly created in catalog.

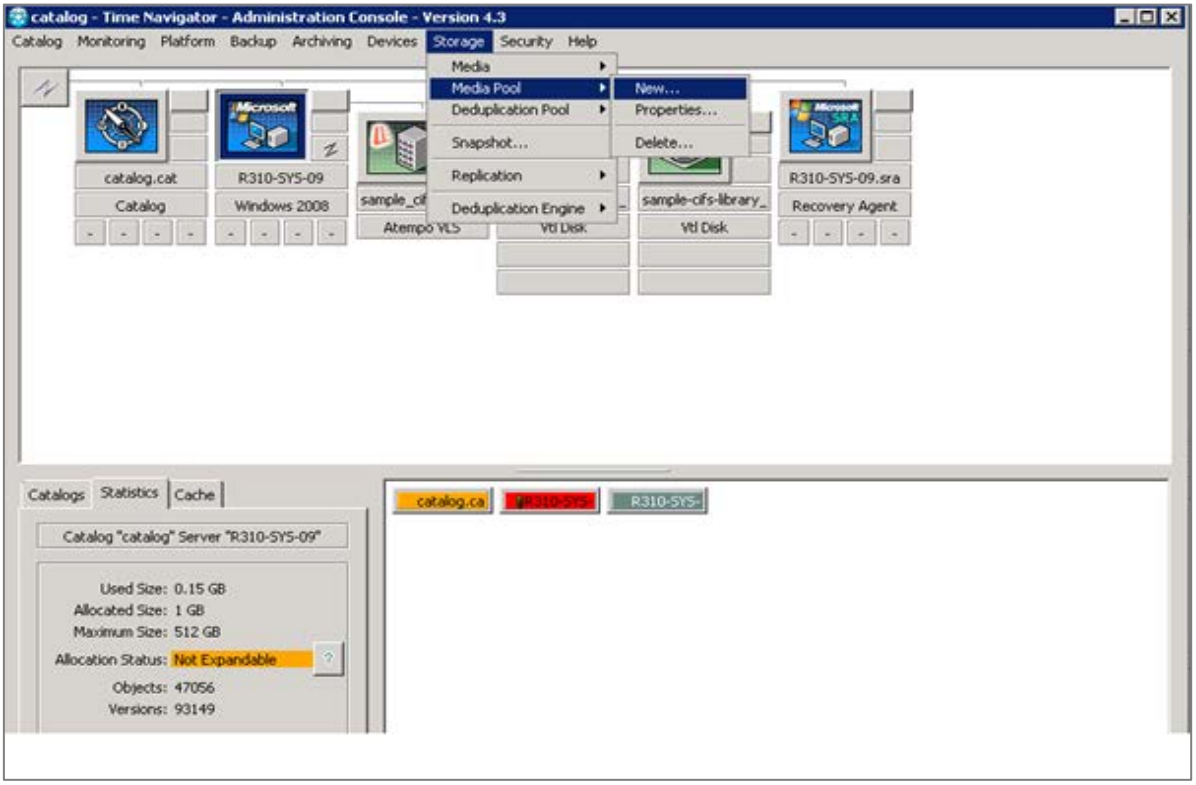
NOTE: TiNa backup services should run as the user with domain administrator or administrator write permissions on the DR Series system.

NOTE: Refer to Appendix A for recommendations on the number of cartridges and size for disk-based dedupe appliances.

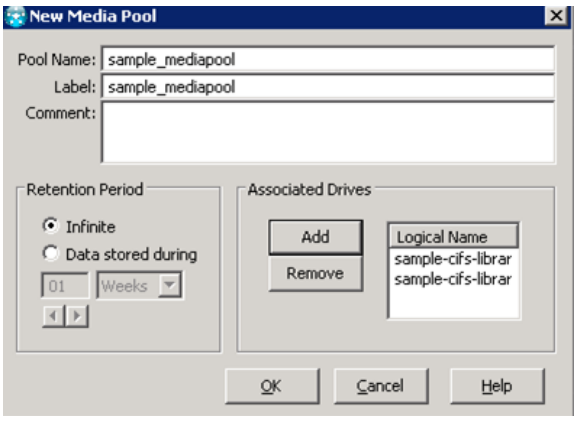


Creating a media pool and attaching the TiNa library

1 On the Storage menu, click **Media Pool** and then click New.

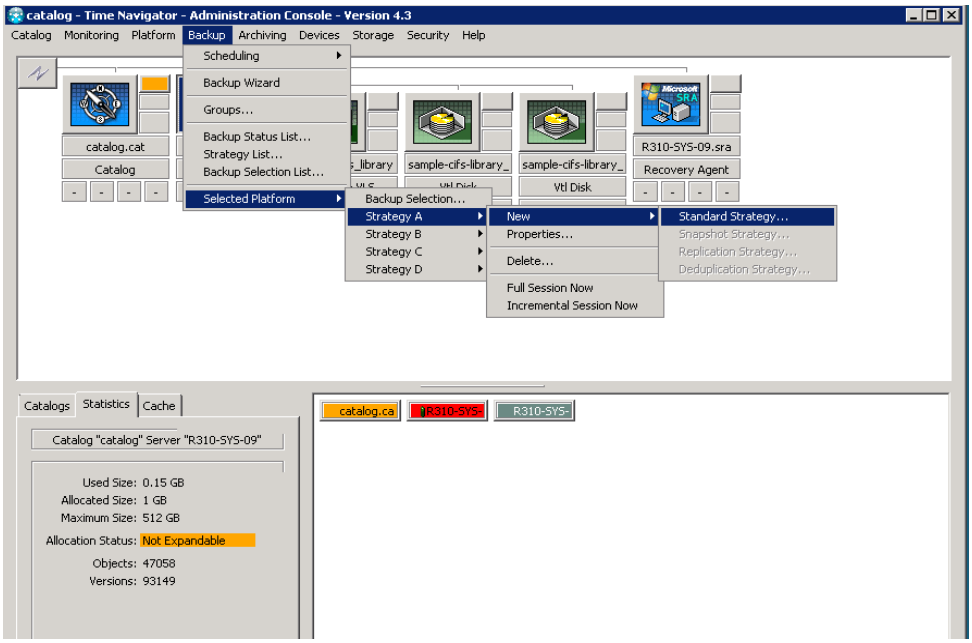


2 Enter a Pool Name and Label, and click **Add**. Select the available **Drives** in the list by clicking **OK**.

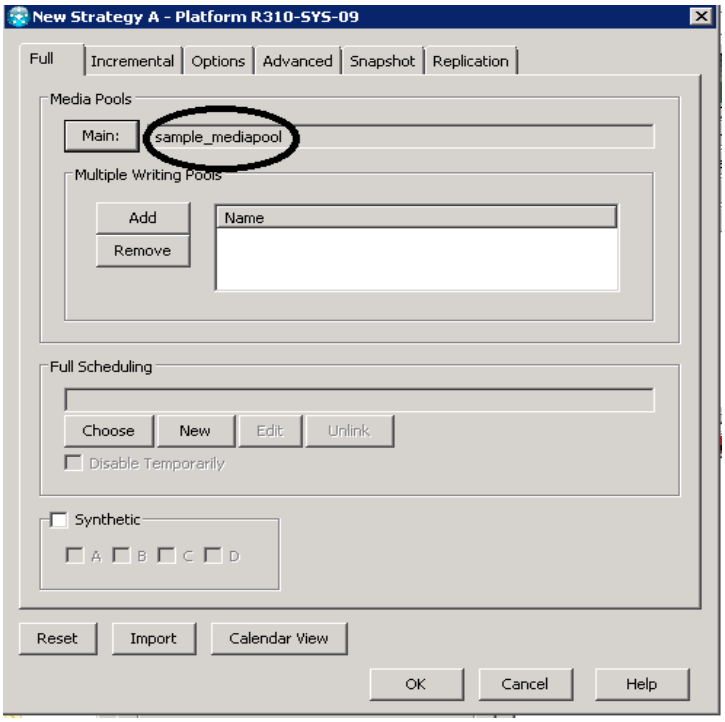


Configuring the TiNa backup strategy

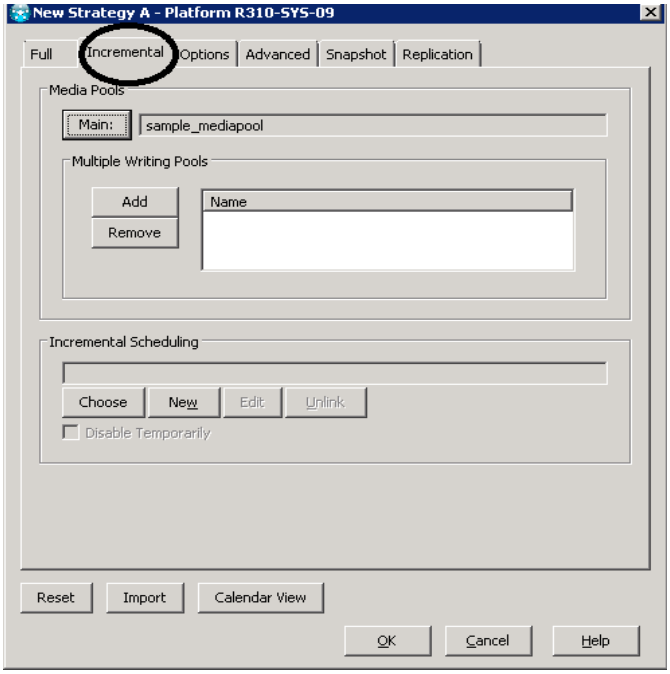
1 Click the **Backup menu** and then select Platform Selection. Select the **Strategy** (for example, **Strategy A**), click **New**, and then click **Standard Strategy**.



2 Click the **Main** button under Media Pools. Select the pool name, and click **OK**.

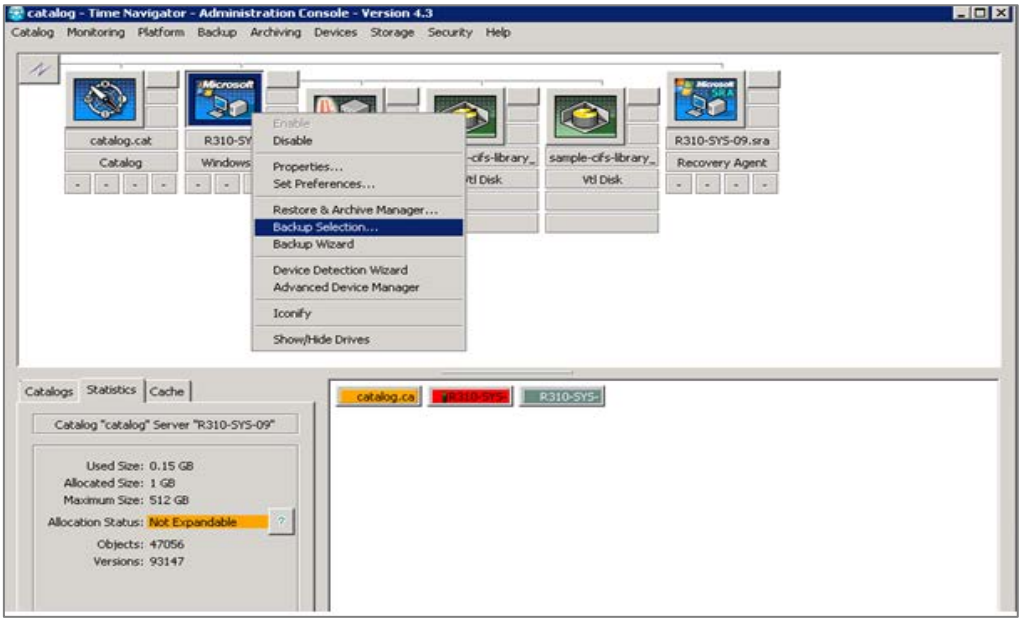


3 Similarly, add it for **incremental** backup. Without this Incremental media Pool, Time Navigator will not accept to take the full backup.

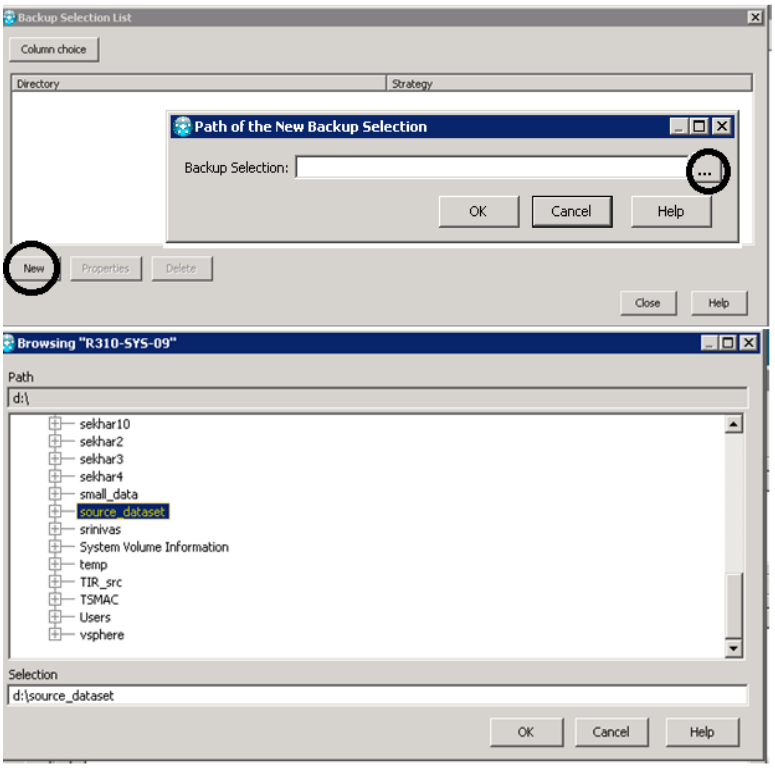


Selecting source data and starting a CIFS backup

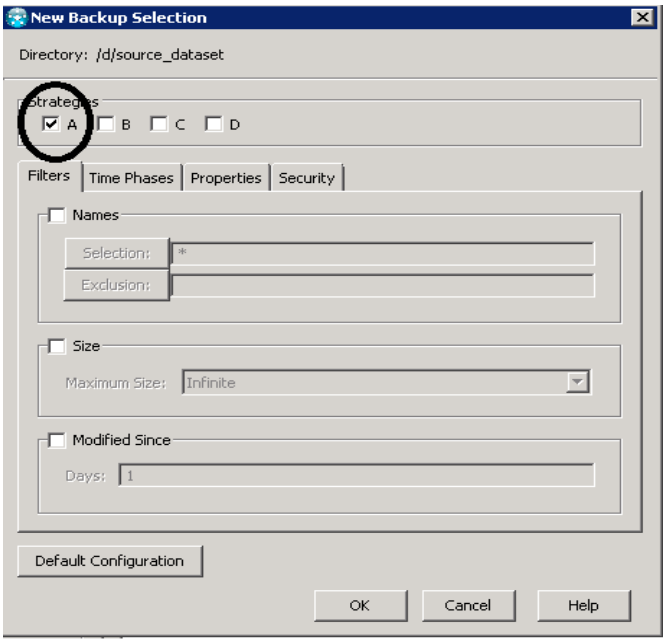
1 Right-click the Time Navigator backup server host icon and click **Backup Selection**.



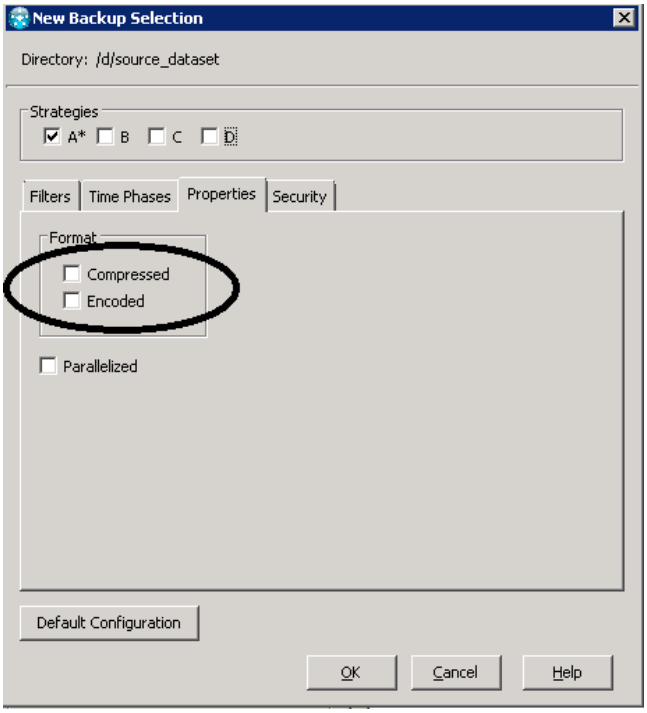
2 Click **New**, and then browse to the path of the data to be backed up. Select the directory location and click **OK**.



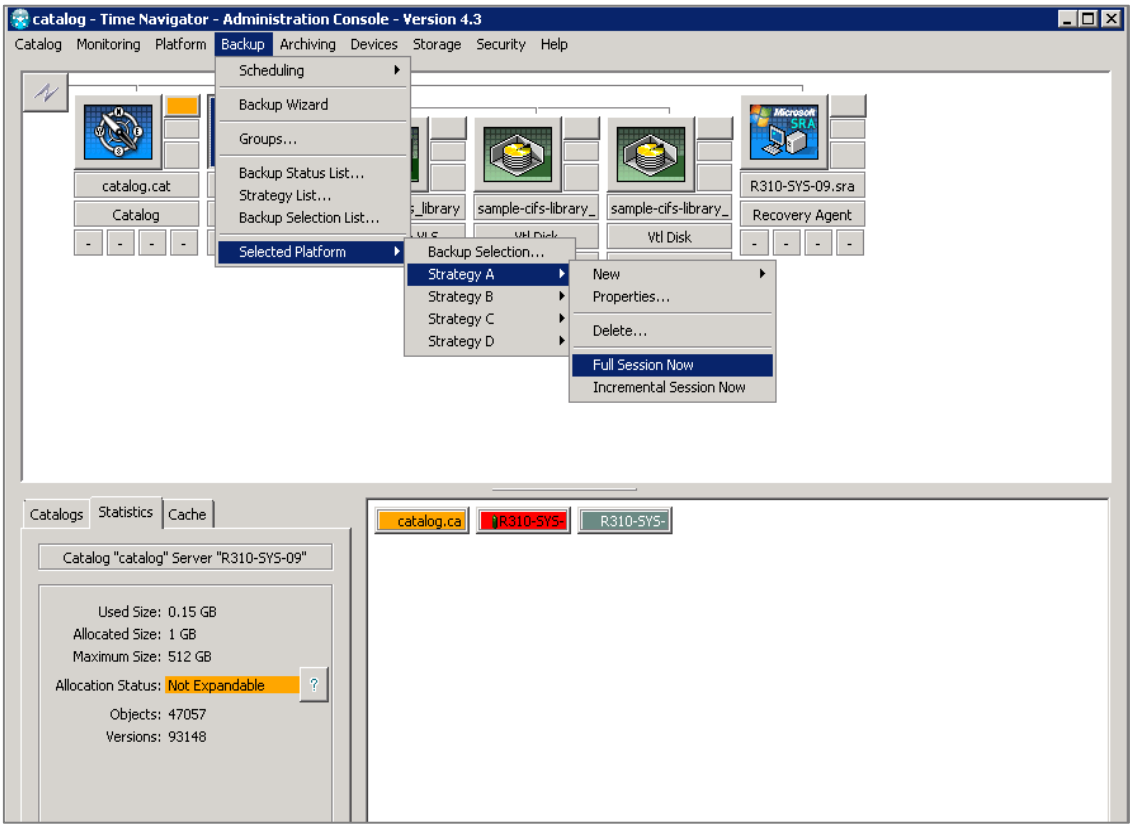
3 Apply a strategy for the new backup selection, and click **OK**.



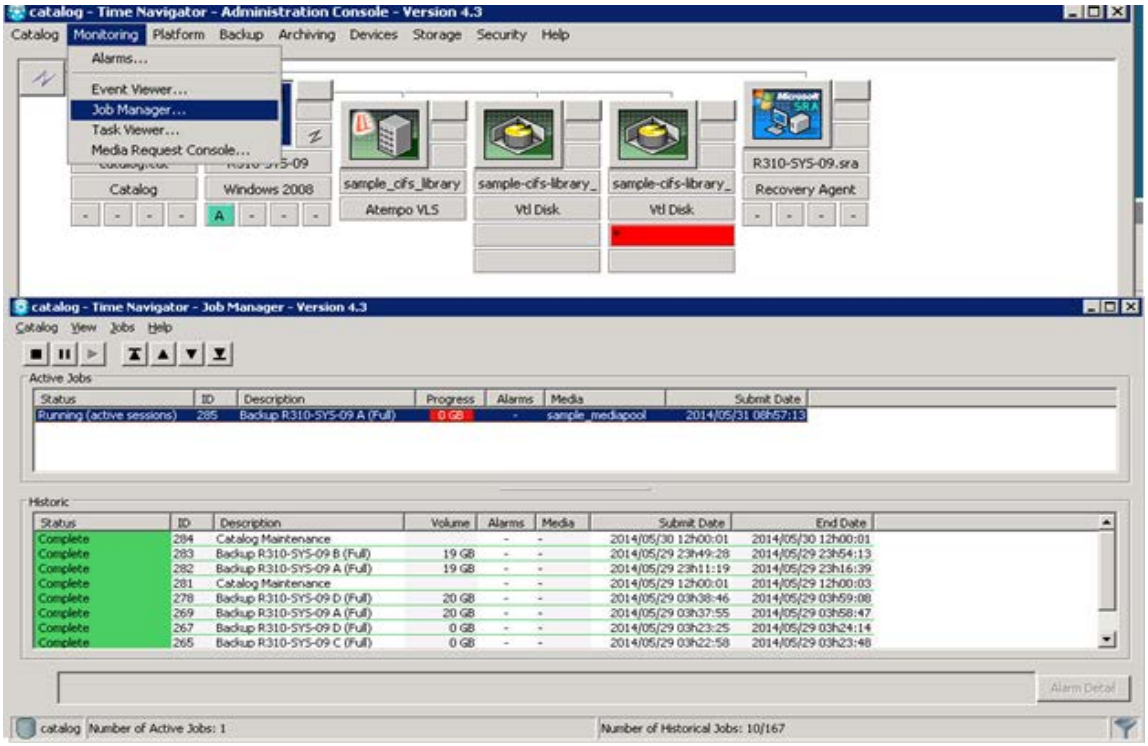
NOTE: Quest recommends that you do **not** enable TiNa's native compression and encryption while doing backup and restore.



4 On the Backup menu, click **Selected Platform > Strategy A > Full Session Now**.

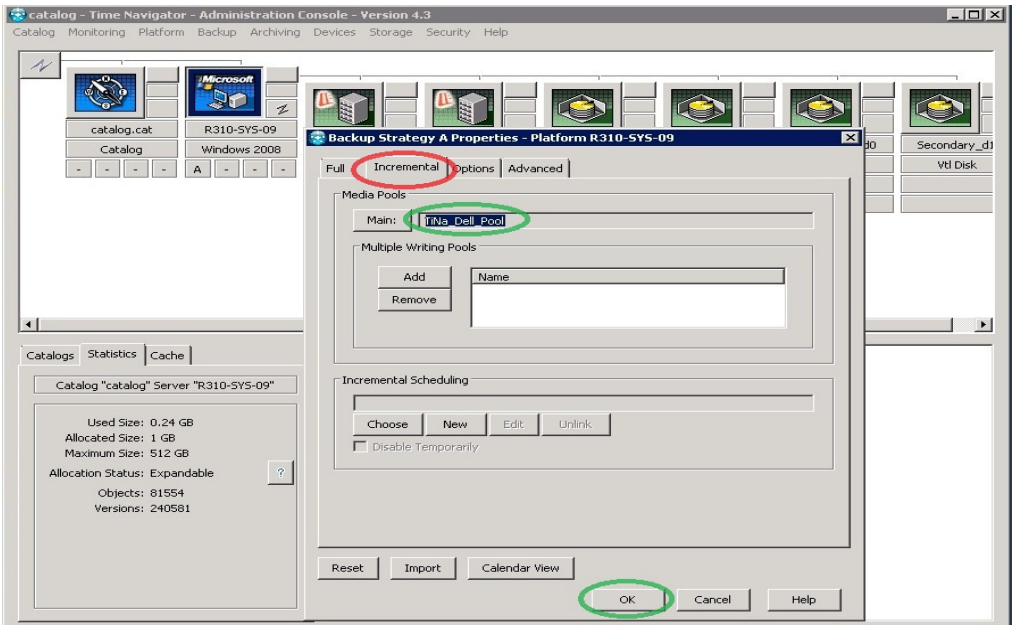


5 Monitor the status of the running job by clicking **Monitoring > Job Manager**.



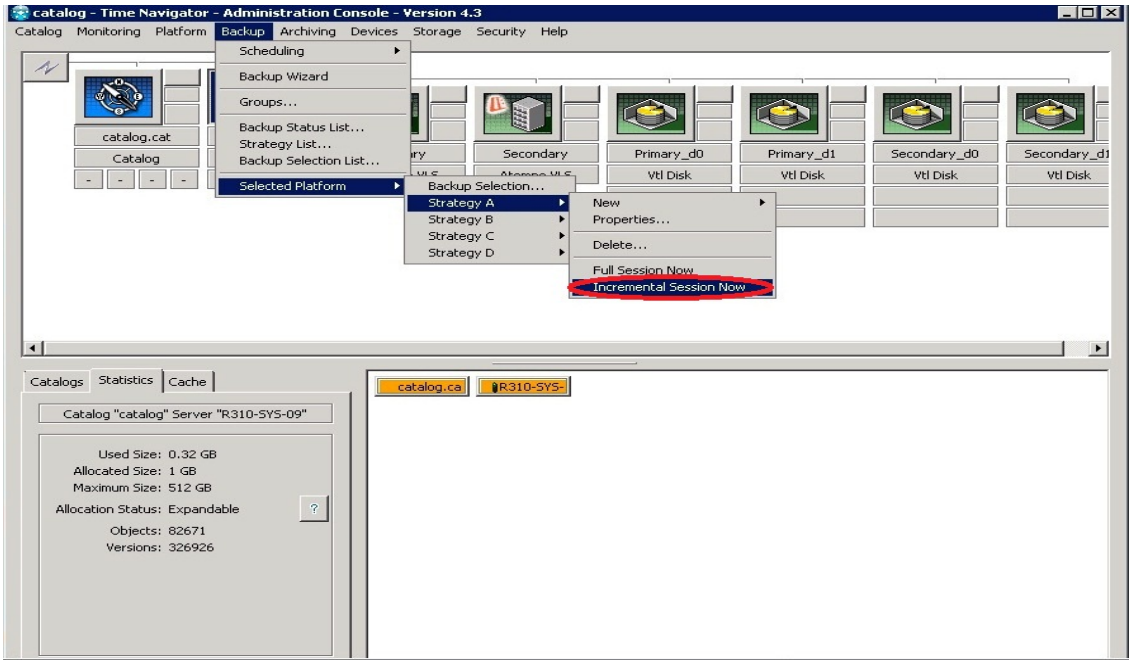
Performing an incremental backup

1 Add the Full backup Media Pool in the **Incremental** tab. Browse the Media pools by clicking **Main**, and then selecting **Full backup Media** Pool in the list.



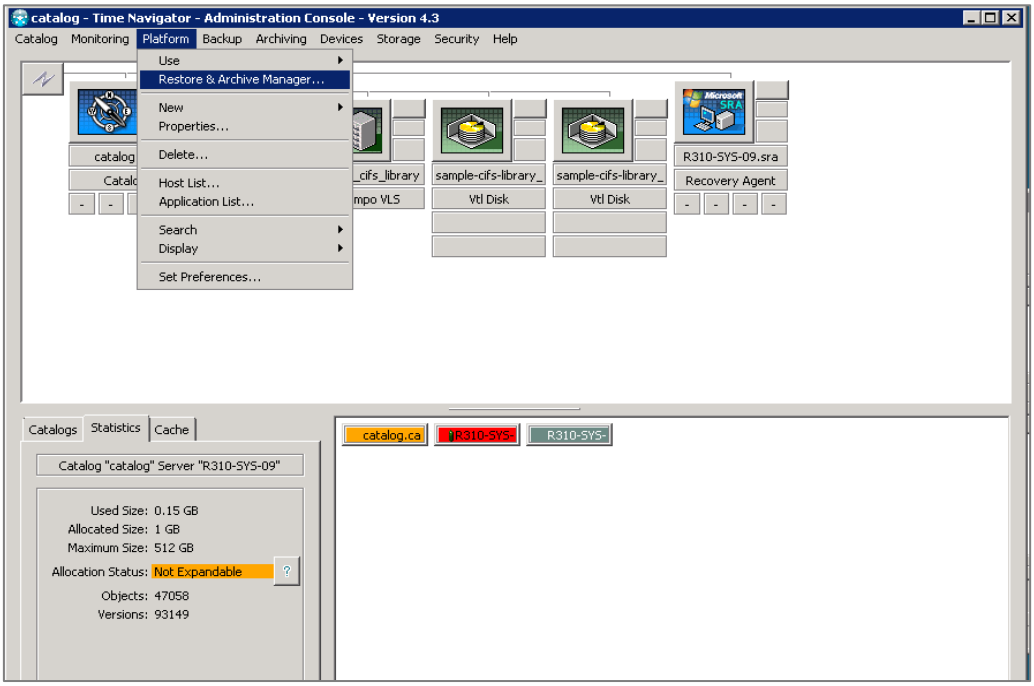
2 Select the full backup strategy by clicking the **Backup > Platform Selection** and then selecting the strategy (for example, **Strategy A**).

3 Click **New > Incremental Session Now**.

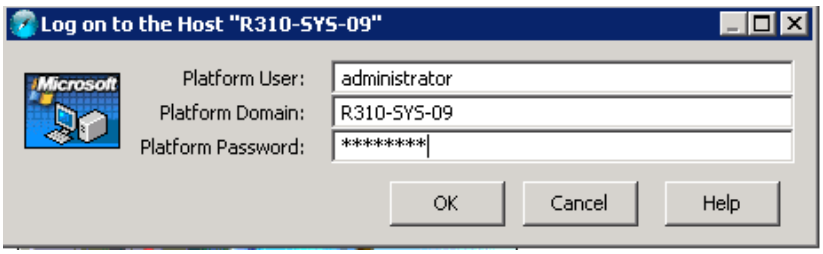


Configuring a restore job on ASG-Time Navigator over a CIFS target

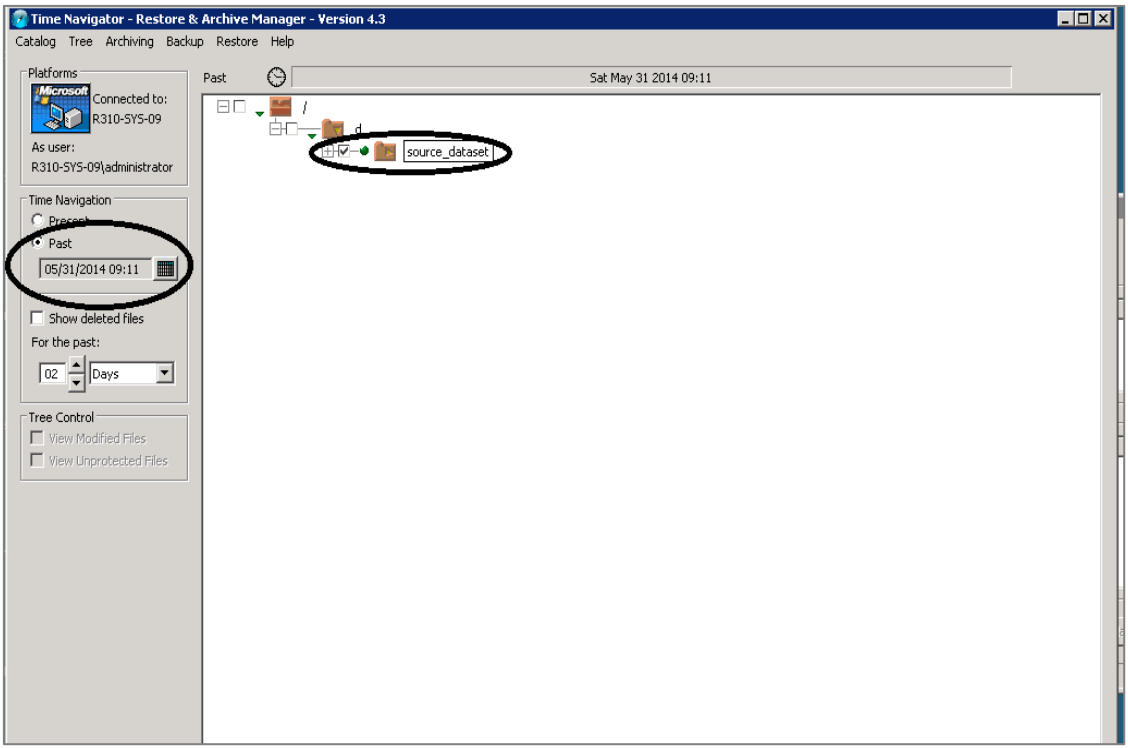
1 When a backup job completes, select the Windows Time Navigator host, and configure the Restore operation by selecting **Platform > Restore & Archive Manager**.



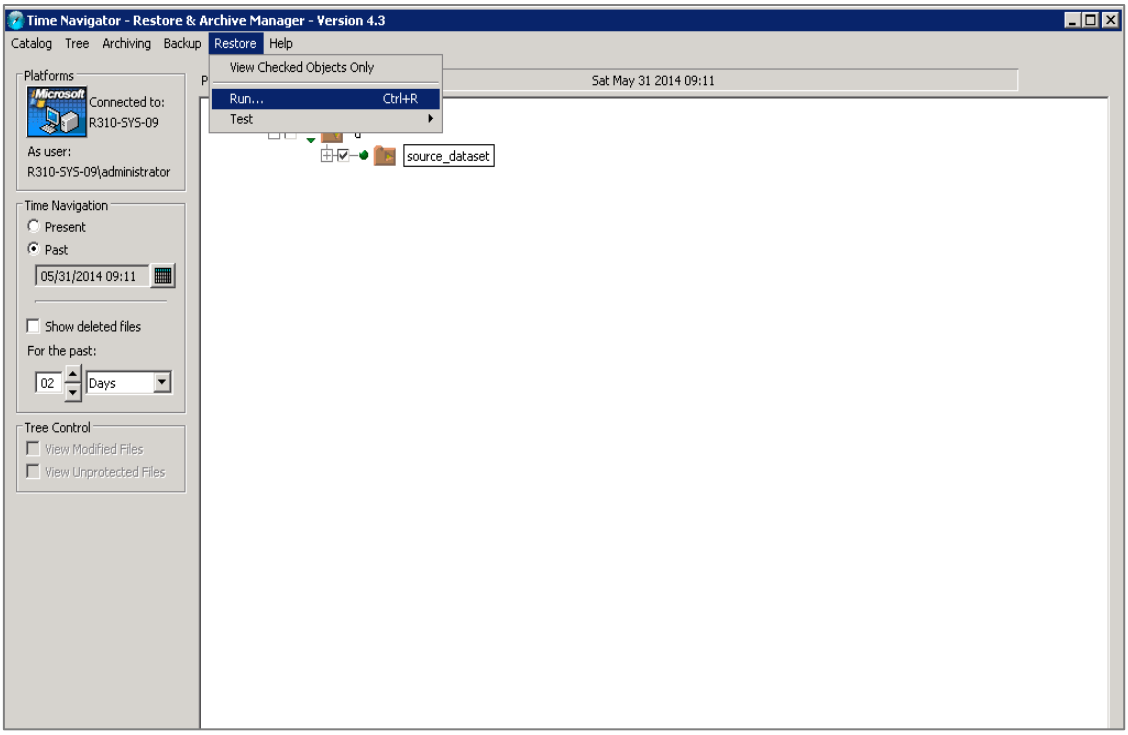
2 Enter the credentials of the Host for the Restore Job configuration and click **OK**.



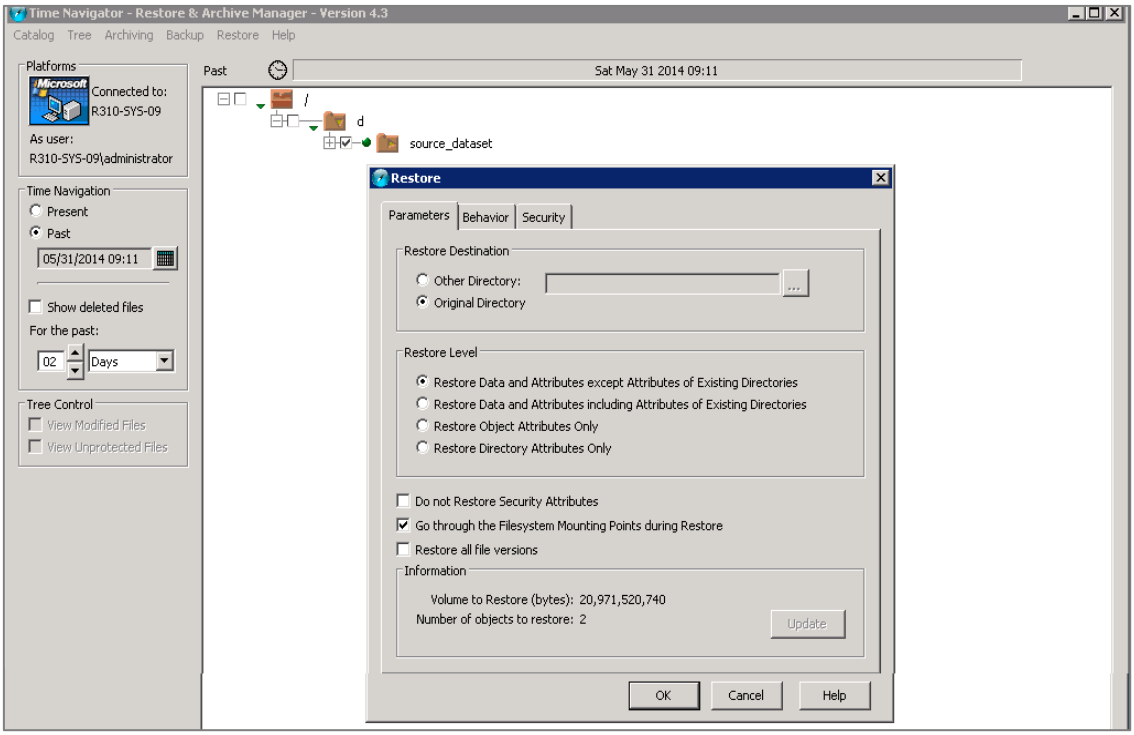
3 Browse to and select the objects to be restored.



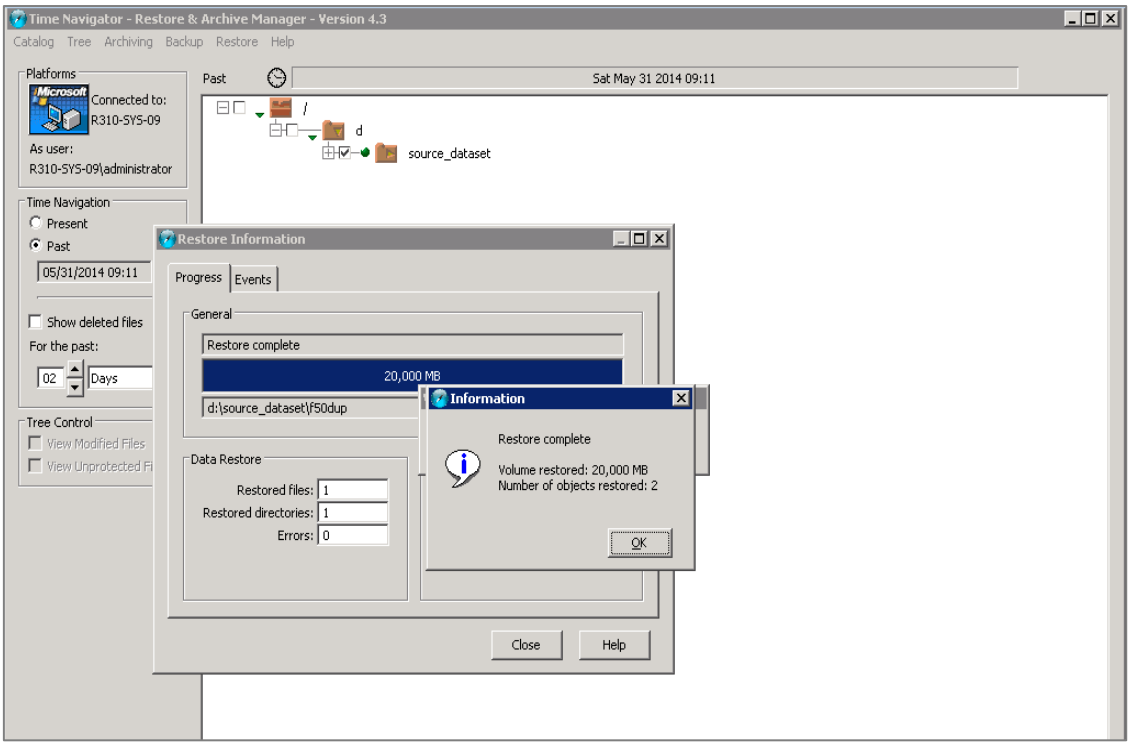
4 On the **Restore** menu, click **Run**.



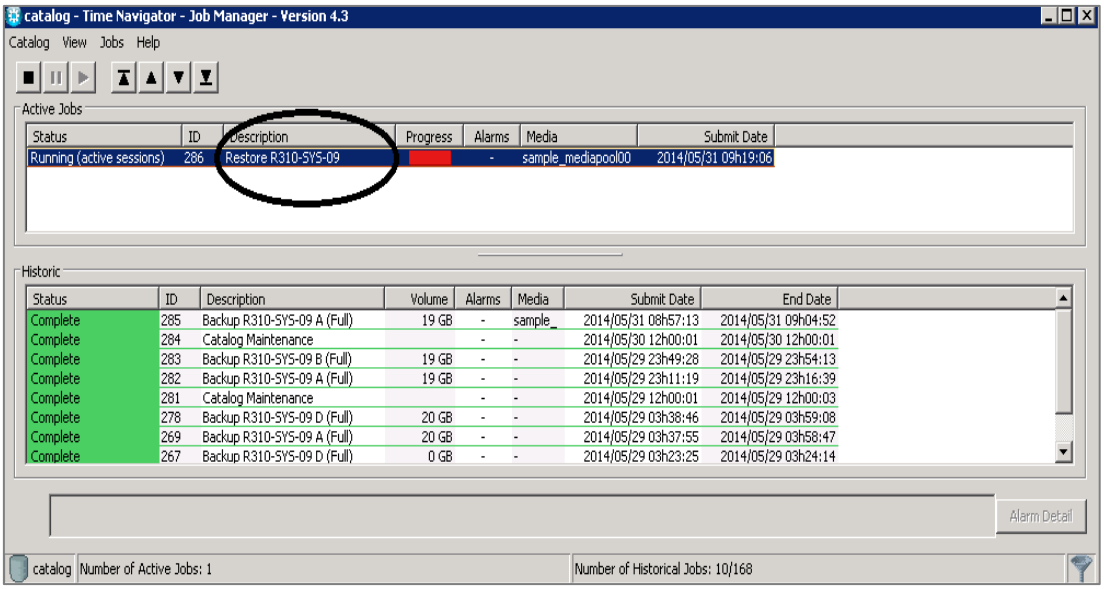
5 Select one of the Restore Destinations and click **OK**.



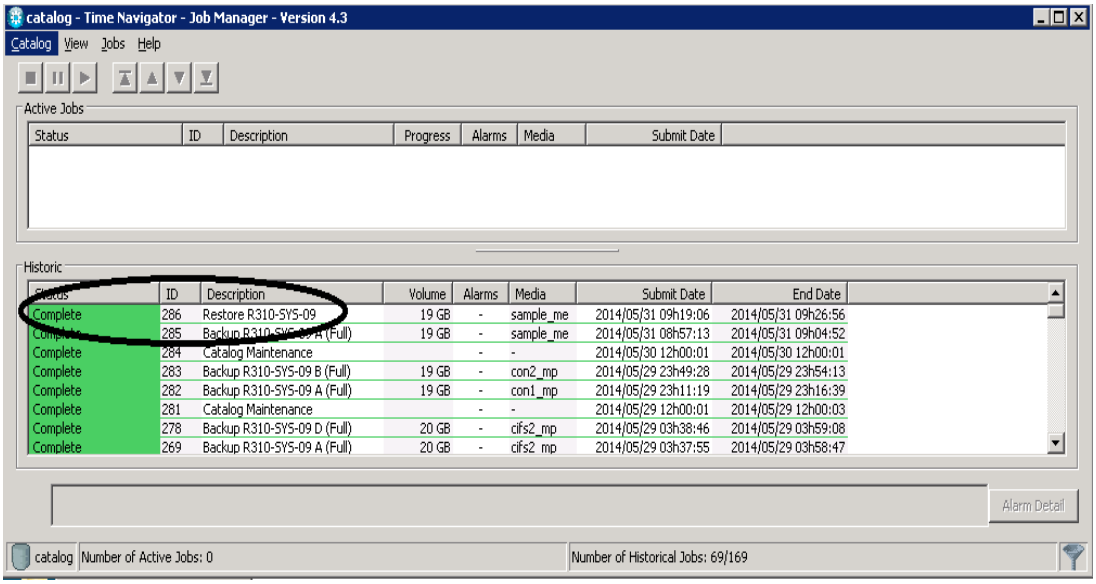
The Restore Information window shows the restore progression to its completion.



6 Monitor the restore job status by clicking **Monitoring > Job Manager**.

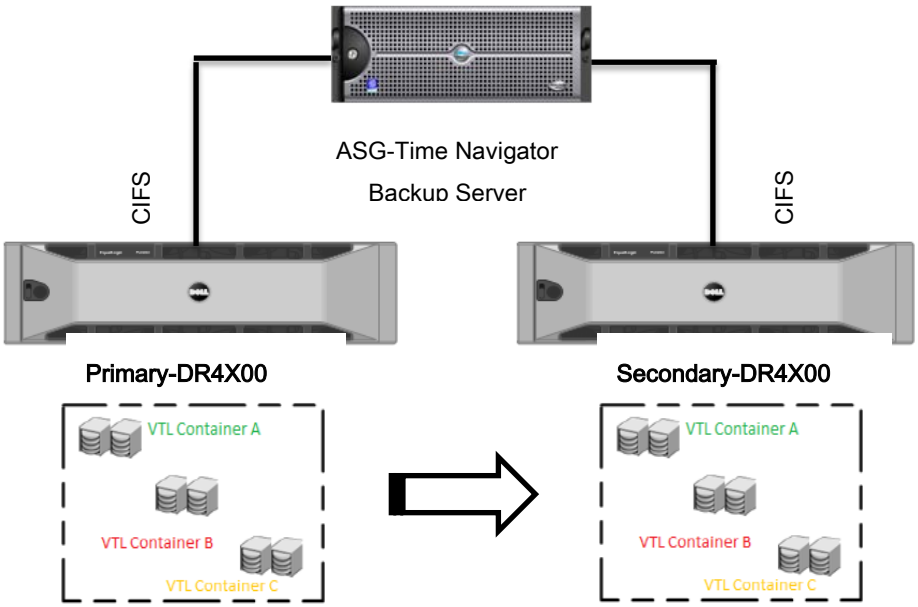


When the Restore job completes, it appears in the Job Manager.



Running a duplication and restore job on a secondary CIFS target

For certain Disaster Recovery scenarios, a duplicate copy of a backup data set from a primary DR Series system can be made available on a secondary DR Series system.



Follow these instructions to create a duplicate copy of a backup.

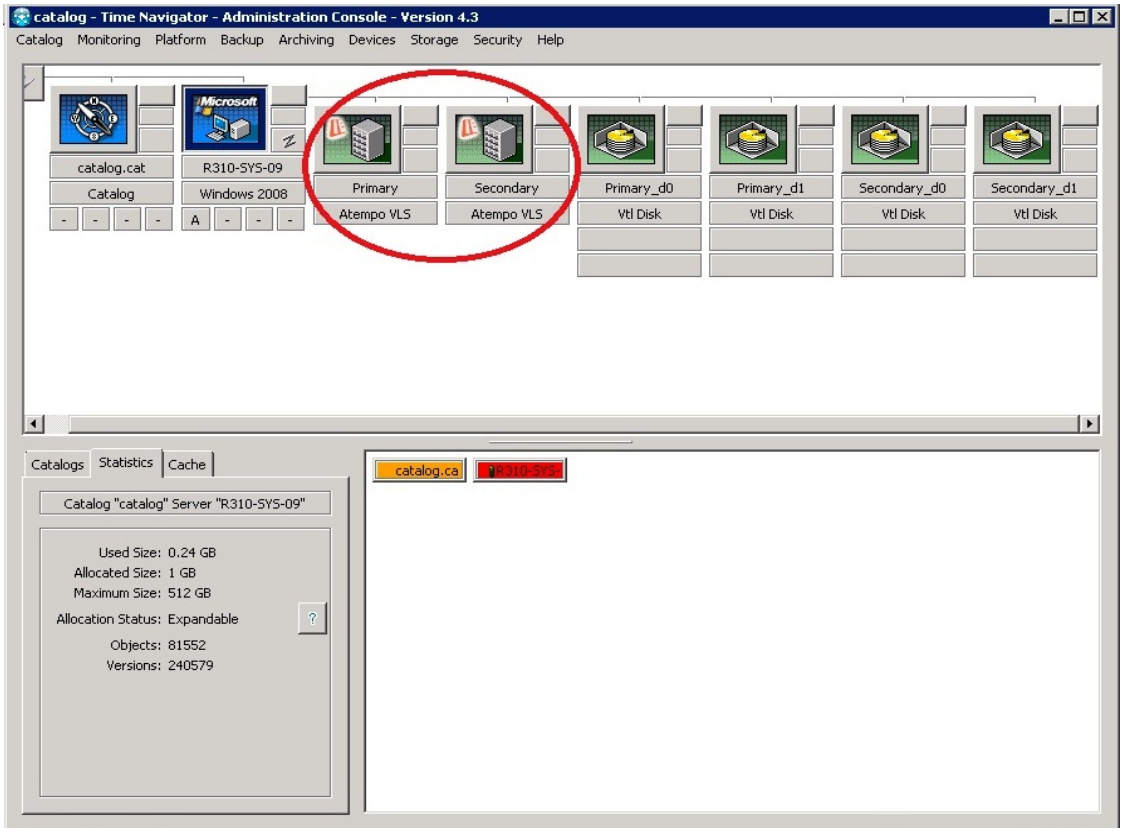
1 On the primary DR Series system, create a CIFS container.

```
login as: administrator
administrator@10.250.242.139's password:
Last login: Sat Jun  7 12:00:42 2014 from 10.16.230.222
Total alert messages            : 2
Run `alerts --show --alerts` to see the alerts.
administrator@swsys-69 > container --add --name primarycontainer
Container "primarycontainer" created successfully.
administrator@swsys-69 > connection --add --type cifs --name primarycontainer
Successfully added connection entry.
CIFS connection IP addresses    : *
CIFS connection Enabled         : Yes
administrator@swsys-69 > container --marker --enable tina --name primarycontaine
r
Successfully enabled container "primarycontainer" with the following marker(s) "
TiNa".
administrator@swsys-69 >
```

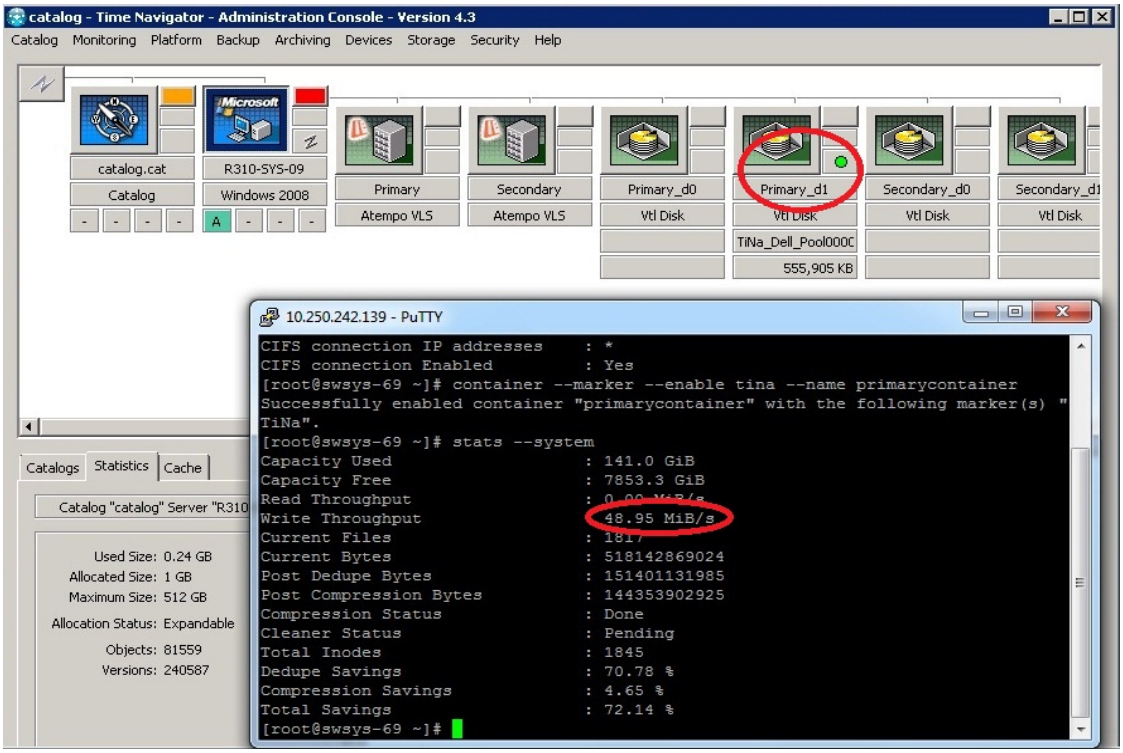
2 On the secondary DR Series system, create a CIFS container.

```
administrator@swsys-73 > container --add --name secondarycontainer
Container "secondarycontainer" created successfully.
administrator@swsys-73 > connection --add --type cifs --name secondarycontainer
Successfully added connection entry.
CIFS connection IP addresses    : *
CIFS connection Enabled         : Yes
administrator@swsys-73 > container --marker --enable tina --name secondarycontainer
Successfully enabled container "secondarycontainer" with the following marker(s) "TiNa".
administrator@swsys-73 >
```

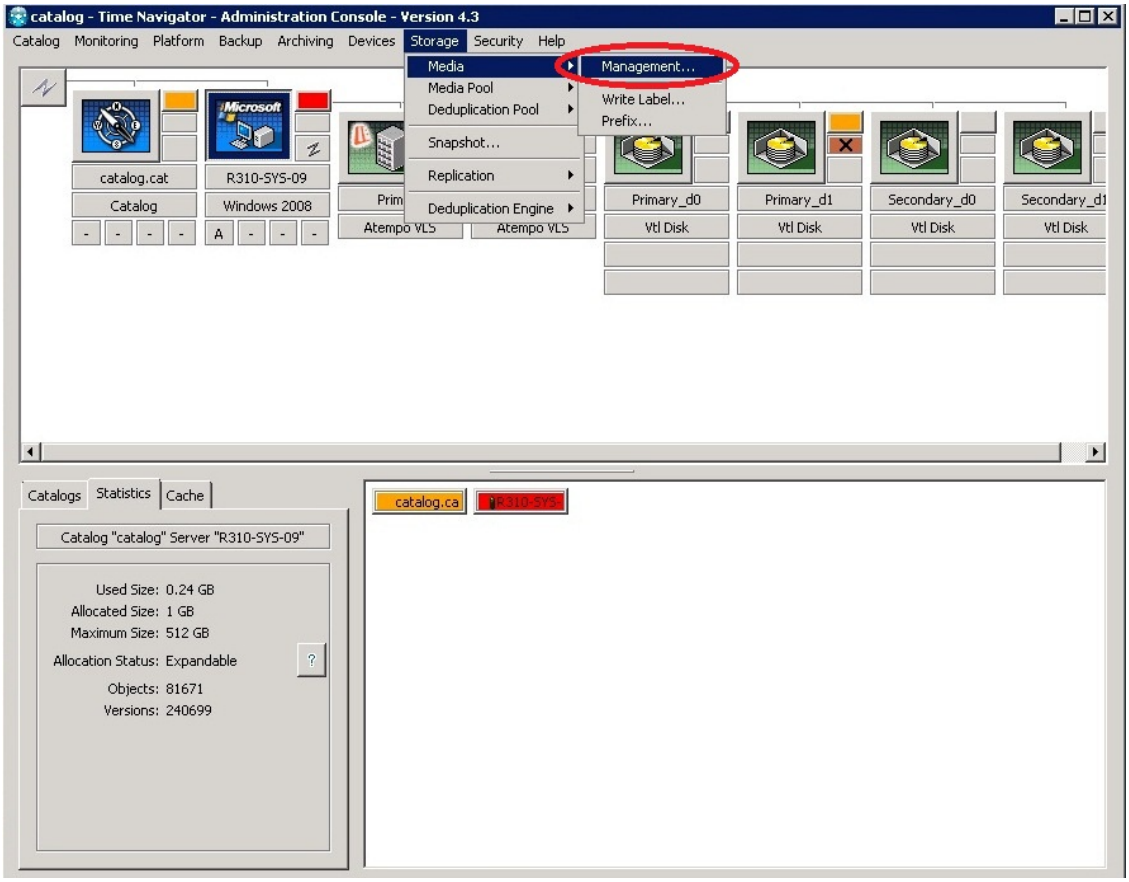
The following figure shows the configured primary and secondary DR containers as Primary-Virtual Library System (VLS) and Secondary-VLS for demonstration of duplication and restore from a secondary DR Series system.



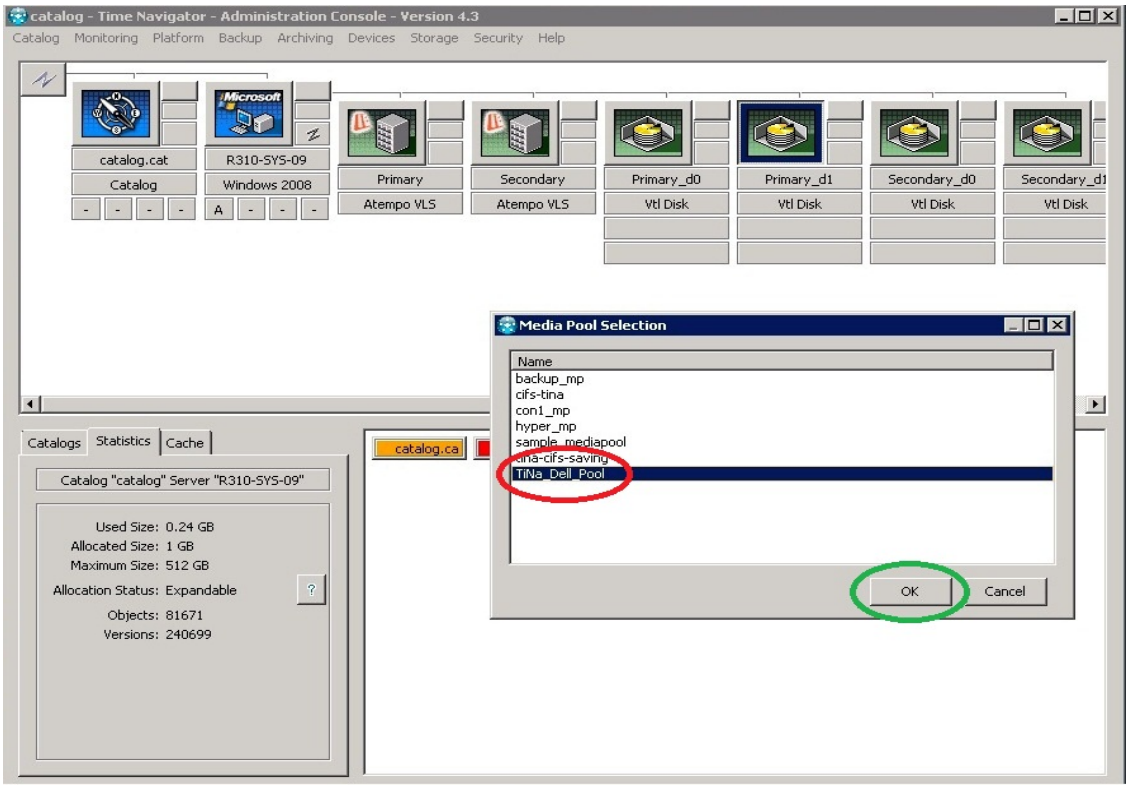
The Backup Job is configured and submitted on the Primary DR Series system.



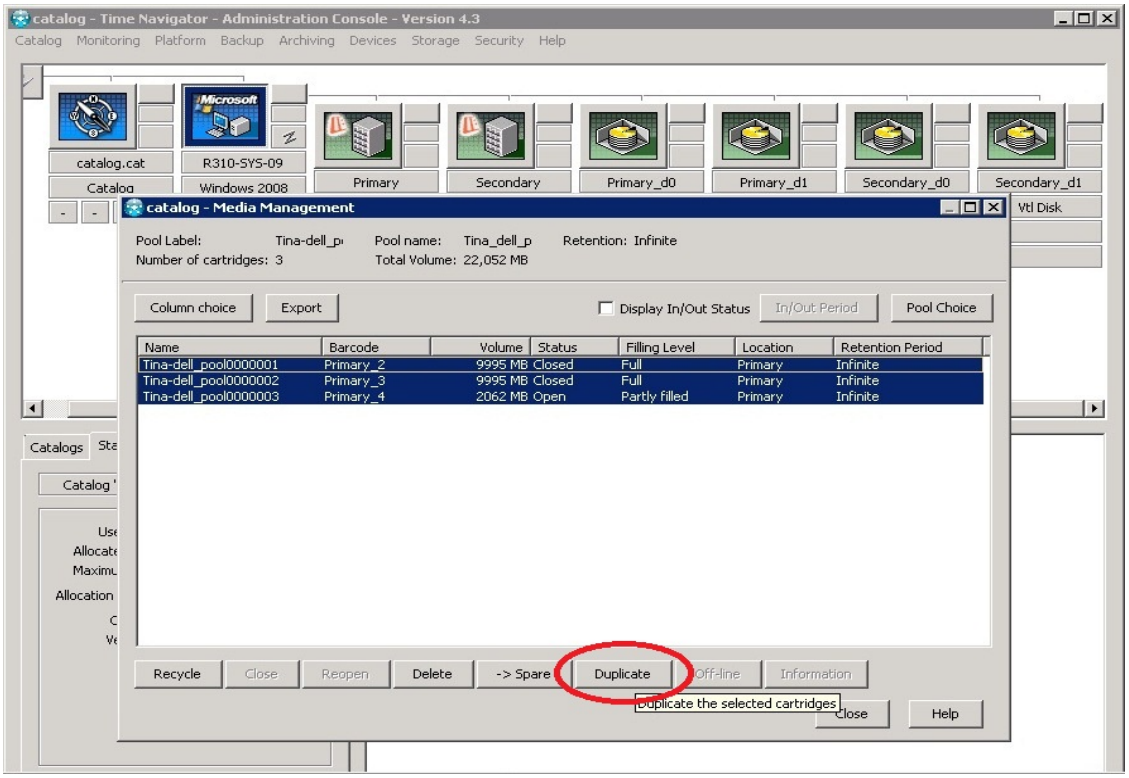
3 For duplication of existing backup data Configuration, when the primary backup job completes, click **Storage > Media > Management**.



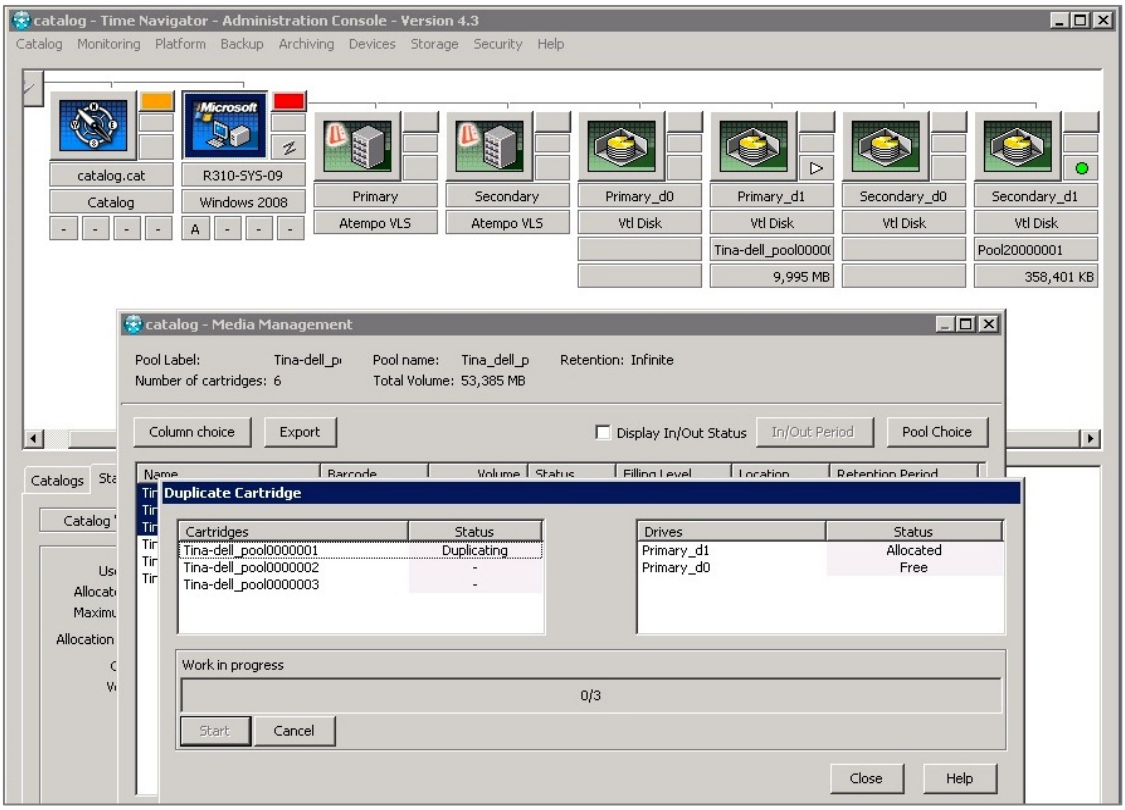
4 Select the **media pool name** on which the secondary logical drives are available and click **OK**.



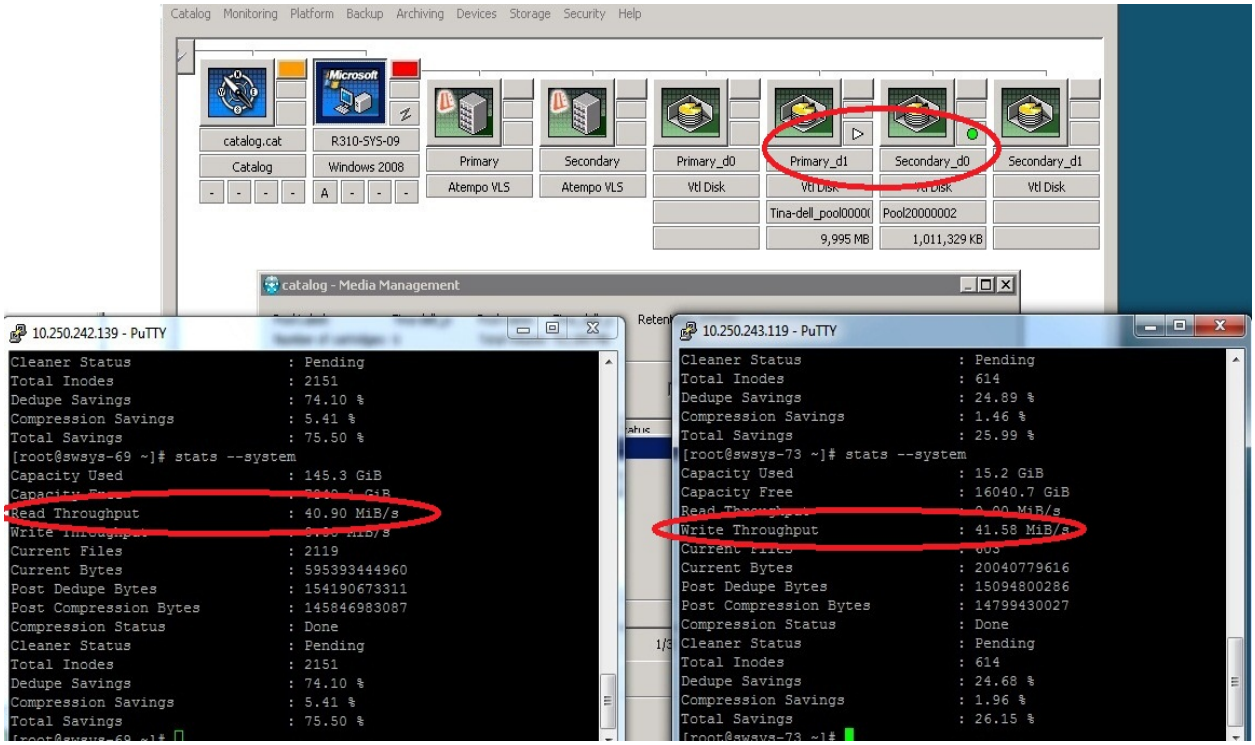
5 Select the Cartridges and click **Duplicate**.



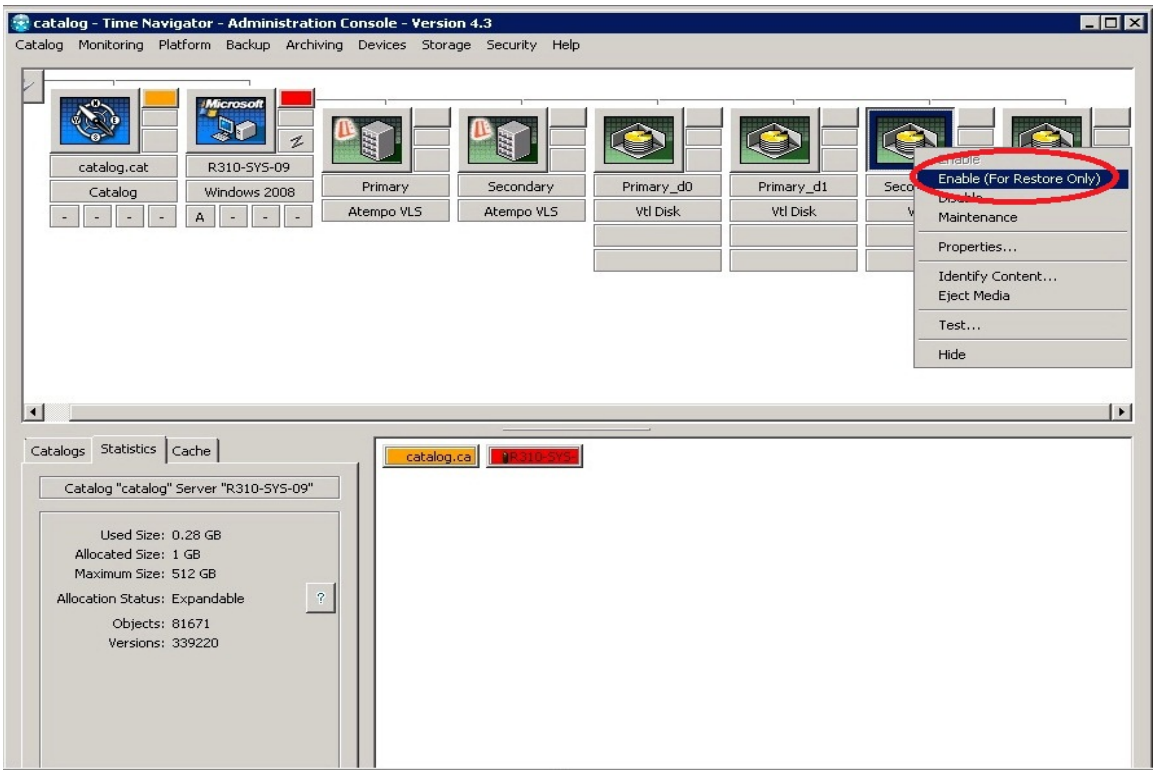
6 Click **Start** to see the duplication in progress.



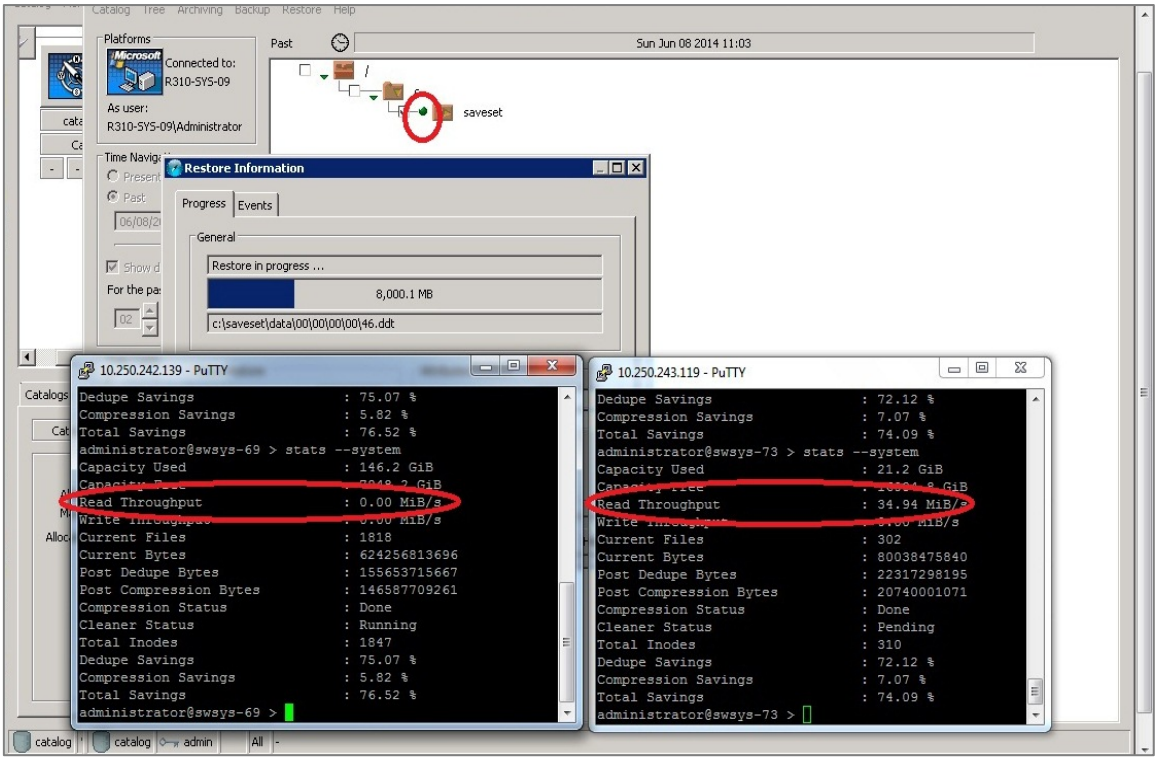
7 Monitor the duplication work in progression on the Primary and Secondary DR Series systems.



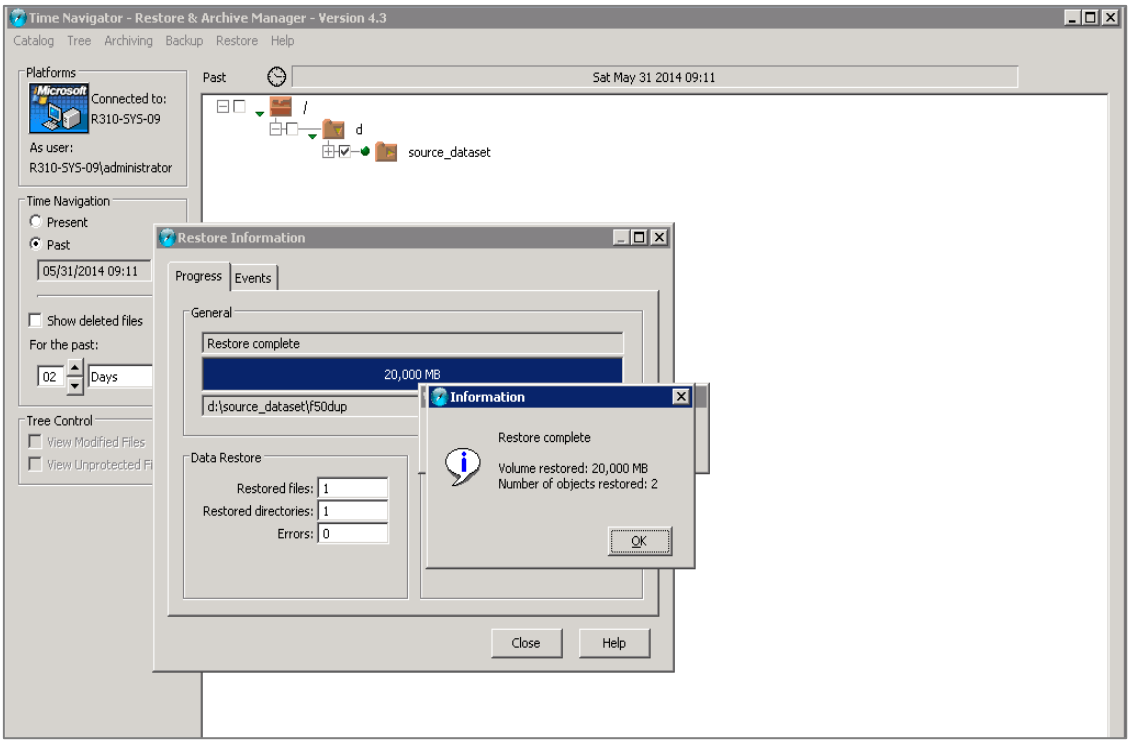
8 Right-click the secondary logical drive and click **Enable (For Restore Only).**



9 Monitor the Restore progress on the secondary system.



10 Wait for the restore to complete from the secondary container to client.



Configuring a backup job on ASG-Time Navigator over an NFS target

The procedure described in this section provides the steps to initiate and configure a backup job using ASG-Time Navigator with the DR Series system. The high level steps are:

1 Configure an NFS container as a TiNa-library (that is, a backup device).

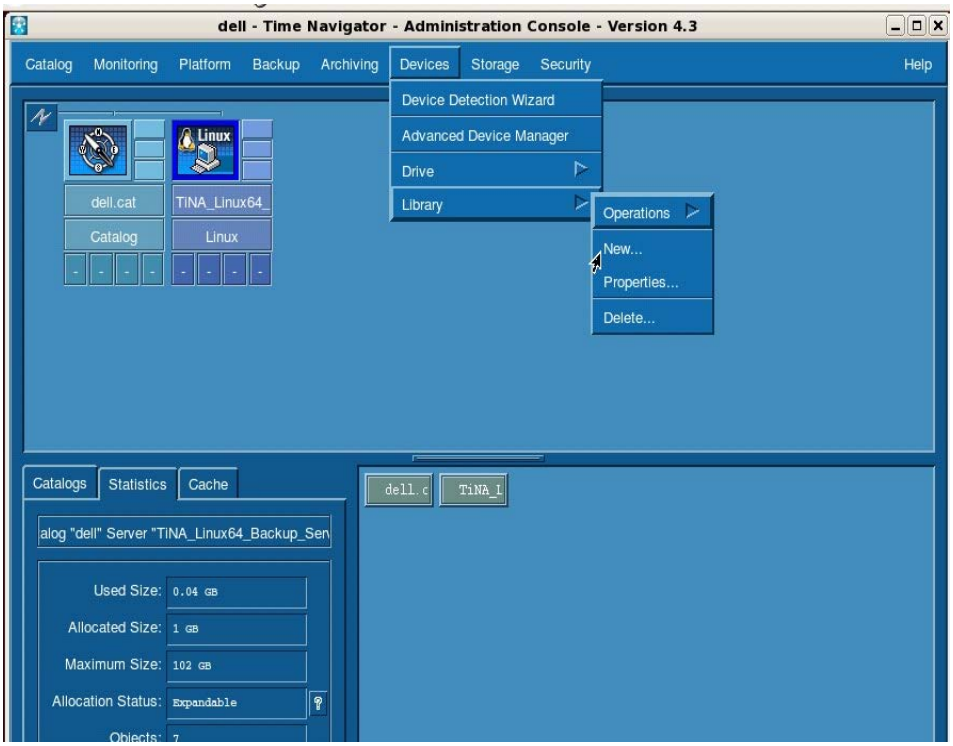
2 Create a media pool and attach TiNa logical drives to this media pool.

3 Configure a TiNa backup strategy.

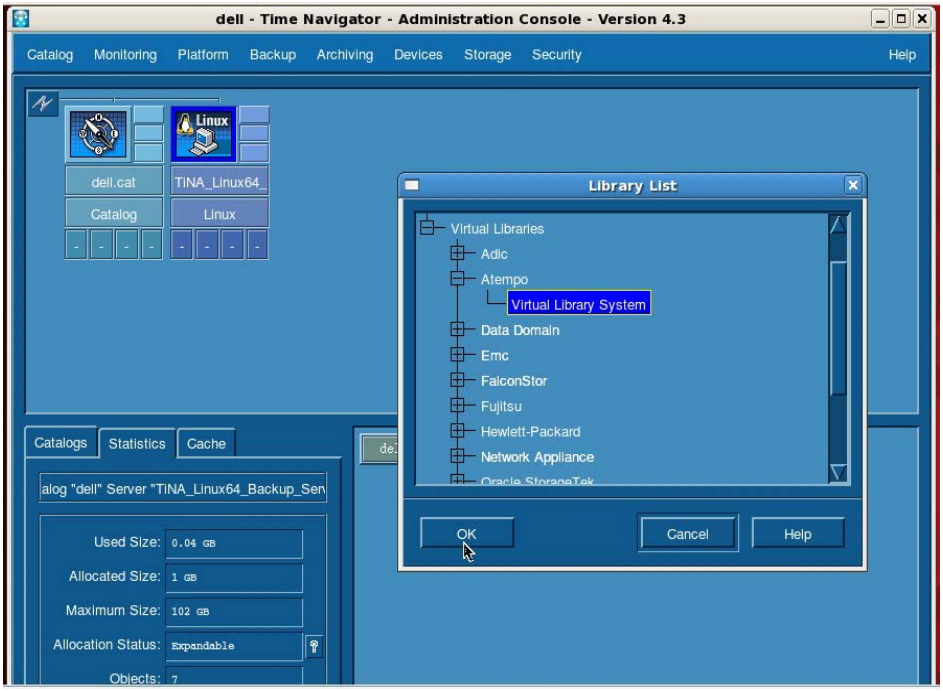
4 Select the data to be backed up, and start a backup job.

Configuring the NFS container as a TiNa-library

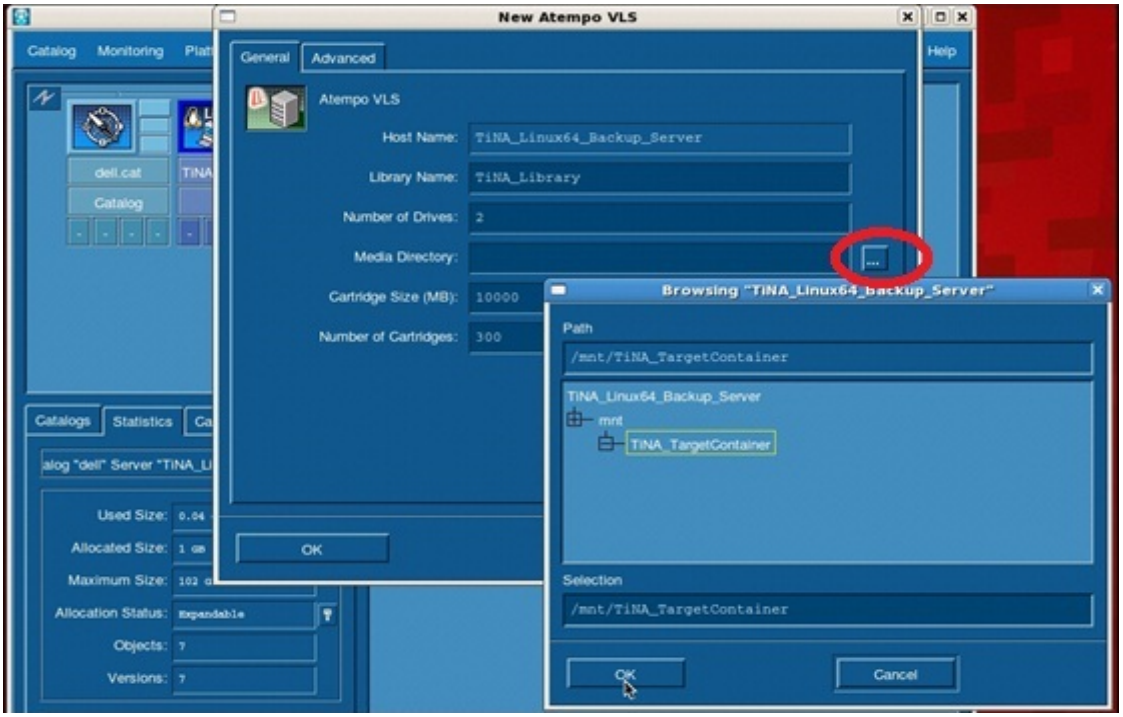
1. Enter the **tina_adm** command from the <TiNa install path>/Bin directory to open the Time Navigator-Administration Console-version 4.3 and configure the backup device in the form of a virtual library system.
2. Click **Library > Devices > New**.



3. Select **Virtual Libraries** and, in the Atempo section, click **Virtual Library System**.

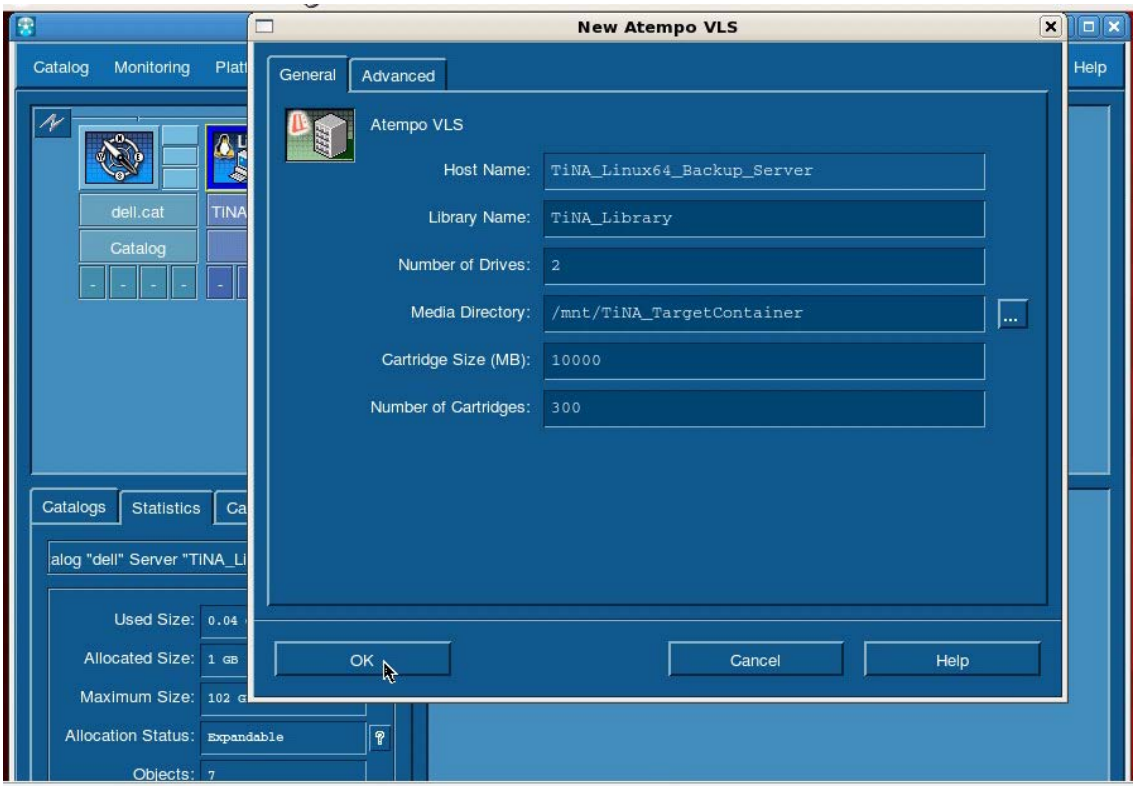


4. **Enter** a library name (for example, TiNA_Library) in the **New Atempo VLS** screen.
5. Browse the **Media Directory** to select the DR container (NFS) mount point, and click **OK**.



The DR container should be mounted on the machine on which TiNa is running.

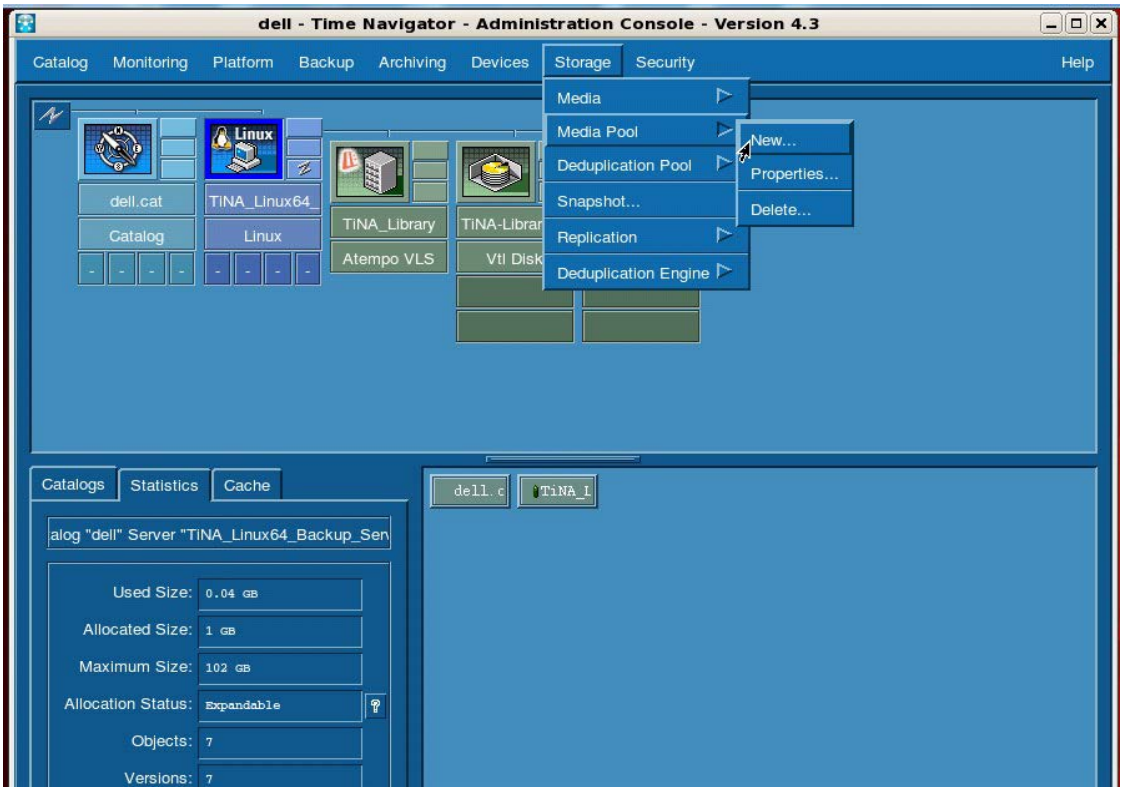
6. Click **OK** to assign the selected mount point on the **New Atempo VLS**



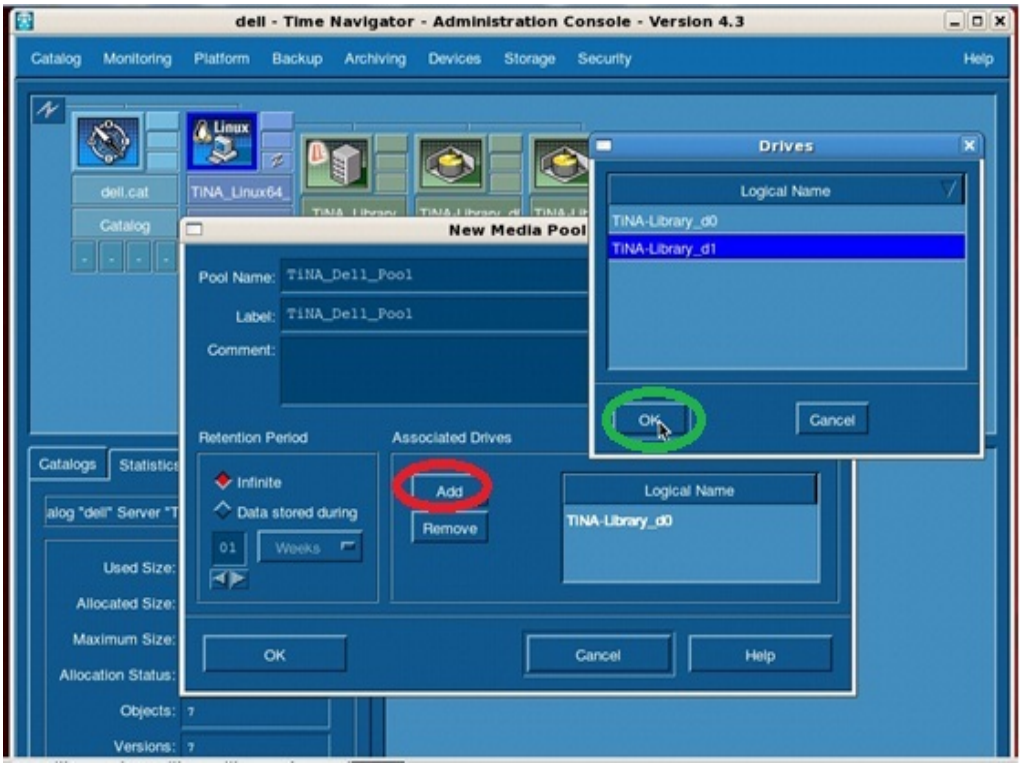
NOTE: See Appendix A for information about best practices, cartridge size, and number of cartridges for the DR Series system.

Creating a media pool and attaching TiNa logical drives

1. To create a Media Pool, select **Storage** > **Media Pool** > **New**.

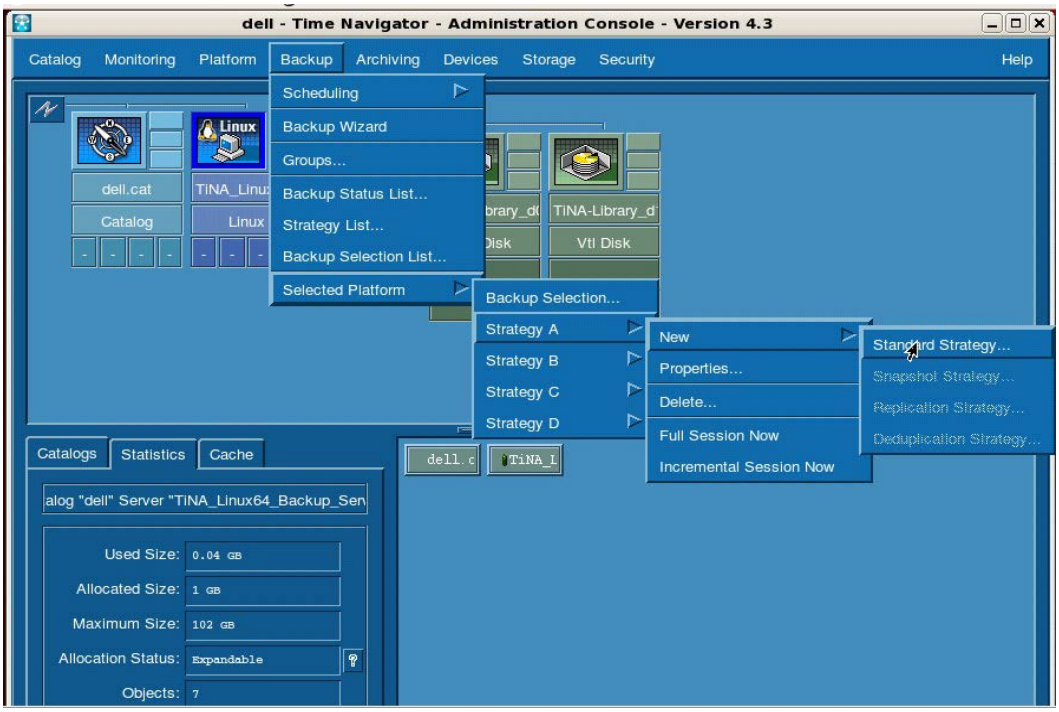


2. Enter a Pool Name and Label and click **Add**.
3. Select the available **Drives** in the list and click **OK**.

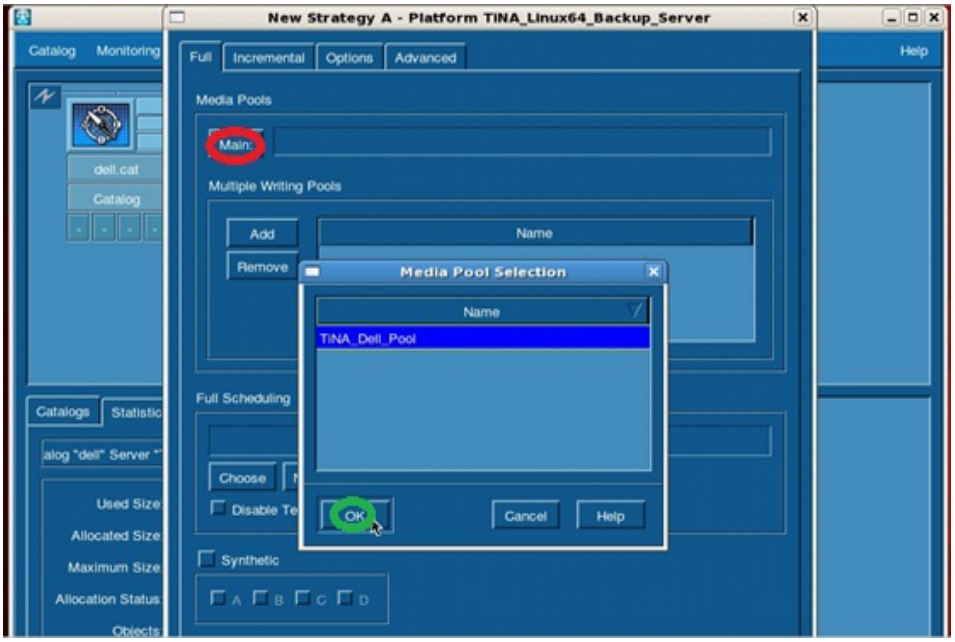


Configuring a TiNa backup strategy

1. Create a backup strategy by clicking **Backup > Platform Selection** and then selecting the Strategy (for example, **Strategy A**).
2. Click **New** and then click **"Standard Strategy."**



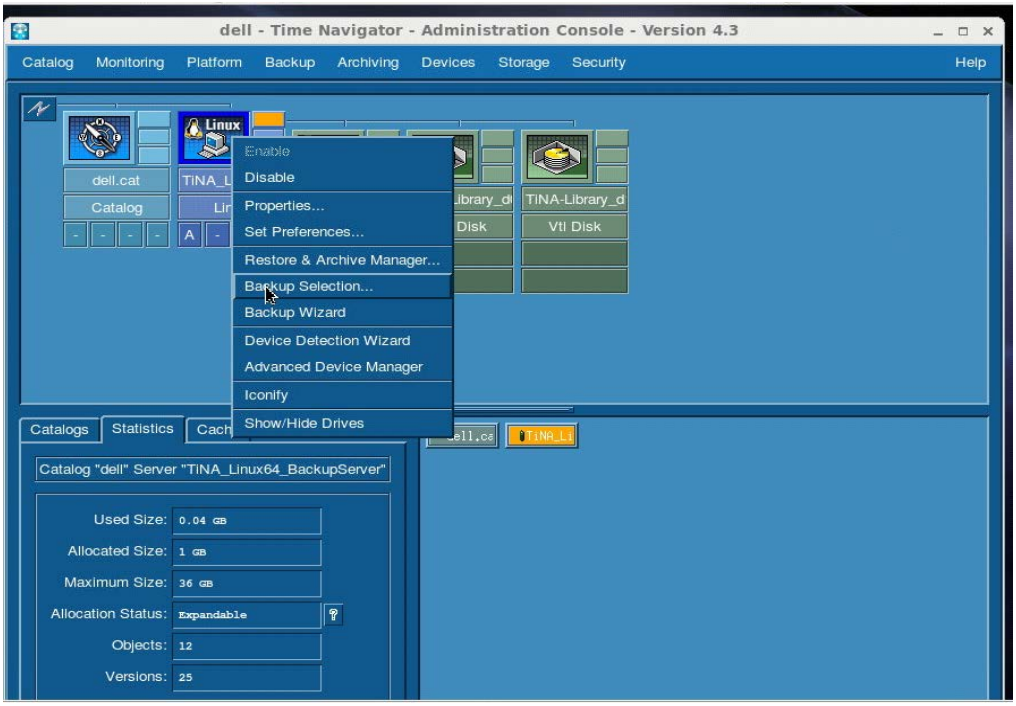
3. Click Main under Media Pools, and, in the Media Pool Selection dialog box, select the pool name and click **OK**.



Selecting the data to be backed up and starting a backup job

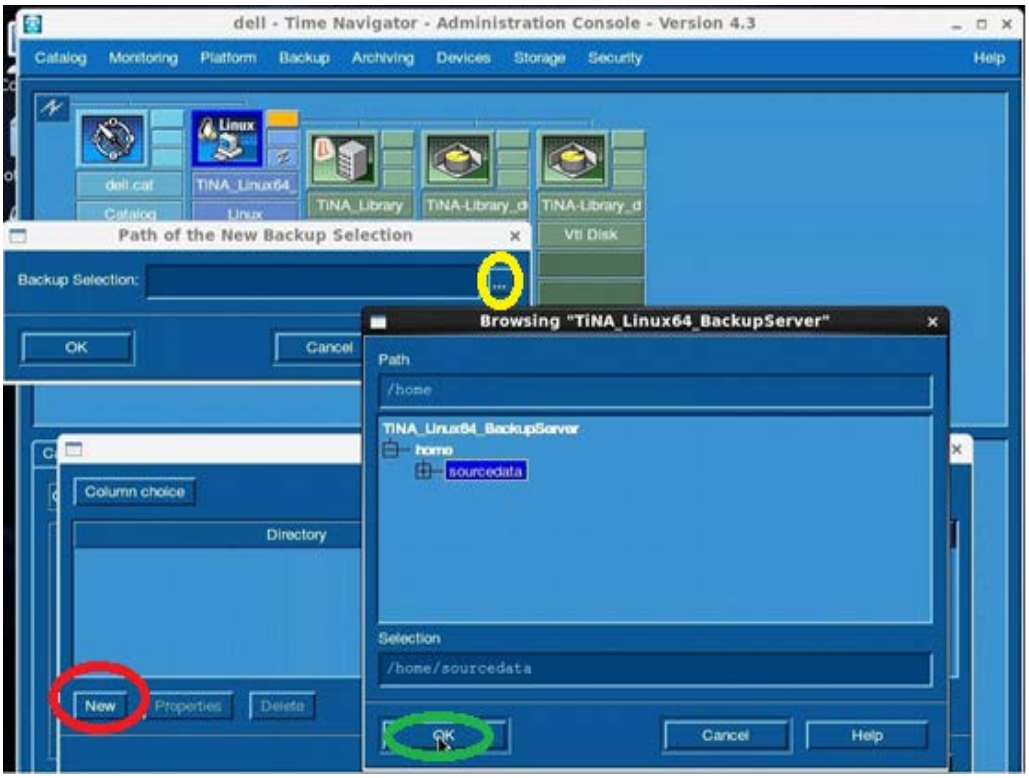
1 Configure the data to be backed up as follows:

a Right-click the Time Navigator backup server host icon and click **Backup Selection**.



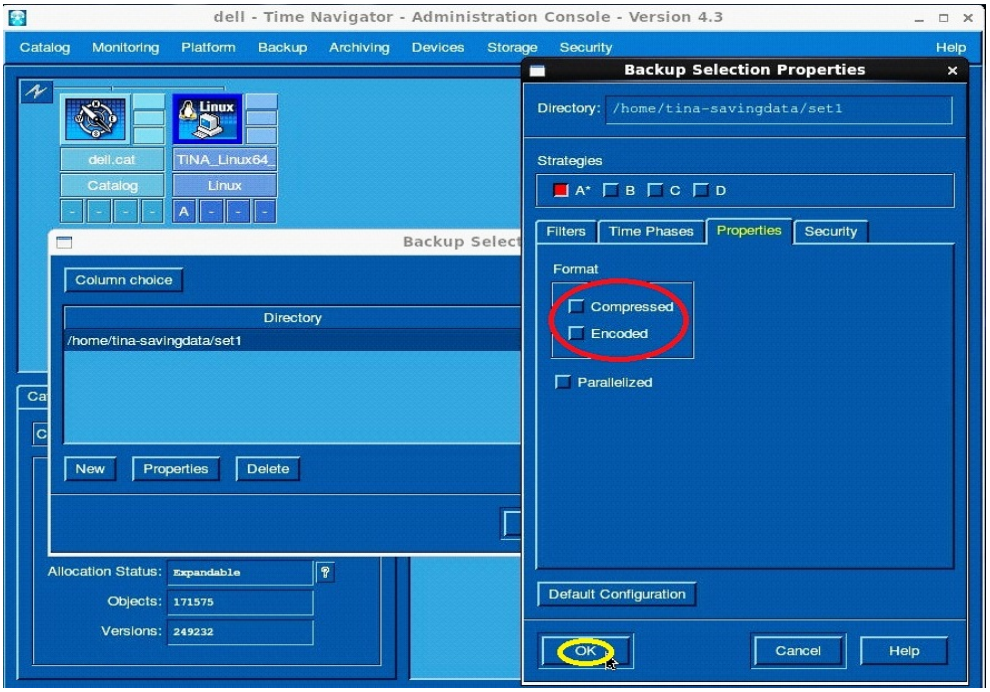
b Click **New** and then browse to the path of the data to be backed up.

c Select the directory location and click **OK**.



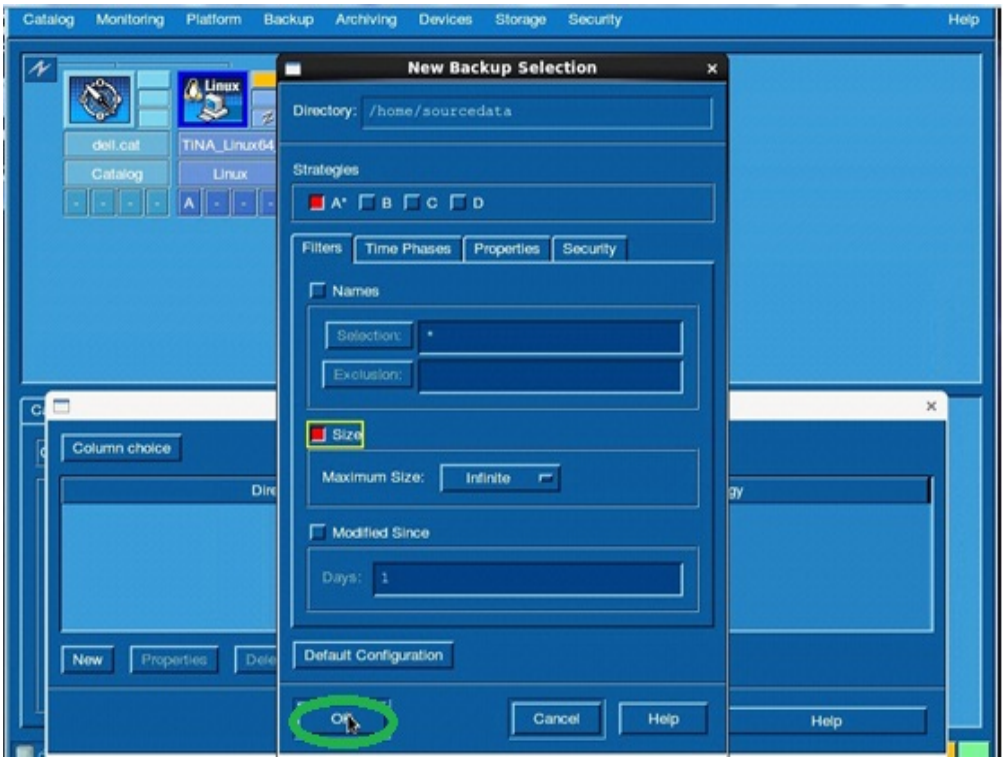
d Click **Properties**, and then clear the **Compressed and Encoded** checkboxes.

e Click **OK**.

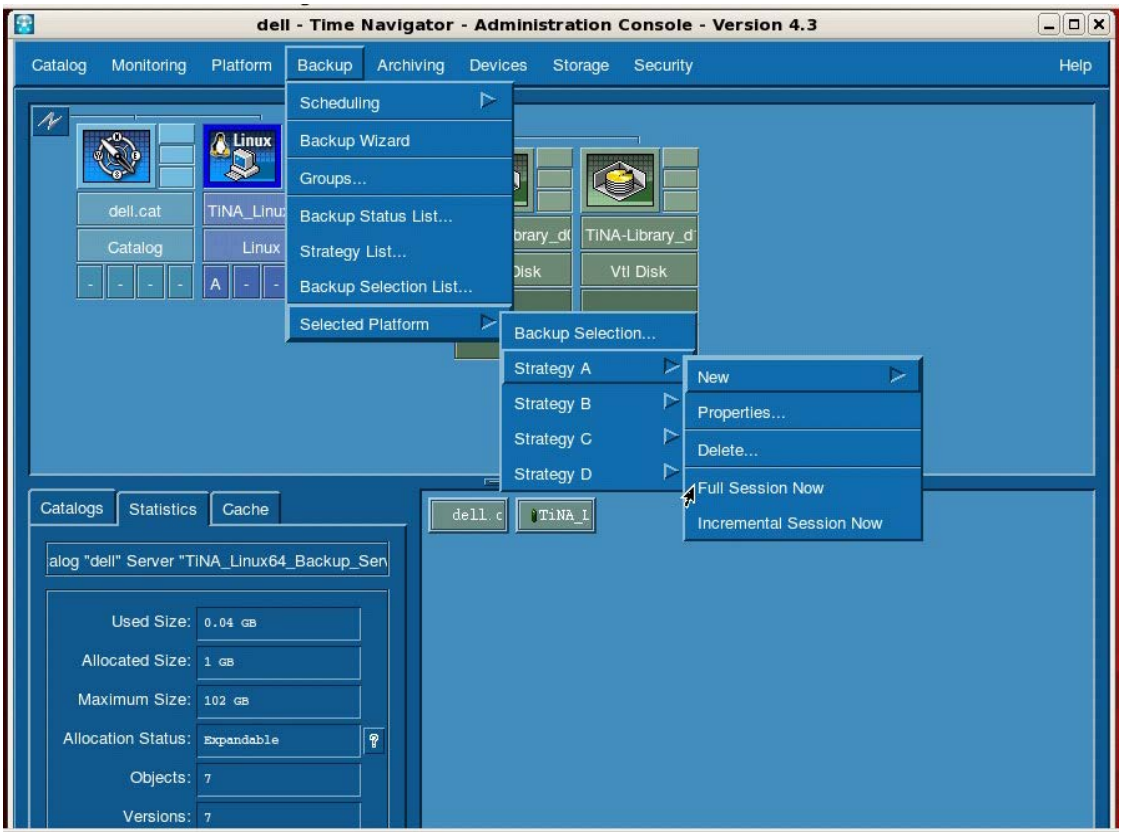


NOTE: Quest recommends that you do not enable the TimeNavigator native compression and encryption features while performing backup/restore.

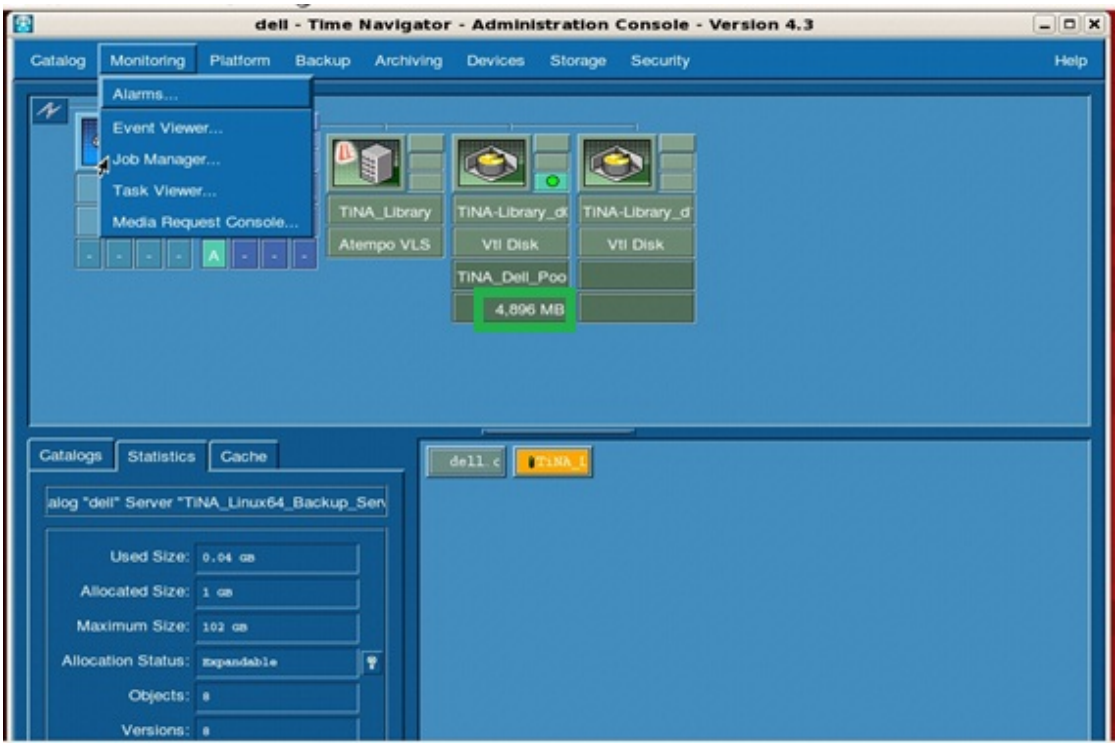
f Configure the properties for the new backup selection as needed, and click **OK**.



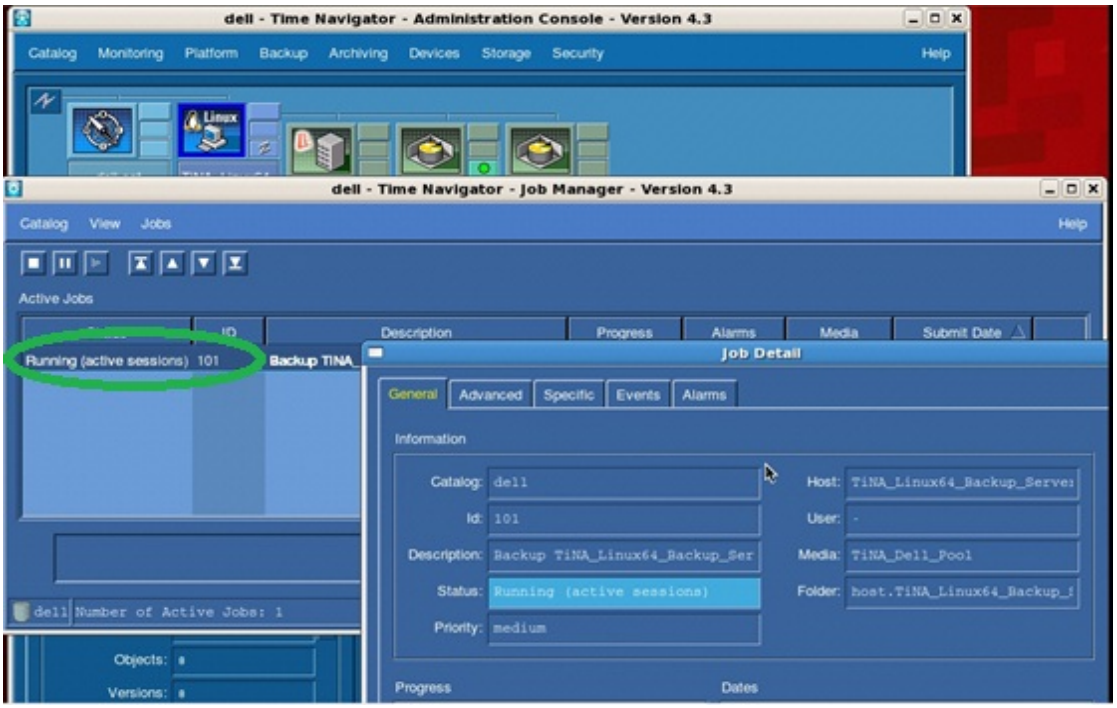
g Select **Backup > Selected Platform**. Select a Strategy, and click **Full Session Now**.



2 Monitor the status of the running job by clicking **Monitoring > Job Manager**. The backup progress is shown in VTL disk (logical drives).

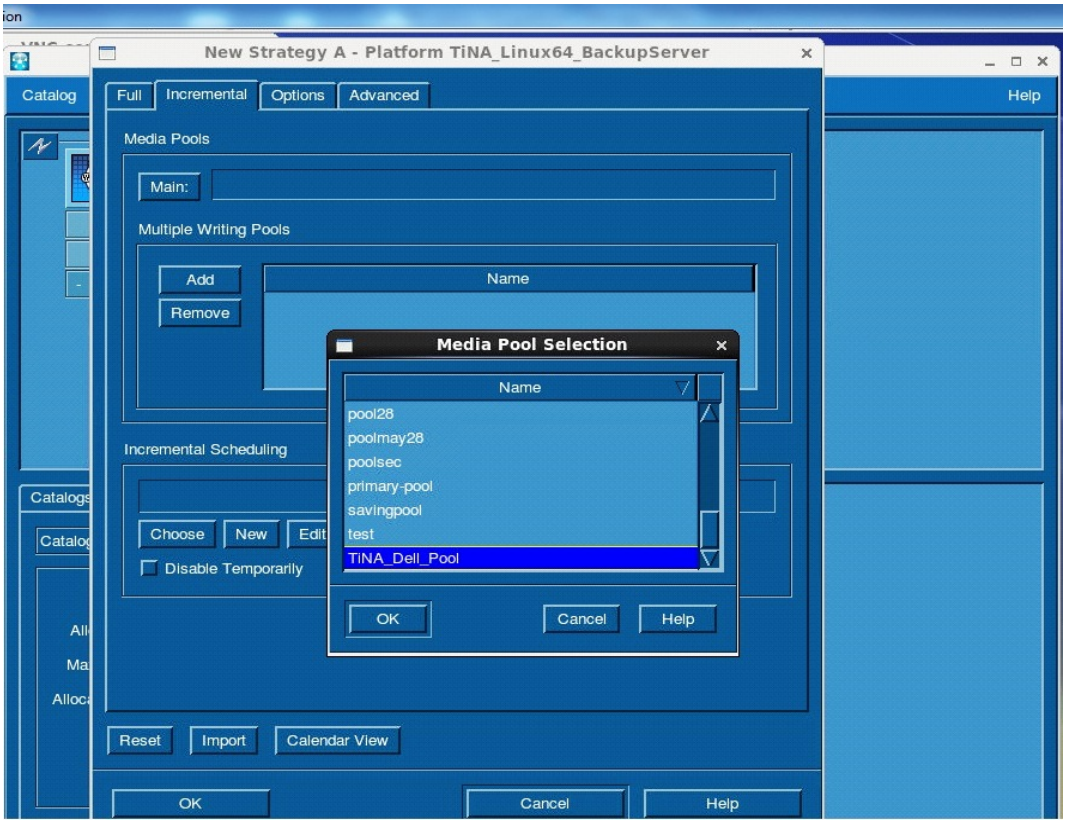


3 Double-click one of the Active Jobs to view the complete details.

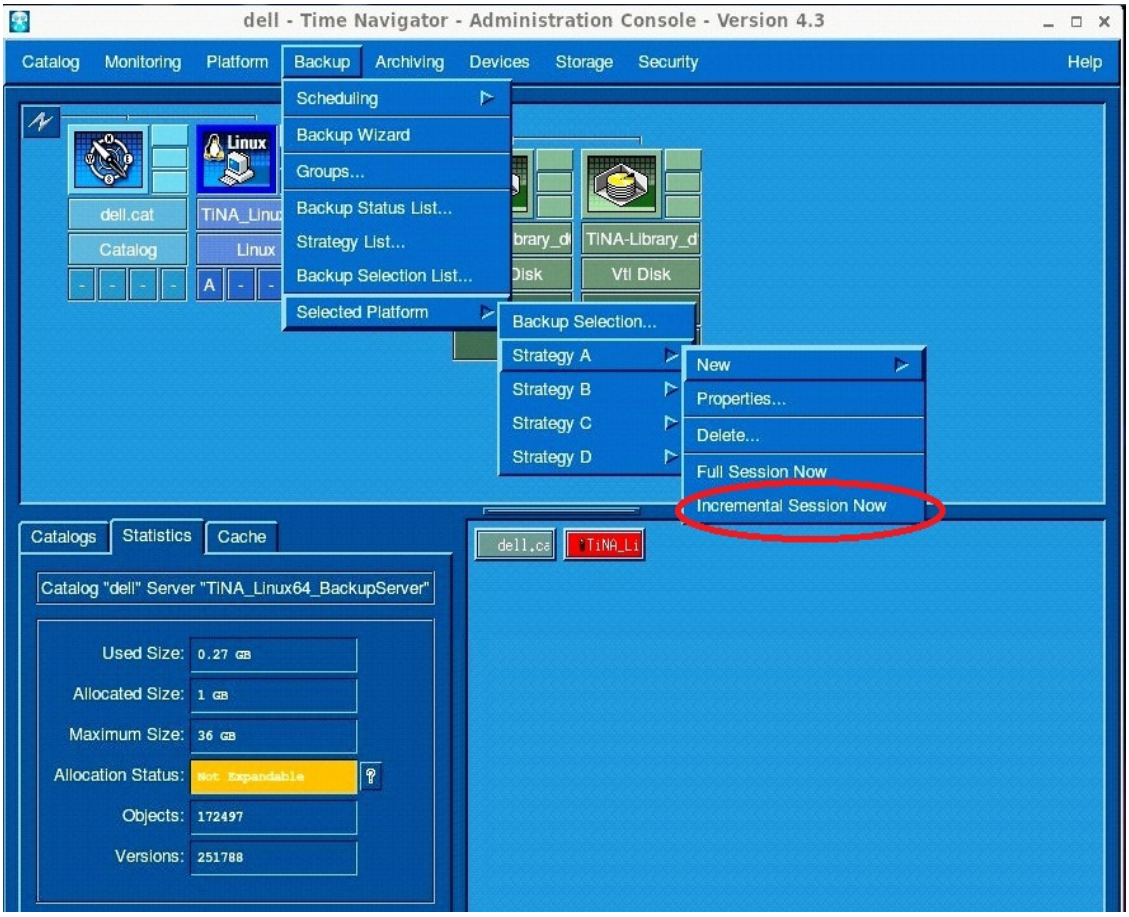


4 For Incremental Backup, add the Full backup Media Pool in the **Incremental** tab.

5 Browse the Media pools by clicking **Main**, and then selecting the Full backup Media Pool in the list.

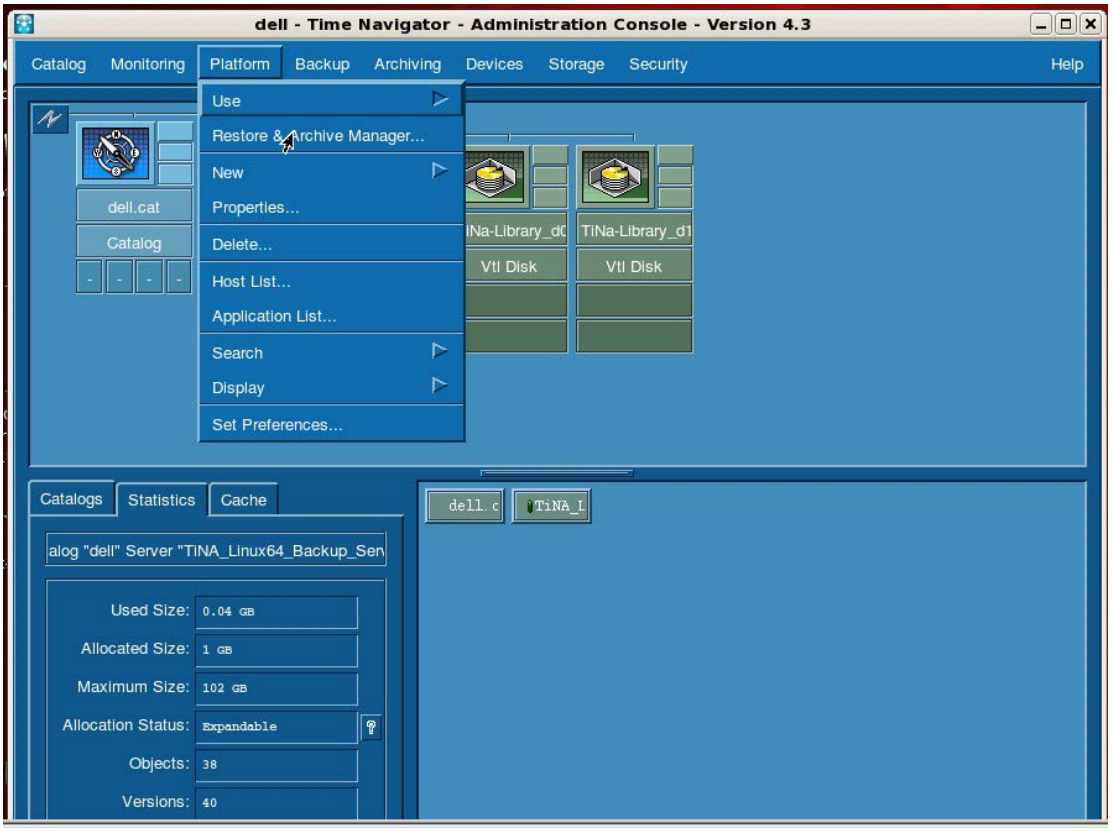


6 Select the full backup strategy by clicking **Backup > Platform Selection** and then selecting the Strategy (for example, **Strategy A**). Click **New > Incremental Session Now**.

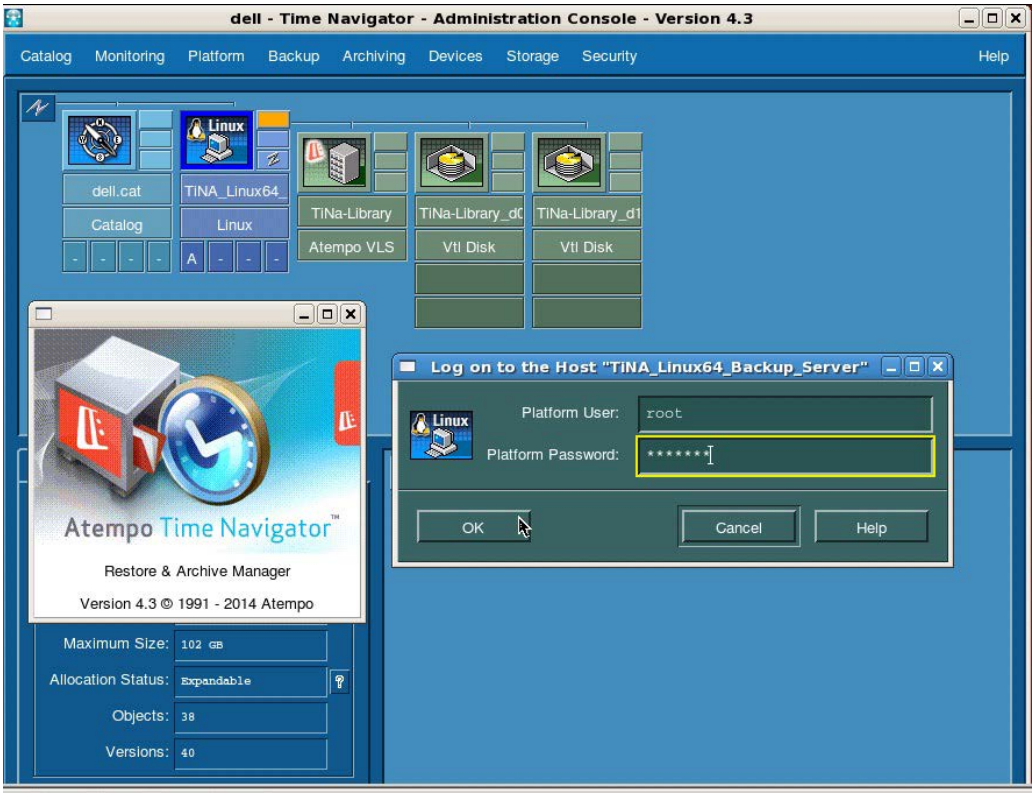


Configuring a restore job on ASG-Time Navigator for an NFS target

1 For a restore operation, select the Linux Time Navigator host, and configure the Restore operation by selecting **Platform > Restore & Archive Manager**.

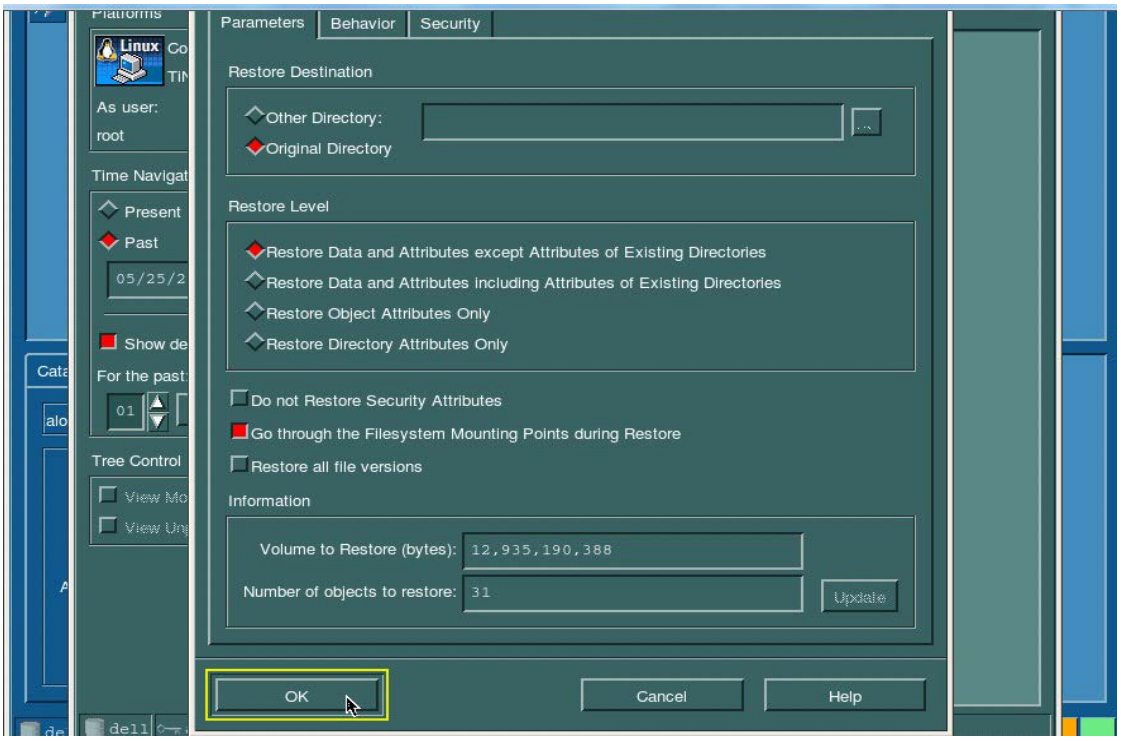


2 Enter the credentials of the Host for the Restore Job configuration and click **OK**.

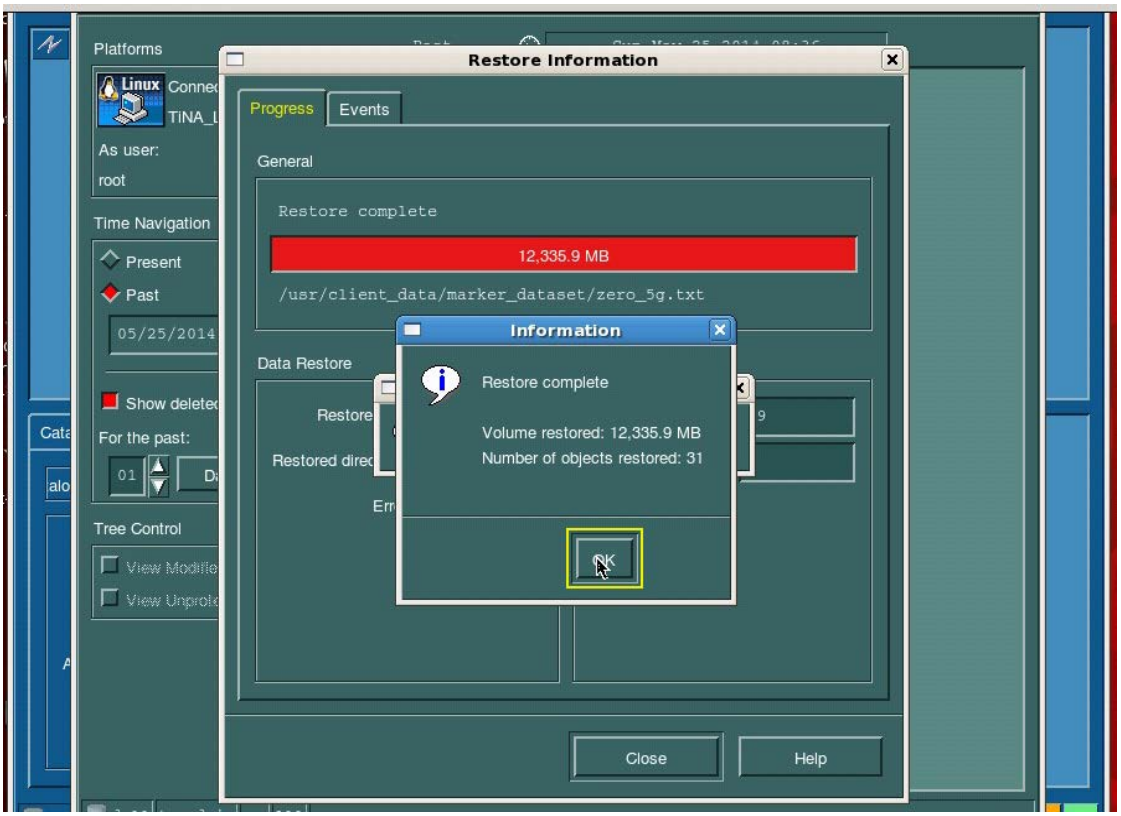


3 Browse to and select the objects to be restored, and then select **Restore > Run**.

4 Select one of the Restore Destinations and click **OK**.

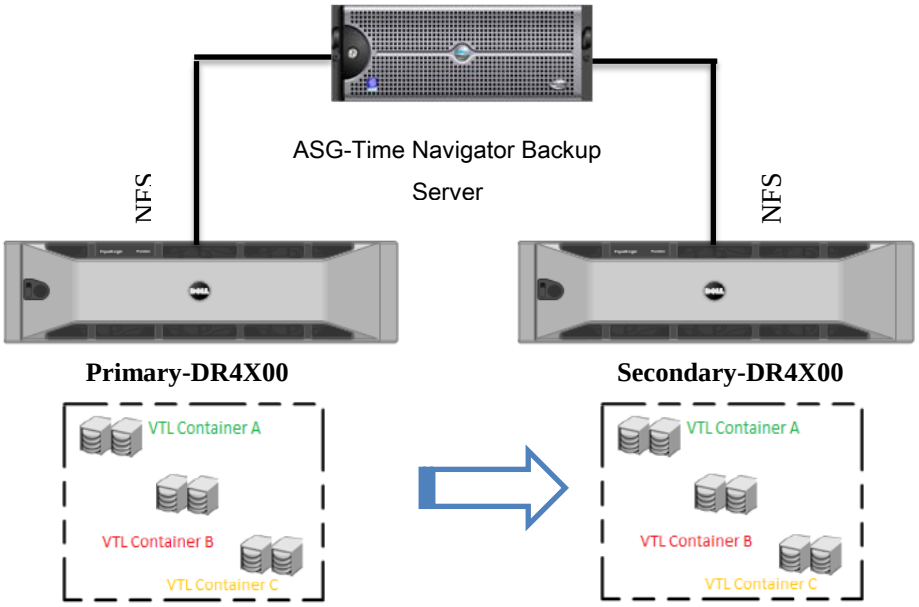


The Restore Information dialog box shows the restore progress.



Running a duplication and restore job on a secondary DR Series system NFS target

For certain Disaster Recovery scenarios, a duplicate copy of a backup data set from a primary DR Series system can be made available on a secondary DR Series system.



1 On the primary DR Series system, create an NFS container.

```
login as: administrator
administrator@10.250.242.139's password:
Last login: Mon Jun  2 12:49:20 2014 from 10.17.248.70
Total alert messages              : 2
Run `alerts --show --alerts` to see the alerts.
administrator@swsys-69 > container --add --name primary
Container "primary" created successfully.
administrator@swsys-69 > connection --add --type nfs --name primary
Successfully added connection entry.
NFS connection IP addresses       : *
NFS connection Root map           : root
NFS connection options            : rw
NFS connection Enabled            : Yes
administrator@swsys-69 > container  --marker --enable TiNa --name primary
Successfully enabled container "primary" with the following marker(s) "TiNa".
```

2 On the secondary DR Series system, create an NFS container.

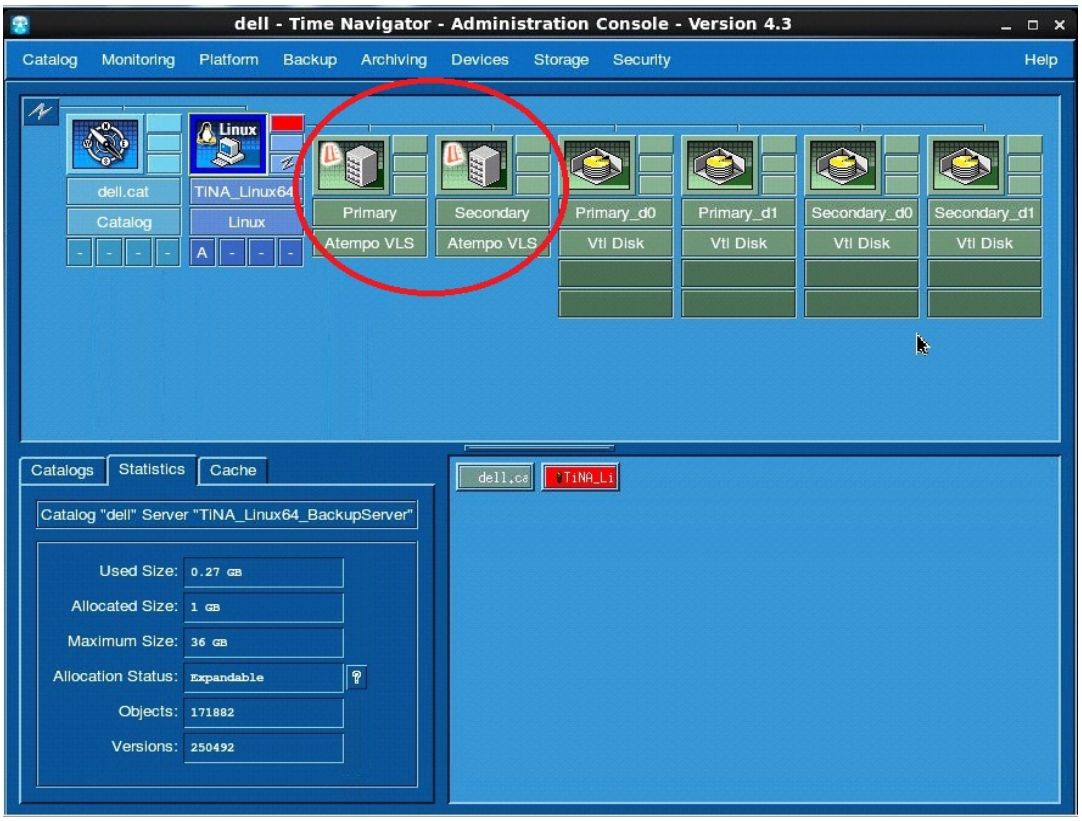
```
login as: administrator
administrator@10.250.243.119's password:
Last login: Thu Jun  5 06:43:55 2014 from 10.115.132.57
Total alert messages            : 0
administrator@swsys-73 > container --add --name secondary
Container "secondary" created successfully.
administrator@swsys-73 > connection --add --type nfs --name  secondary
Successfully added connection entry.
NFS connection IP addresses     : *
NFS connection Root map         : root
NFS connection options          : rw
NFS connection Enabled          : Yes

administrator@swsys-73 > container --marker --enable TiNa --name secondary
Successfully enabled container "secondary" with the following marker(s) "TiNa".
administrator@swsys-73 >
```

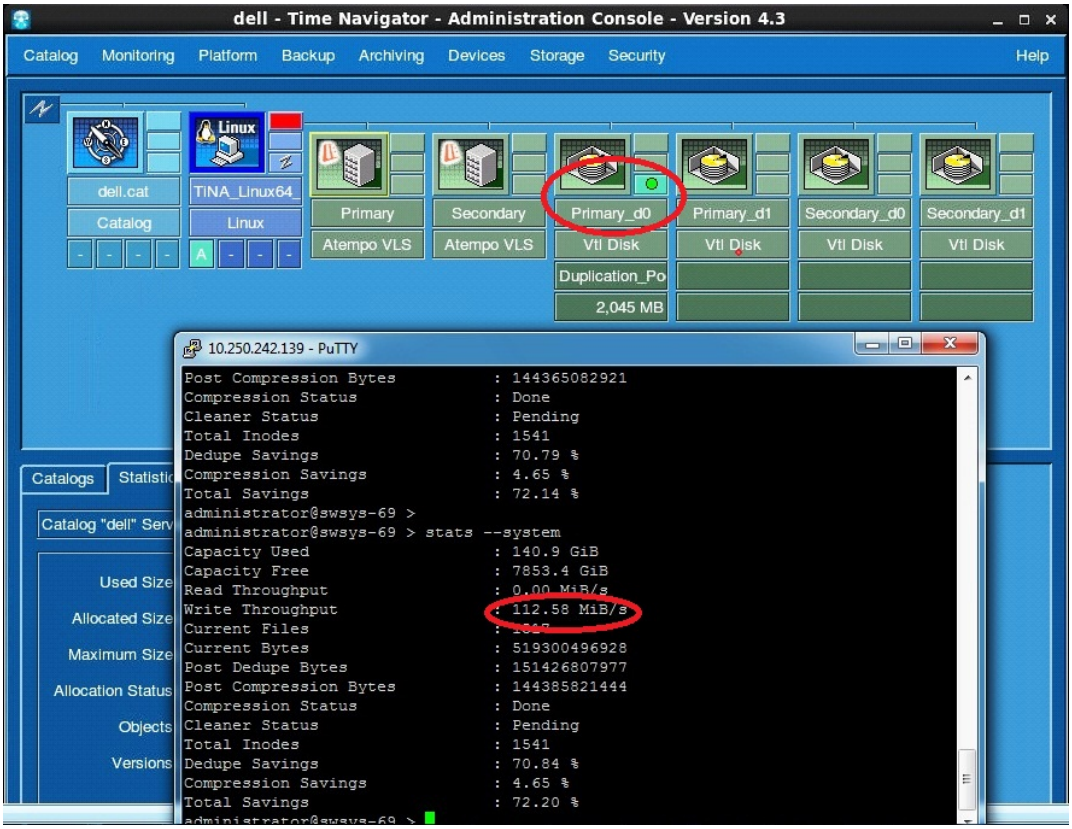
3 Mount the primary and secondary DR containers on Time Navigator backup server

```
[root@TiNA_Linux64_BackupServer ~]# mount -t nfs 10.250.242.139:/containers/primary /mnt/primary/
[root@TiNA_Linux64_BackupServer ~]# mount -t nfs 10.250.243.119:/containers/secondary /mnt/secondary/
```

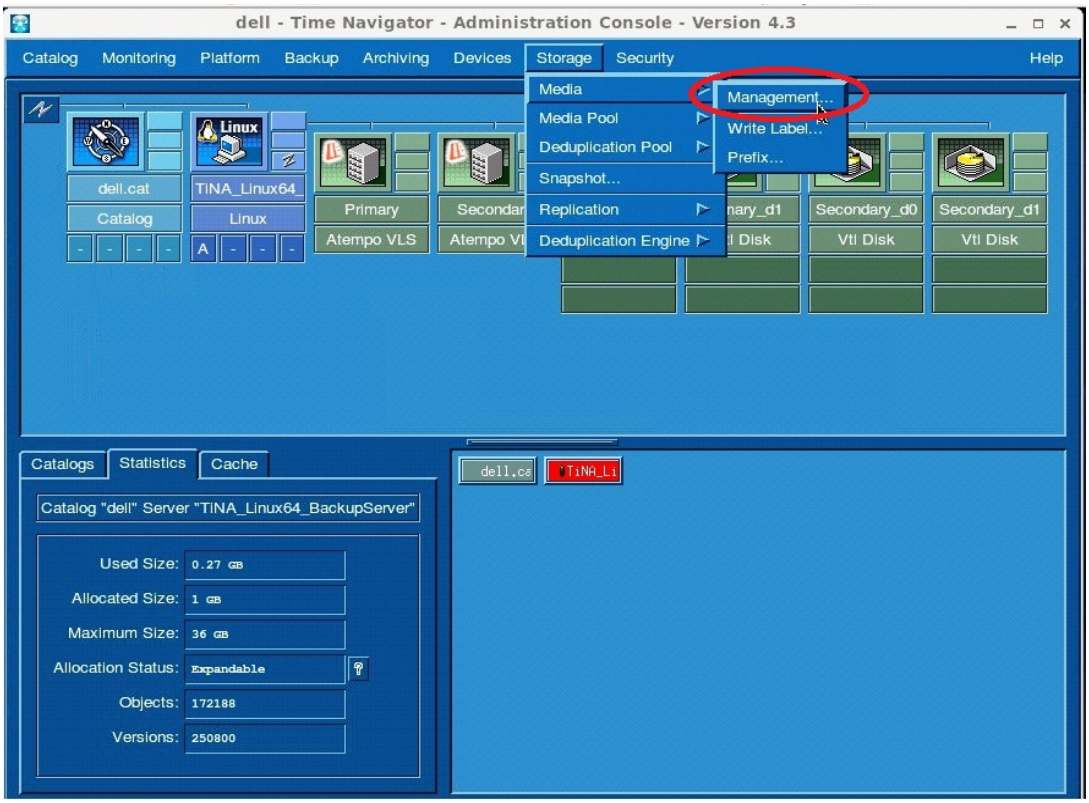
4 The following figure shows the configured primary and secondary **DR** containers as **Primary-VLS** and **Secondary-VLS** for demonstration of duplication and restore from the secondary DR system.



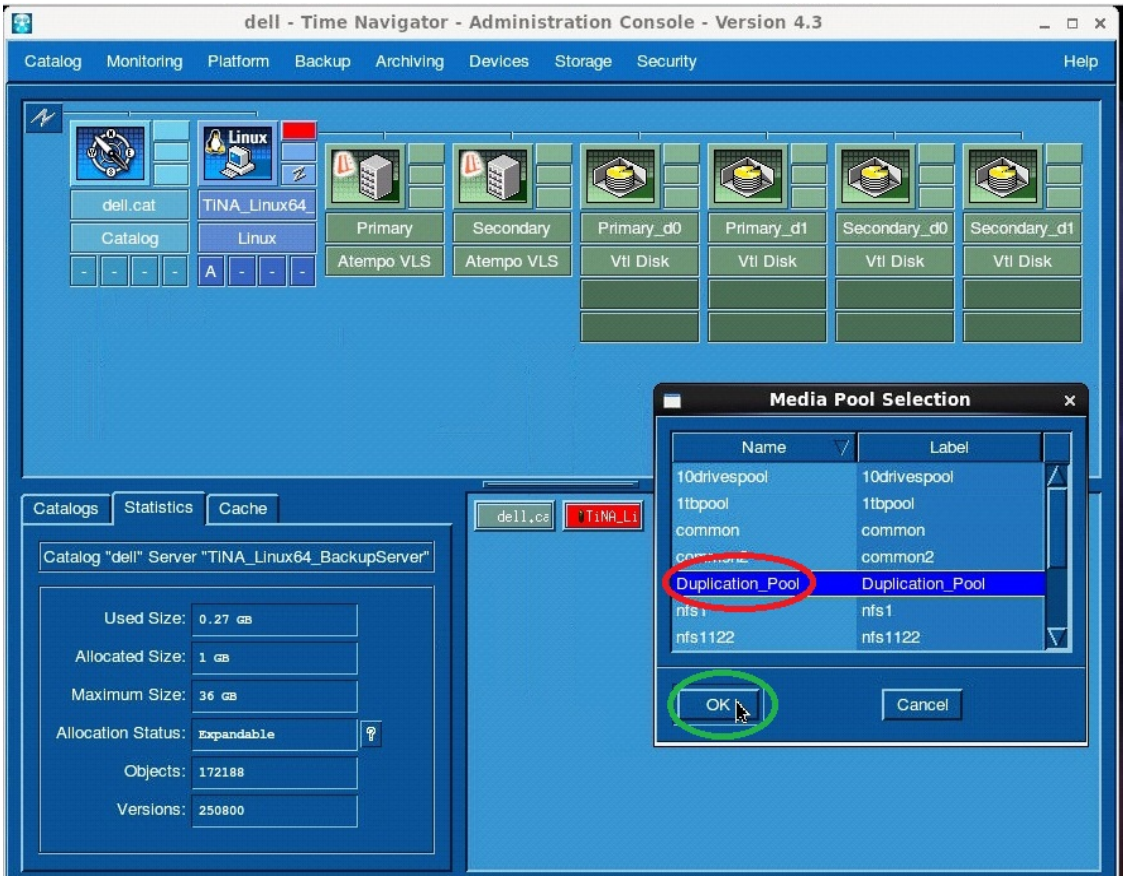
The Backup Job is configured and submitted on the primary DR Series system.



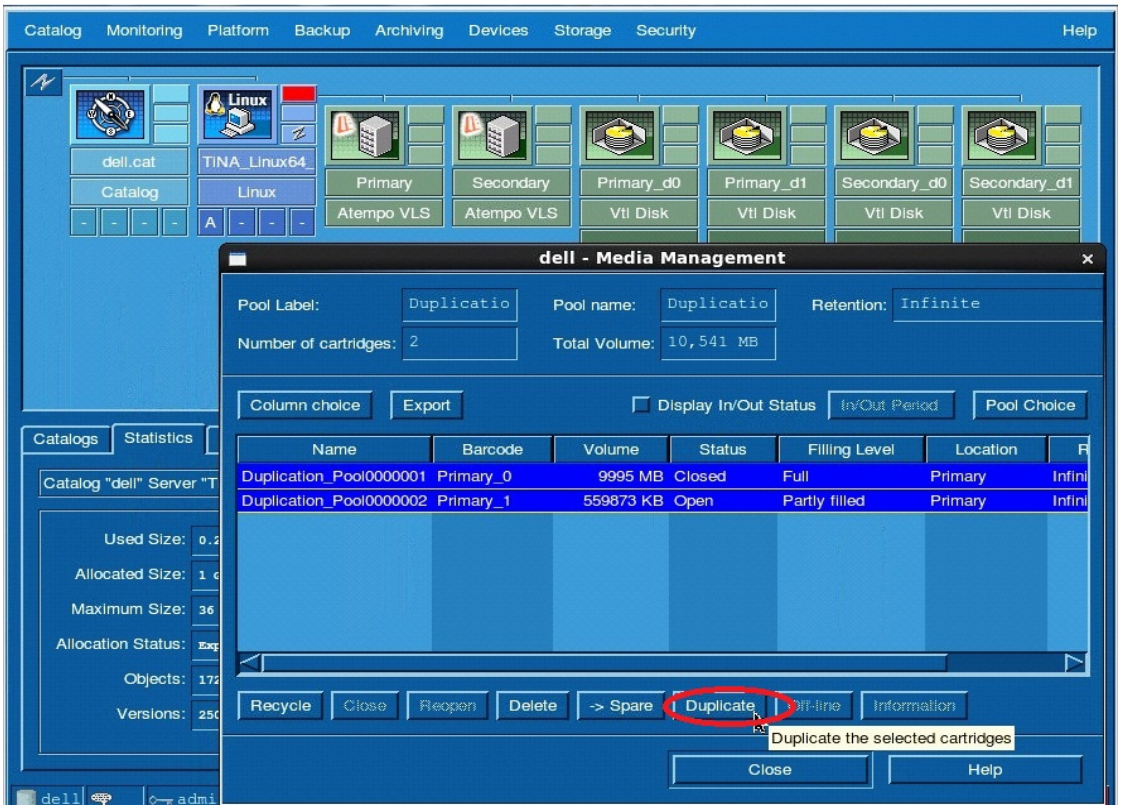
5 For duplication of existing backup data Configuration, when the primary backup job is completed, click **Storage > Media > Management**.



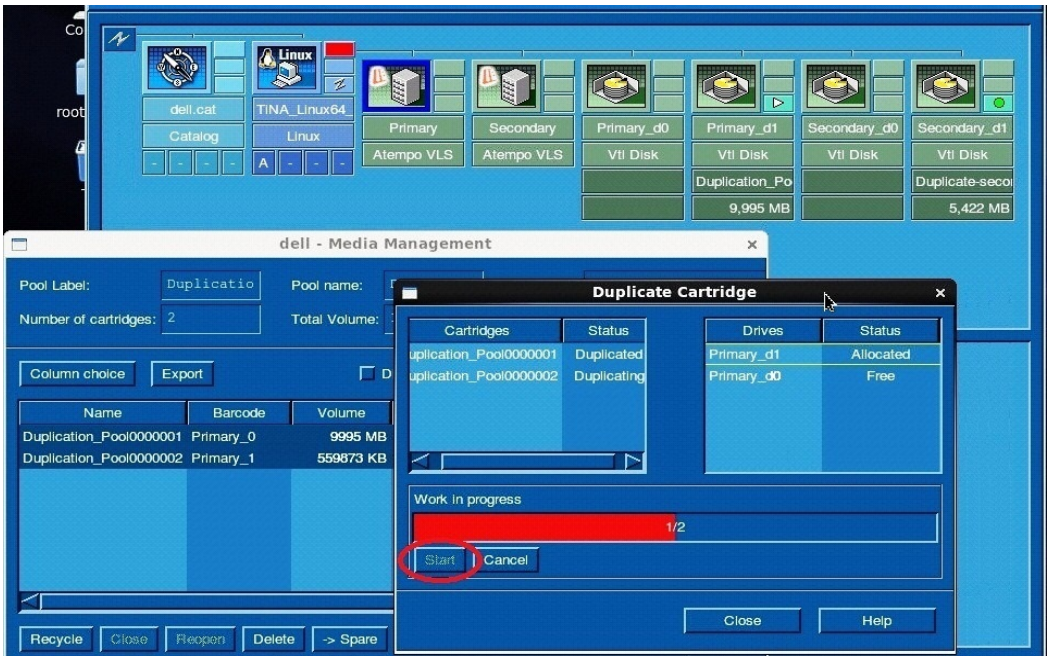
6 Select the media pool name on which the secondary logical drives are available and click **OK**.



7 Select the cartridges and click **Duplicate**.



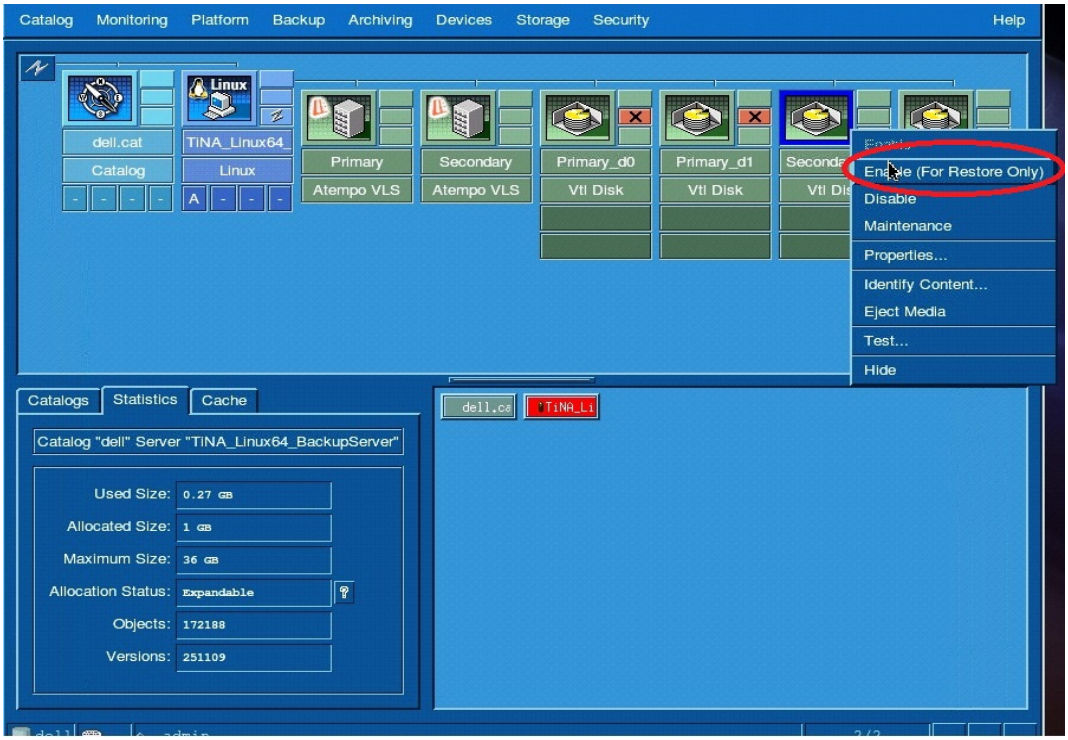
8 Click **Start** to see the Duplication in progress.



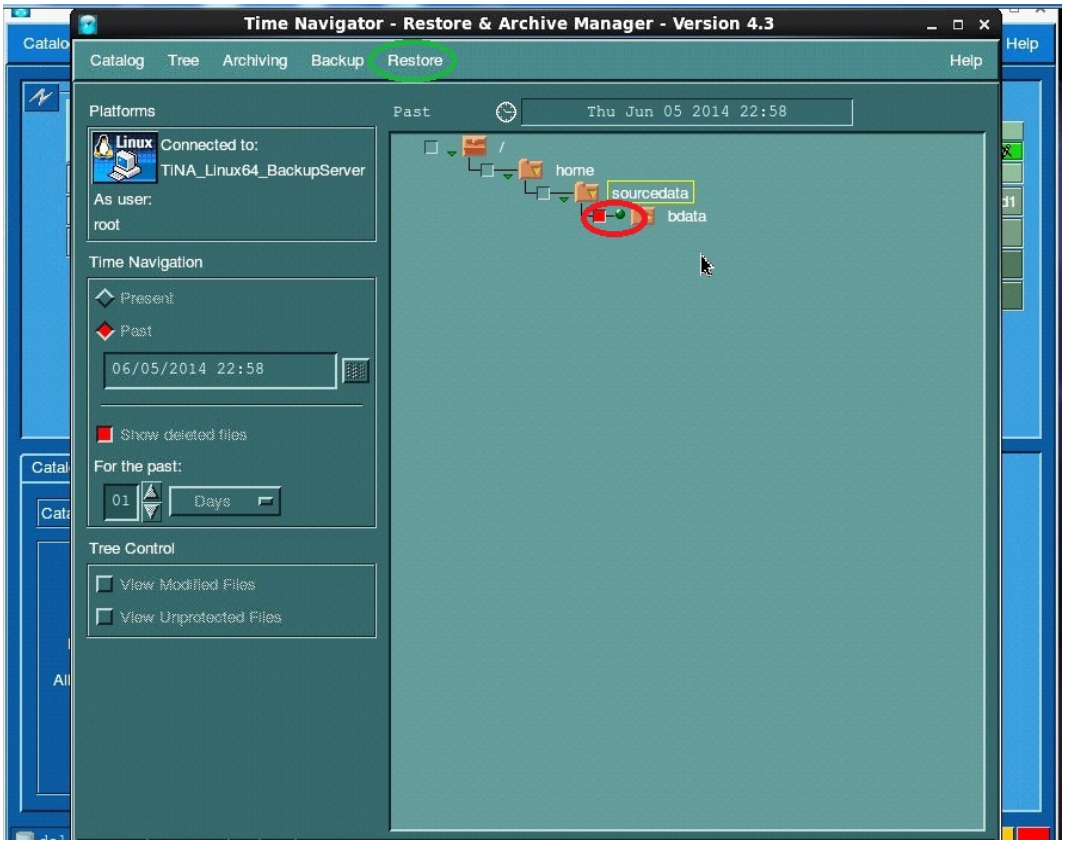
9 Restore from secondary is required when the primary is down or inaccessible.

```
administrator@swsys-69 > connection --disable --type nfs --name primary
Successfully updated connection entry.
NFS connection IP addresses     : *
NFS connection Root map         : root
NFS connection options          : rw
NFS connection Enabled          : No
administrator@swsys-69 >
```

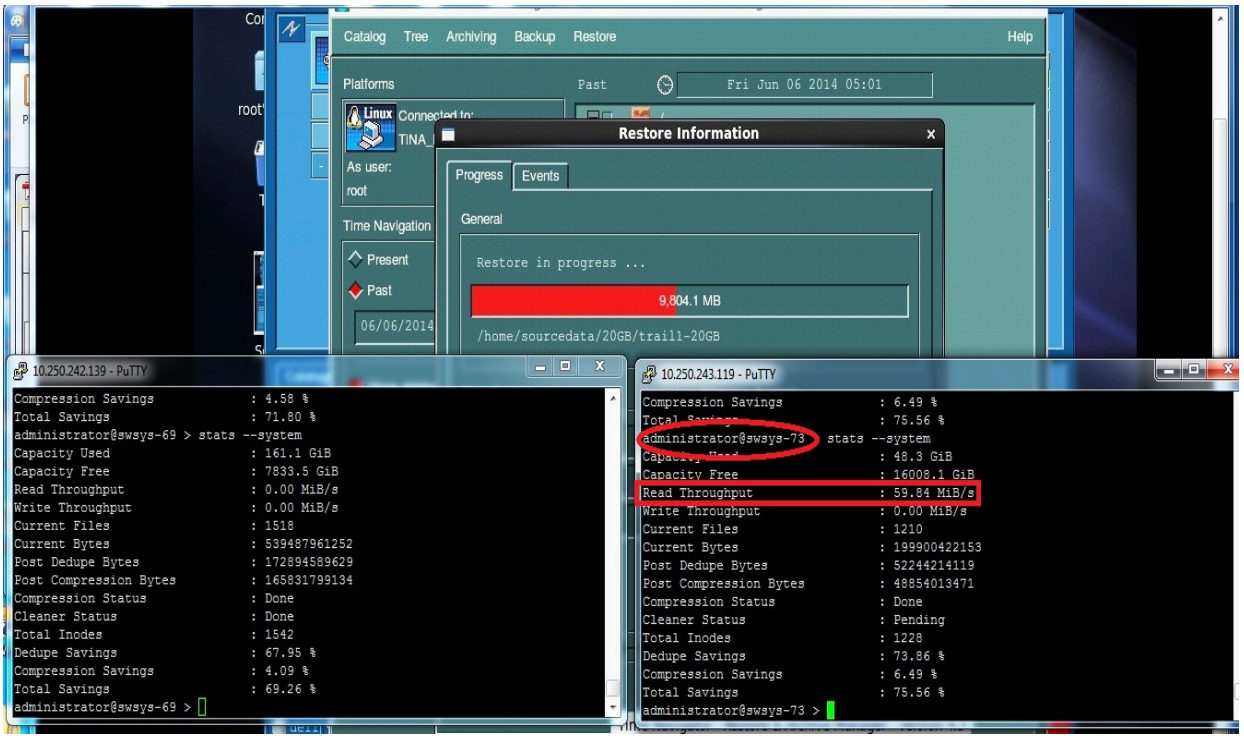
10 Right-click the secondary logical drive and click **Enable (For Restore Only).**



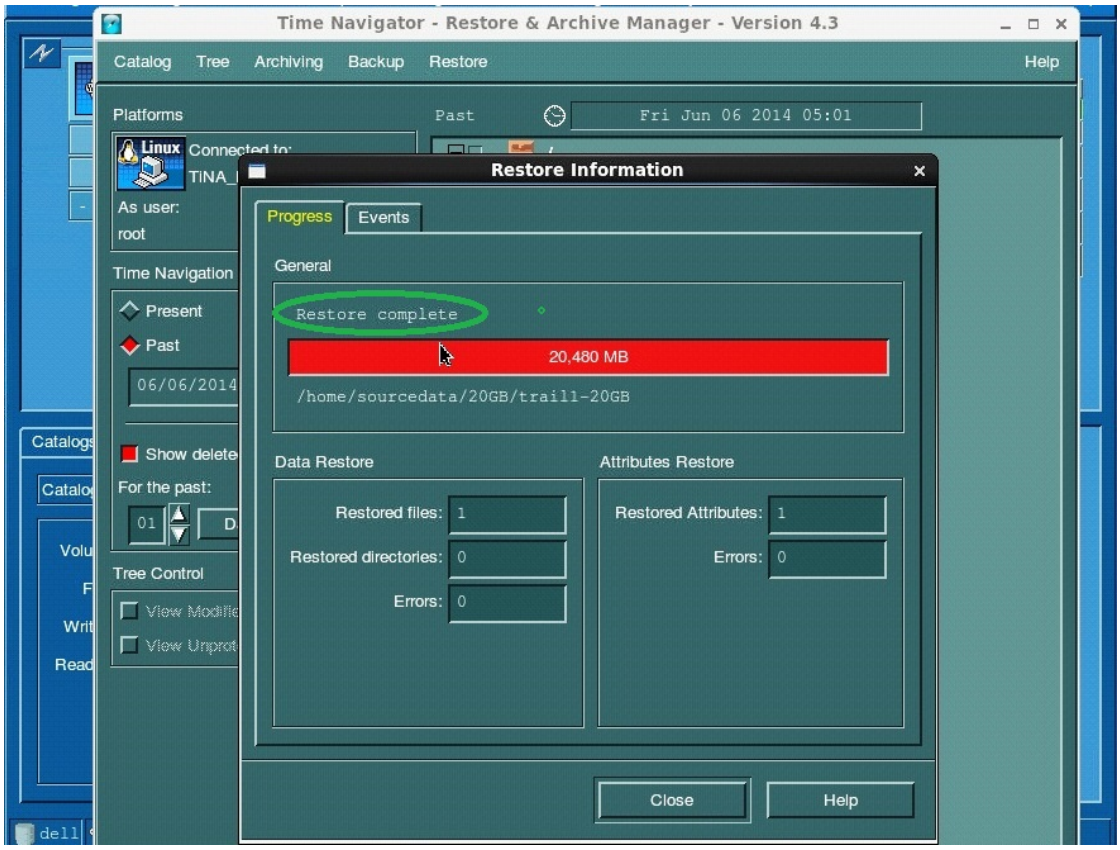
11 Restore data selection.



12 Monitor restore progress on the secondary DR Series system.



13 Restored data from secondary DR container to client.



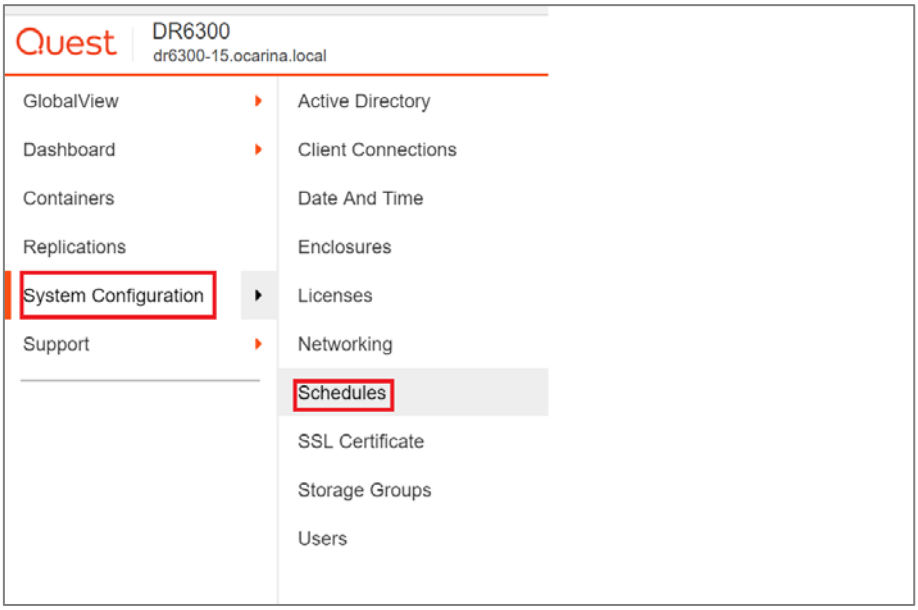
Setting up the DR Series system cleaner

Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from system containers in which files were deleted as a result of deduplication.

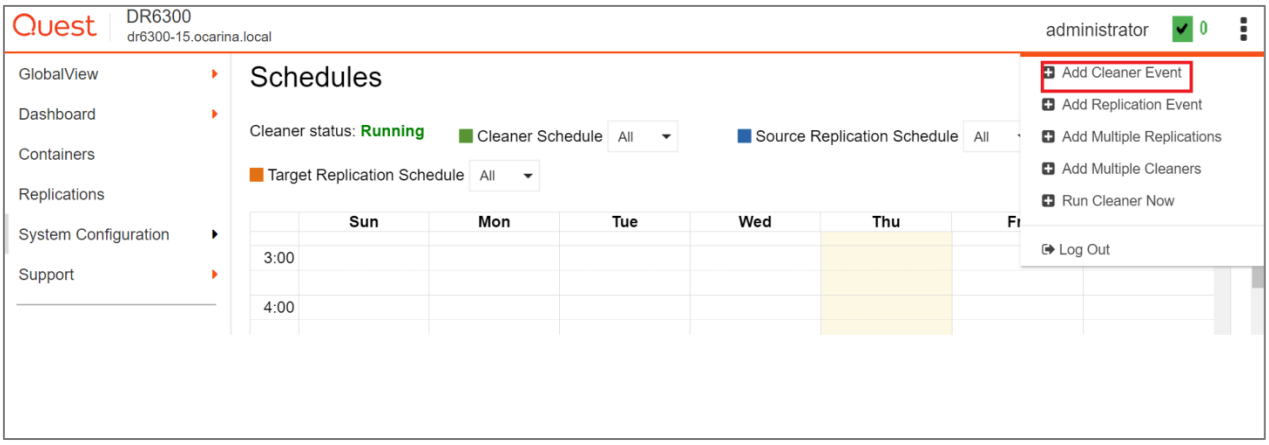
The system cleaner runs during idle time. If your workflow does not have a sufficient amount of idle time on a daily basis, then you should consider scheduling the cleaner to force it to run during a scheduled time.

If necessary, you can perform the procedure shown in the following example steps to force the cleaner to run. After all of the backup jobs are set up, the DR Series system cleaner can be scheduled. The DR Series system cleaner should run at least 40 hours per week when backups are not taking place, and generally after a backup job has completed.

1 Click System Configuration > Schedules.

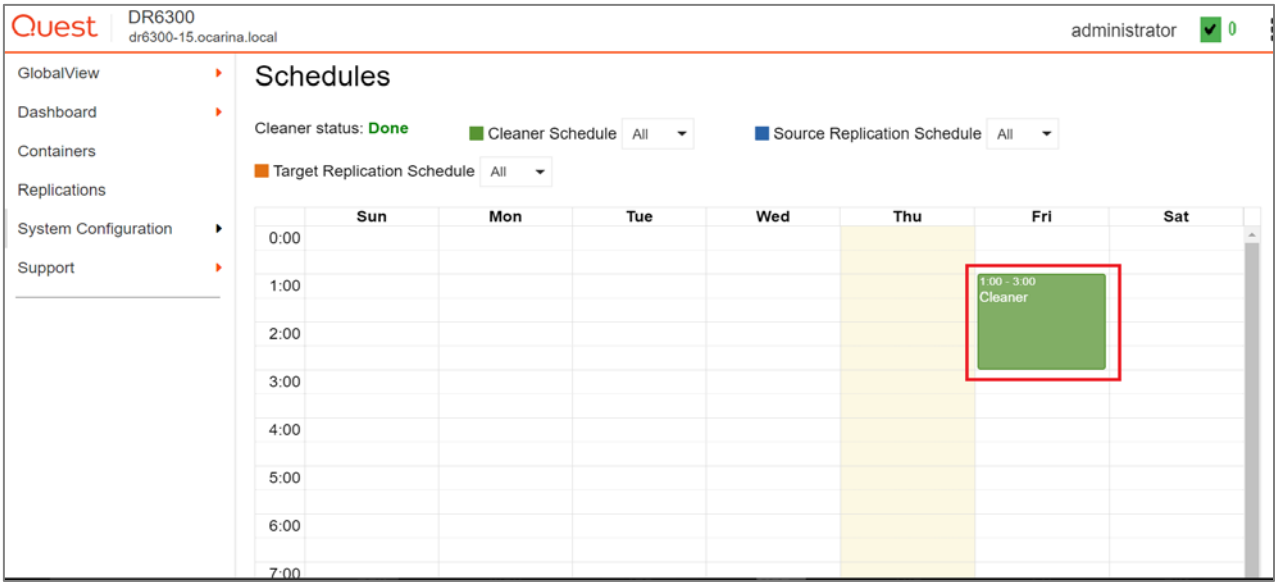


2 In the Action menu, click **Add Cleaner Event**.



3 Define the cleaner schedule and click **Save**.

The new schedule will appear on the Schedules page.



Monitoring deduplication, compression, and performance

After backup jobs have run, the DR Series system tracks capacity, storage savings, and throughput on the DR Series system dashboard. This information is valuable in understanding the benefits of the DR Series system.

NOTE: Deduplication ratios increase over time. It is not uncommon to see a 2-4x reduction (25-50% total savings) on the initial backup. As additional full backup jobs are completed, the ratios will increase. Backup jobs with a 12-week retention will average a 15x ratio, in most cases

A - Best practices for setting up ASG-Time Navigator VTL on a DR Series system

The DR Series systems are capable of running a cleaning cycle on a regular basis to recover data space that is no longer required by the deduplication process. Using a DR Series system as an ASG-Time Navigator VTL repository requires periodic maintenance to achieve the best usage from the system. Space reclamation from virtual media of a ASG-Time Navigator VTL hosted on a DR Series system has some specific requirements. Even though ASG-Time Navigator can locate and blank media that is marked for spare or reuse, the DR Series system will not know that ASG-Time Navigator has marked the media for spare or reuse and will not reclaim the space on the next clean cycle. This is due to the fact that ASG-Time Navigator will only update the header on the media and not scrub through and remove the old data.

To ensure that the cleaner cycle can reclaim space, the marked for reuse media must be identified and cleared using the tina_libary_control. Tina_cart_control utilities must be removed and then re-added as a new file. Since the new file no longer has any content, the DR Series cleaner cycle can reclaim the space.

Due to various factors such as data set size, data set iteration or count, retention period, and change rate, it can be difficult to determine the best VTL size and configuration for any given deduplication situation. One of the best practices is to:

- Size the VTL to no more than 10x the physical available disk space.
- Or, assess how much data you have to back up and the required retention periods for each set of data so as to not exceed either one of these two guidelines when creating the virtual media for the virtual tape library.
- And, set the drive count to be equal to the number of simultaneous jobs or data streams desired, without exceeding the maximum guidelines set forth by the vendor.

For Example: Starting with a storage appliance with 2TB of physical disk space. Based on the 10X usage recommendation, you can create a VTL of 20TB of total storage. But, given that the data backed up per week is

2TB and data retention is 4 weeks, the total amount of data stored at any given time would only be 8TB. Reducing the VTL space to 10TB would then be a more efficient use of space.

Once the overall size of the VTL is determined, the number of virtual drives to create and the granularity of the VTL is the next consideration.

Most storage appliance operating environments can effectively handle a set number of streams. Any read or write operation to and from a VTL virtual drive would denote a stream. As a rule of thumb, the number of virtual drives to create in the VTL should reflect what is required to support simultaneous streams, or concurrent jobs. Creating an excessive number of drives does not yield any benefits and could lead to performance degradation. It is important to also never exceed the number of streams supported by the appliance vendor's operating environment when creating VTLs and virtual drives.

Media size is the final consideration when creating a VTL. Unlike physical media, virtual media can be created to any size within the allowed range set by the appliance. So proper media size selection is important to ensure smooth operation of the VTL. Creating a small number of large media will extend the retention of expired data and prevent proper recycling within a media pool. Creating a large number of small media puts a strain on the ASG-Time Navigator Media Management process and can cause contention of resources. We recommend that the media size be made to accommodate for the media group retention policy such that when the retention period is expired for that group all items on the media should expire as well thus allowing for the reuse of the virtual media in question.

B - Creating a storage device for CIFS

There are two options for ASG-Time Navigator to authenticate to a DR Series system through CIFS.

- The DR Series system is joined into an Active Directory Domain: Integrate ASG-Time Navigator and DR Series system with Active Directory and ensure the Active Directory user has appropriate ACLs to the DR Series system container share.
- The DR Series system is a standalone CIFS server: Make sure this CIFS user has appropriate access permission to the DR Series system container share. The ASG-Time Navigator Backup Node will use this user to authenticate to the DR Series system share in Workgroup mode. To set the password for local CIFS administrator on the DR Series System, log on to the DR using SSH.
    - Log on with username Administrator and password St0r@ge!
    - Run the following command:

      ```
      authenticate --set --user administrator
      ```

NOTE: The CIFS administrator account is a separate account from the administrator account used to administer the appliance. After an authentication method is chosen, set the ASG-Time Navigator service account to use the CIFS administrator account.

C - Creating a storage device for NFS

For NFS backup using the ASG-Time Navigator, a target folder needs to be created as an NFS share directory. This is the location to which backup objects will be written. This is not required while adding CIFS share.

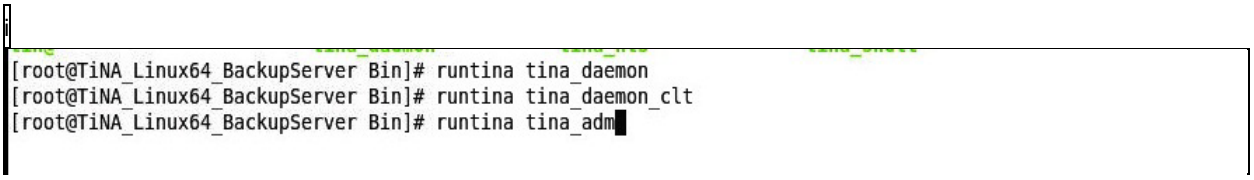
1 Mount the DR Series System NFS share onto the NFS share directory to which backup objects will be written in the ASG-TimeNavigator environment. For example:

```
mount –t nfs <ip address of DRXXXX>:/containers/sample
/mnt/TiNA_targetContainer
```

2 Verify the NFS share. One way is to use the Linux command "`cat /proc/mounts`". The rsize and wsize of the NFS share in the command output should be 512K.

D - Launching a Time Navigator administration console in Linux

Go to the **/Bin** directory location **/usr/Atempo/TimeNavigator/tina/Bin** on the Time Navigator Backup server. The Time Navigator *tina_daemon and tin_daemon_clt* must be started each time the platform starts, with the *root* user:



NOTE: The services/daemon must be running on the Linux Time Navigator backup server at all times. It is not possible to start a backup or to use a peripheral on a platform if the service or daemon is not running. The services/daemon must also be running on the Time Navigator Server; otherwise, the application stops. An X_Window graphical display is required on the Linux Time Navigator Backup server. Users must check that the environment variable DISPLAY is correctly defined for launching the tina_adm.