Setting Up the Dell™ DR Series System as a Backup Target on CA Arcserve

Dell Engineering
April 2015

A Dell Technical White Paper

Revisions

Date	Description
January 2014	Initial release
April 2015	Updated for DR Series system software release 3.2.

Table of contents

Executive summary

This paper provides information about how to set up the Dell DR Series system as a backup target for CA ARCserve R16.

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://www.dell.com/powervaultmanuals

Note: The DR Series system/CA ARCserve build version and screenshots used for this paper may vary slightly, depending on the version of the DR Series system/ CA ARCserve software version used.

1 Installing and configuring the DR Series system

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

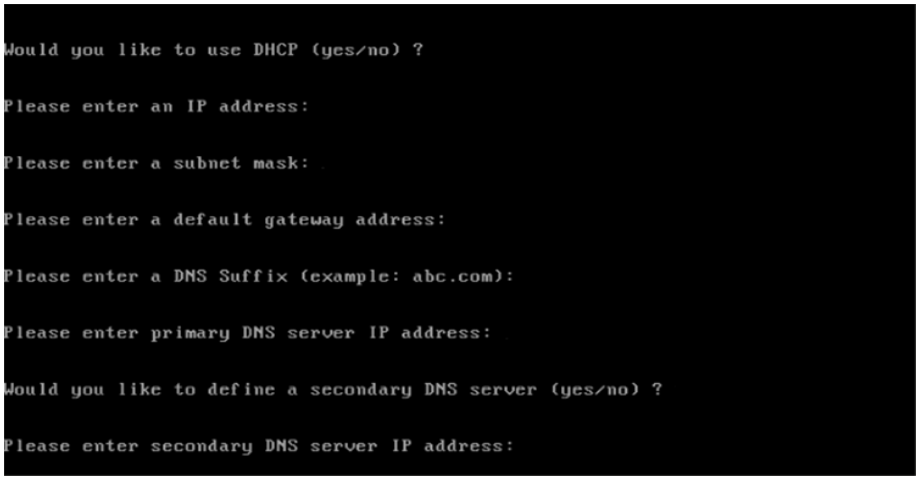
   For more information, refer to the following topics in the *Dell DR Series System Administrator Guide:* "**iDRAC Connection**", "**Logging in and Initializing the DR Series System**", and "**Accessing IDRAC6/Idrac7 Using RACADM.**"

2. Log on to iDRAC using the default address **192.168.0.120**, or the IP address assigned to the iDRAC interface. Use the user name and password: "**root/calvin**".

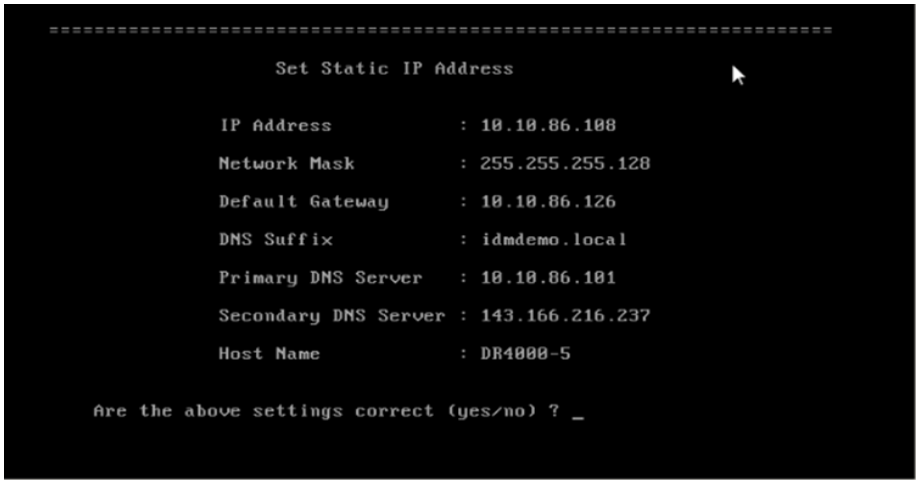
3. Launch the virtual console.

4. After the virtual console is open, log on to the system as the user **administrator** with the password: **St0r@ge!** (The "0" in the password is the numeral zero).

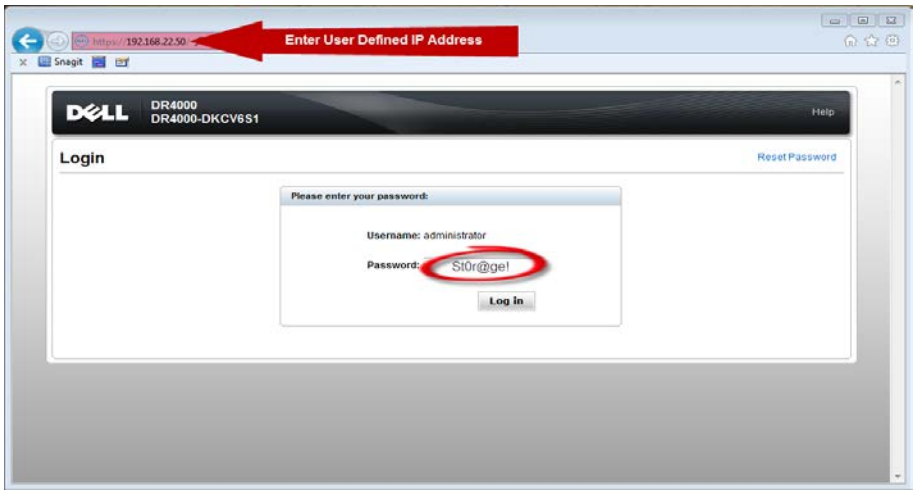
5. Set the user-defined networking preferences.



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



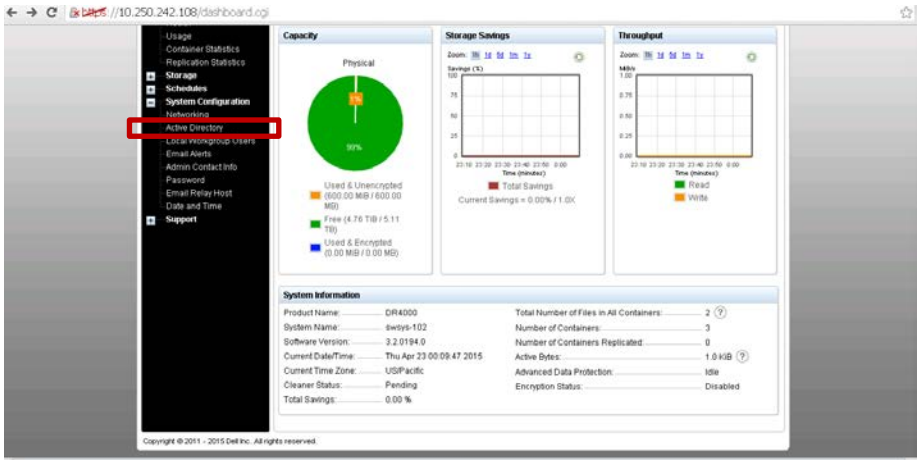
7. Log on to the DR Series system administrator console with the IP address you just provided for the DR Series system and with the username: **administrator** and password: **St0r@ge!** (The "0" in the password is the numeral zero.).



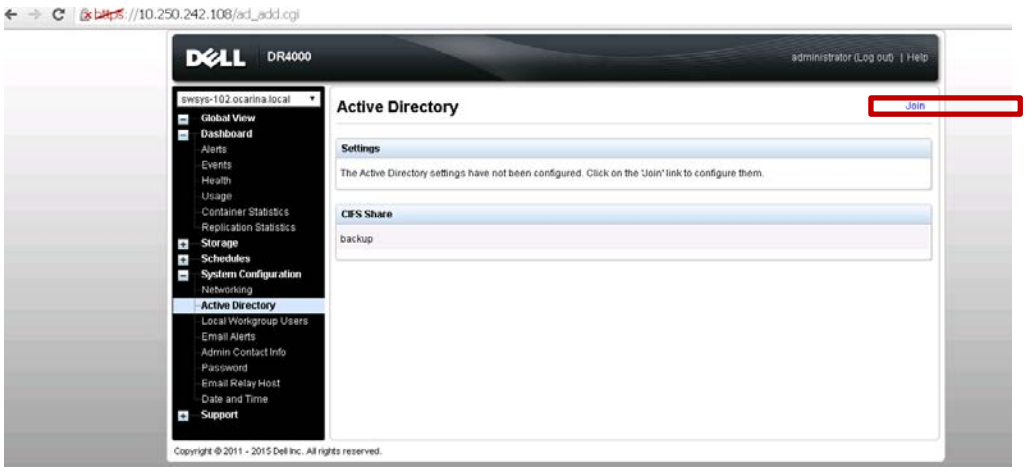
8. Join the DR Series system to Active Directory by completing the following steps.

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

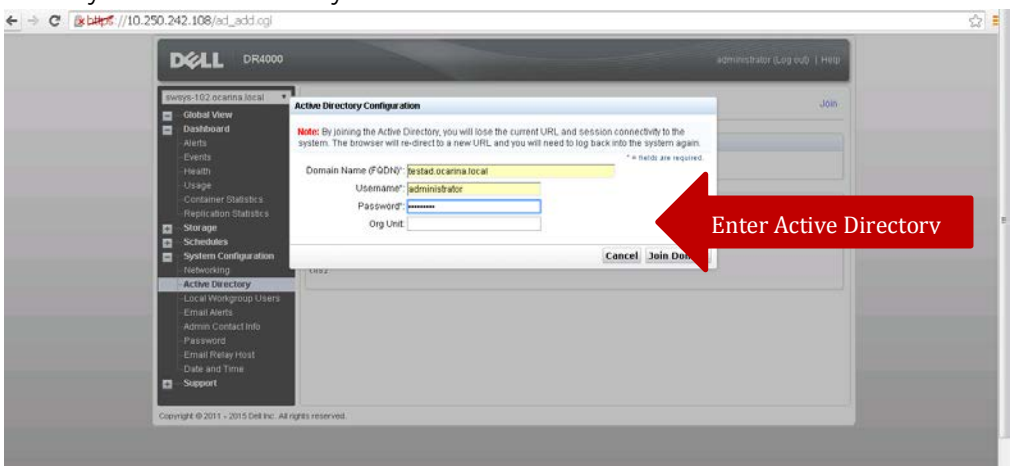
a. Select Active **Directory** from the left navigation area.



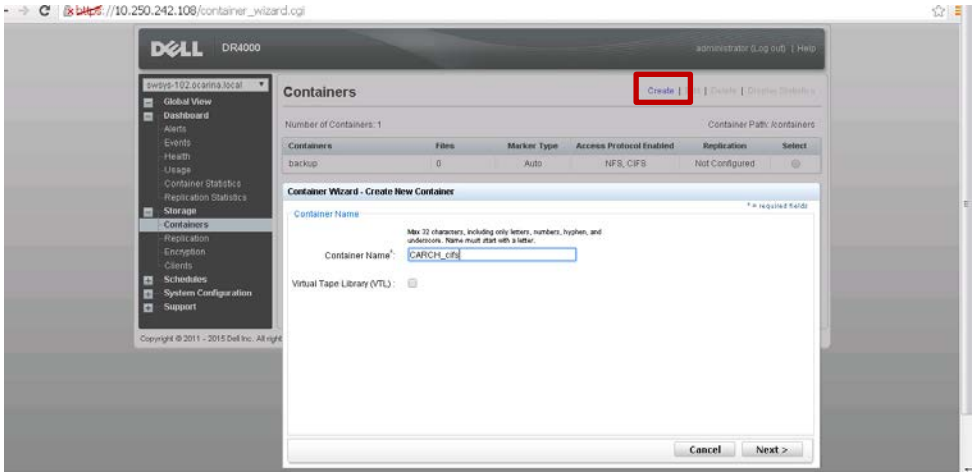
b. Click **Join** to configure Active Directory.



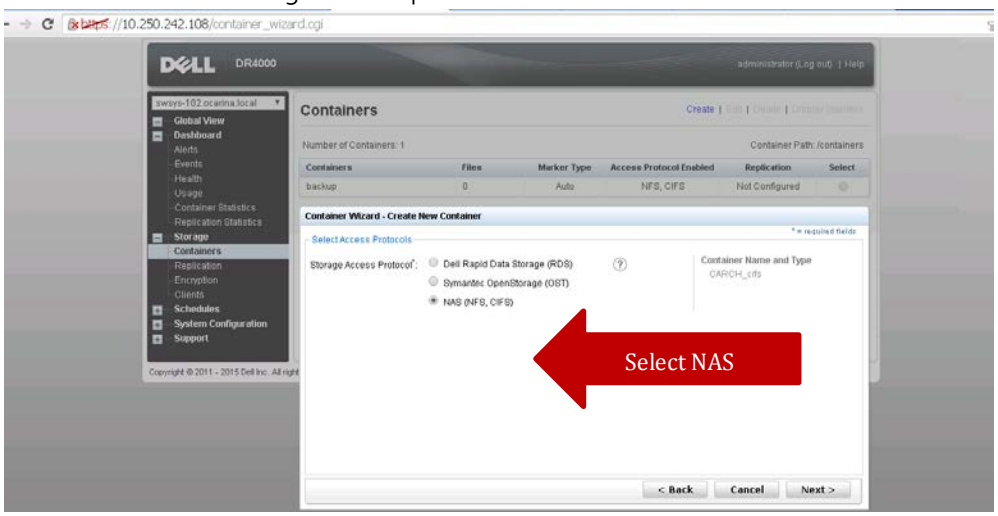
c. Enter your Active Directory credentials.



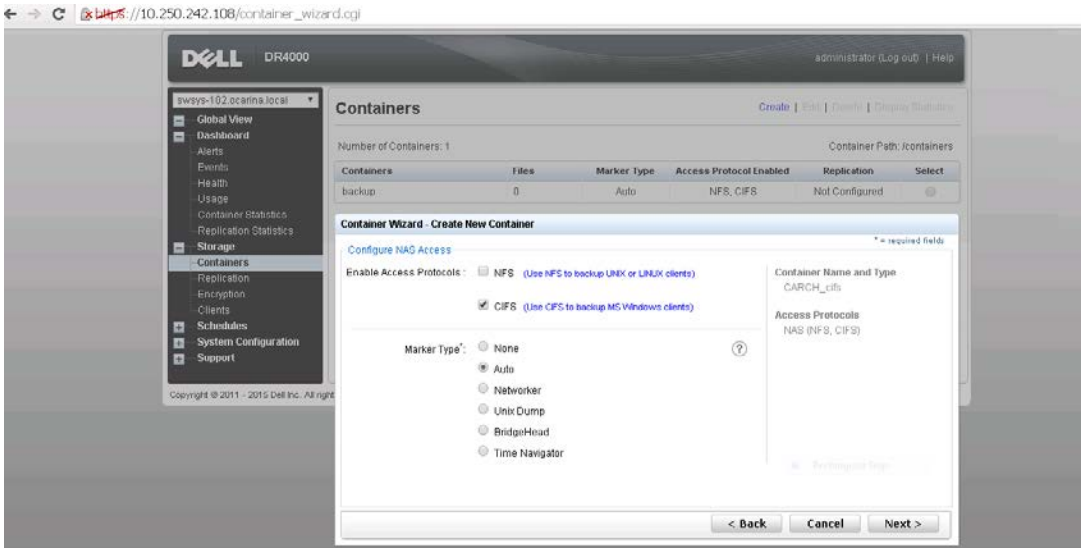
10. Create and mount the container. Select **Containers** in the left navigation area, and then click **Create** at the top of the page.
11. Enter a **Container Name** and click **Next**.



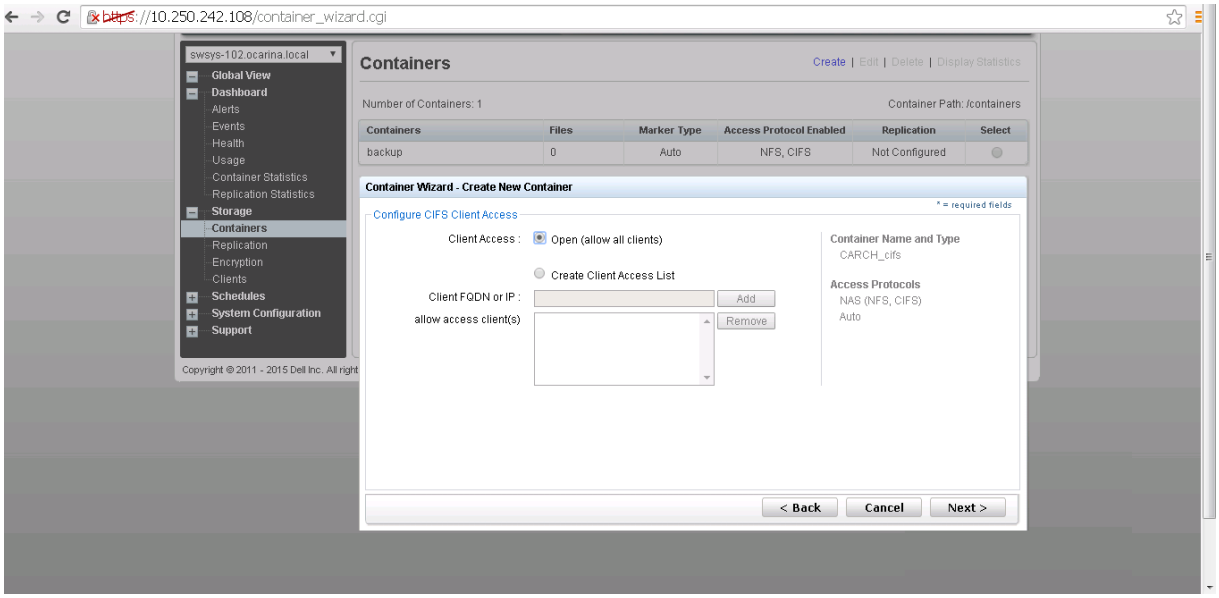
12. Select **NAS** as the storage access protocol. Click **Next**.



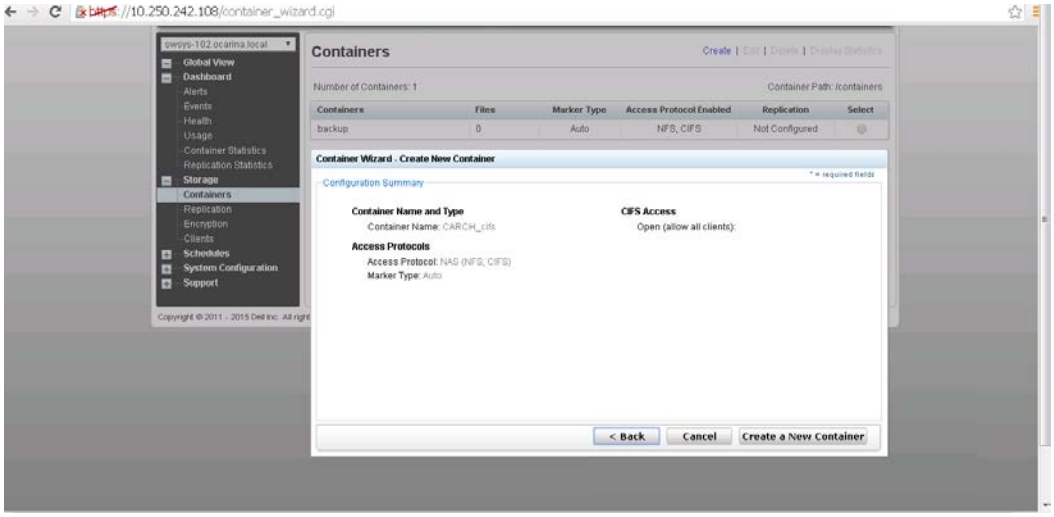
13. Enable the required protocol as **CIFS** and select the marker type as **Auto**. Click **Next**.



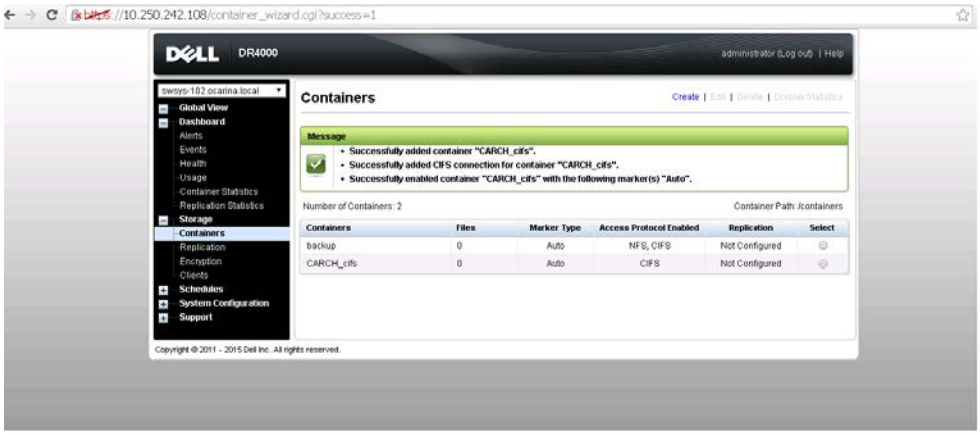
14. Select client access type and click **Next**.



Click **Create a New Container**.



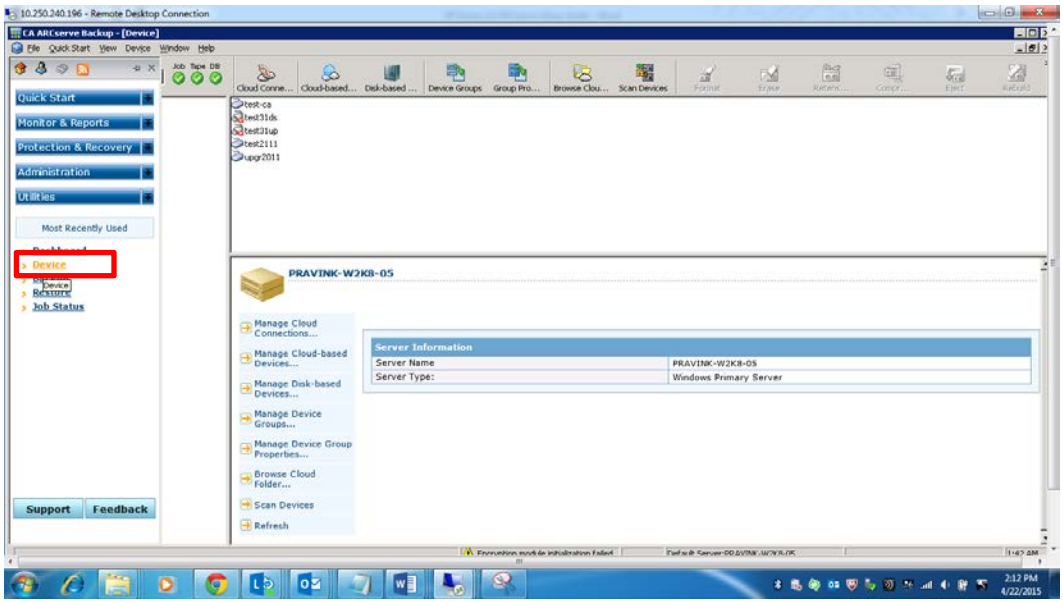
15. Confirm that the container is added.



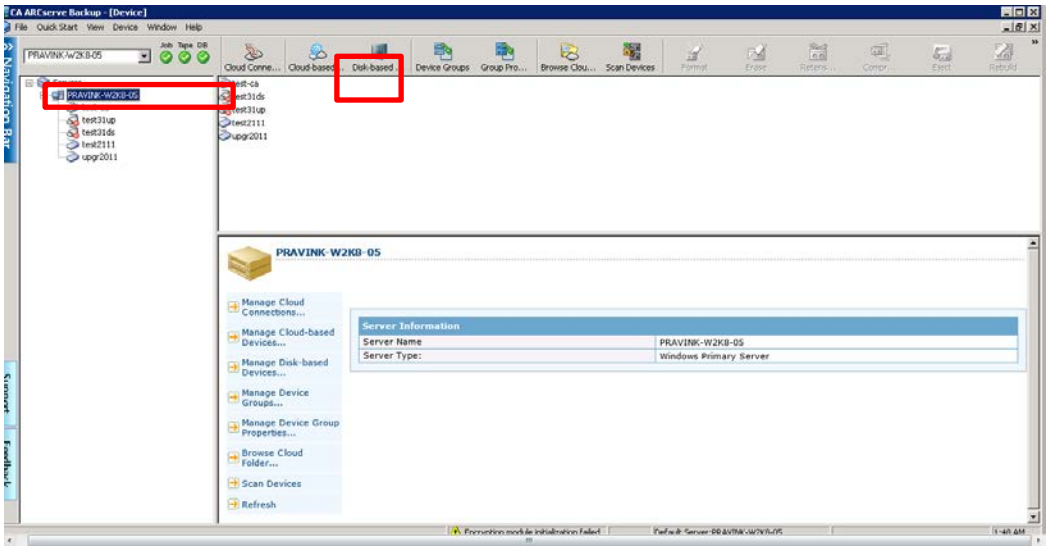
2 Creating a disk-based target device on CA ARCserve

2.1 For Windows environments

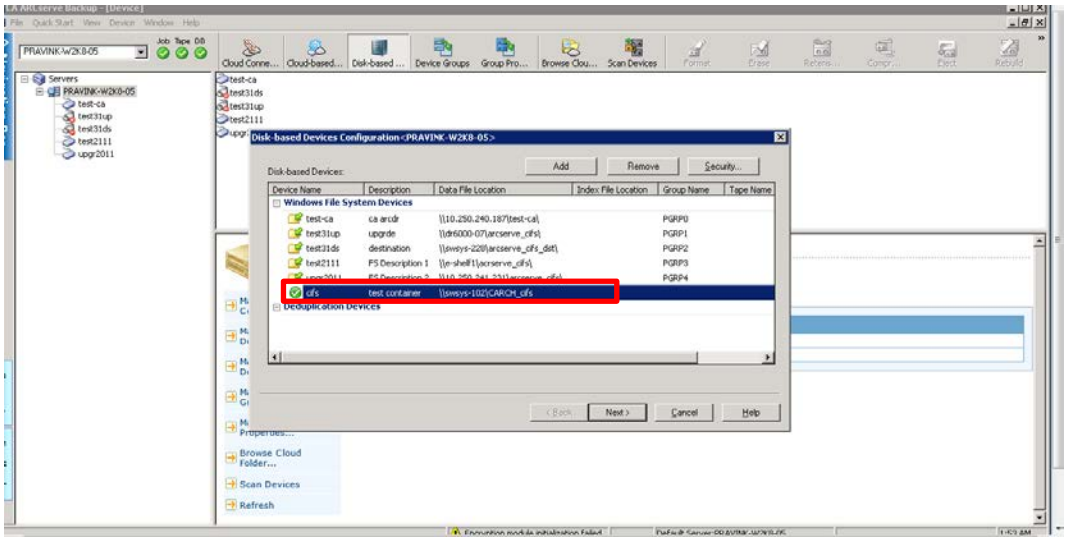
1. Open CA ARCserve Manager. In the Navigation pane, expand **Administration**, and click **Device**.



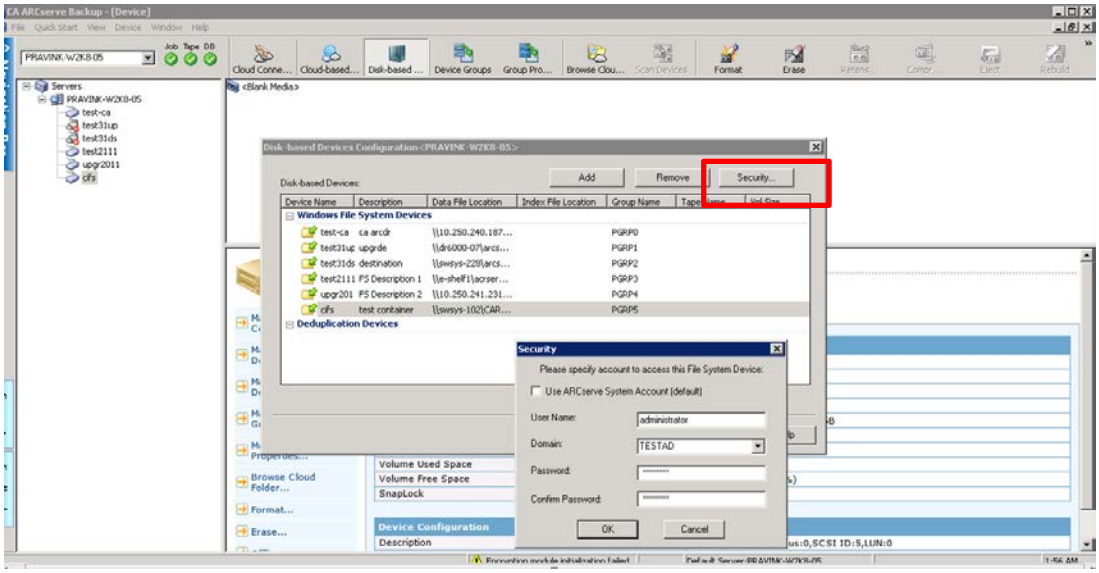
2. Select a **Server** and then click **Disk-Based Device**.



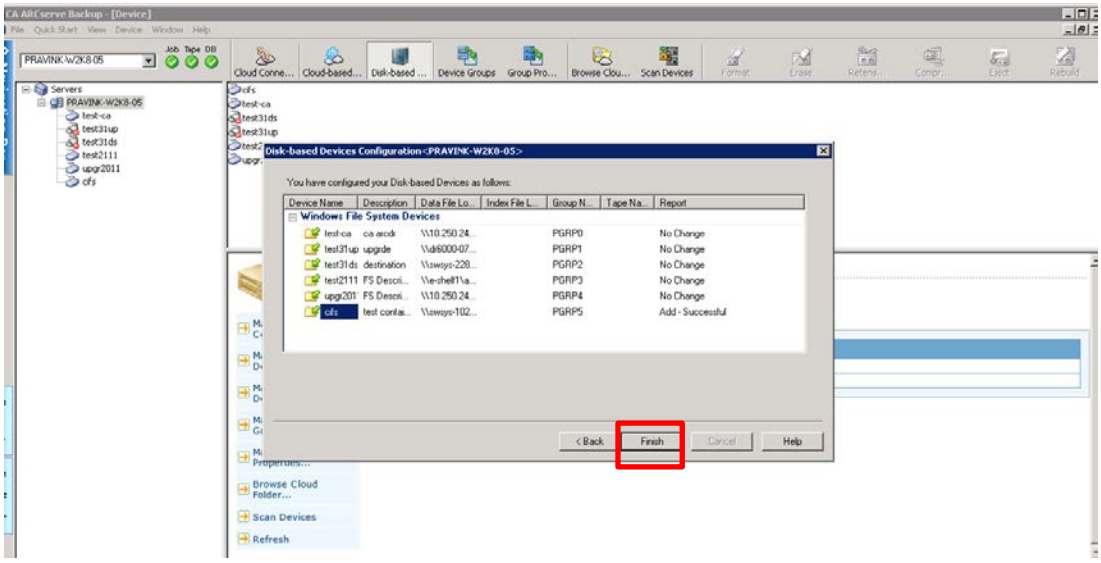
3. Select **Windows File System Devices** and then enter a Device name, Description, and the DR container share path as **Data File Location**.



4. Click **Security**, enter the credentials of the domain, and click **OK.**



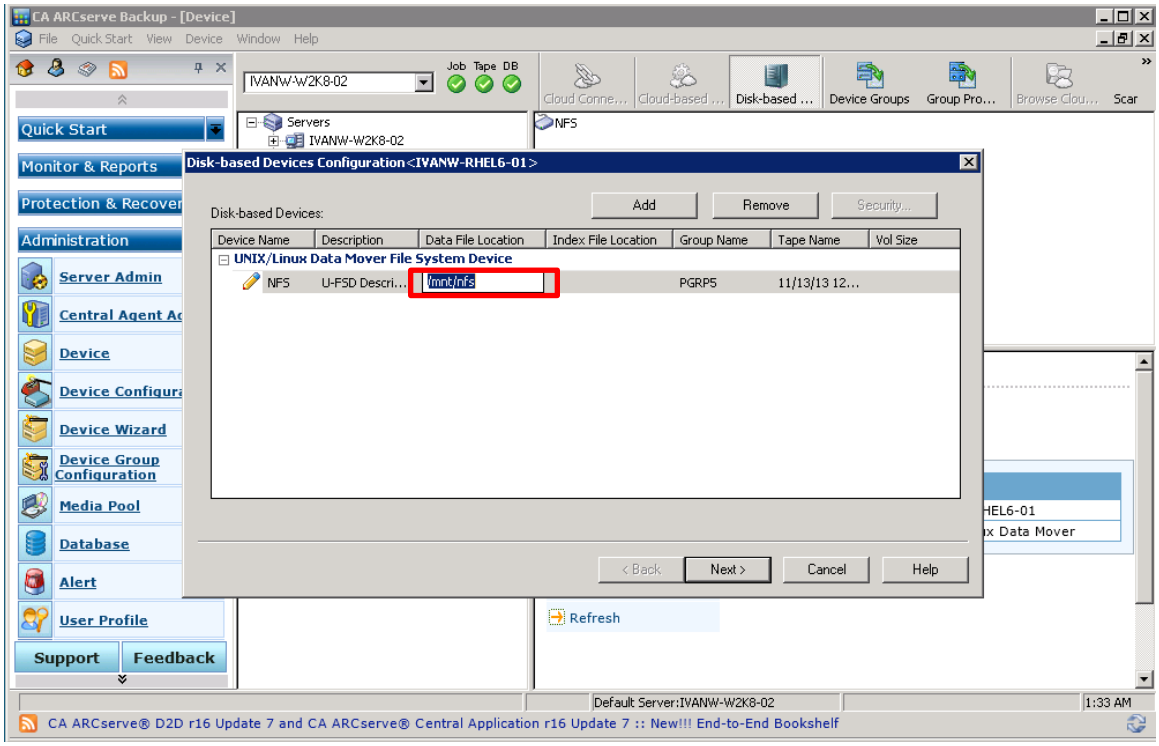
5. Click **Finish**.



2.3 For Unix/Linux environments

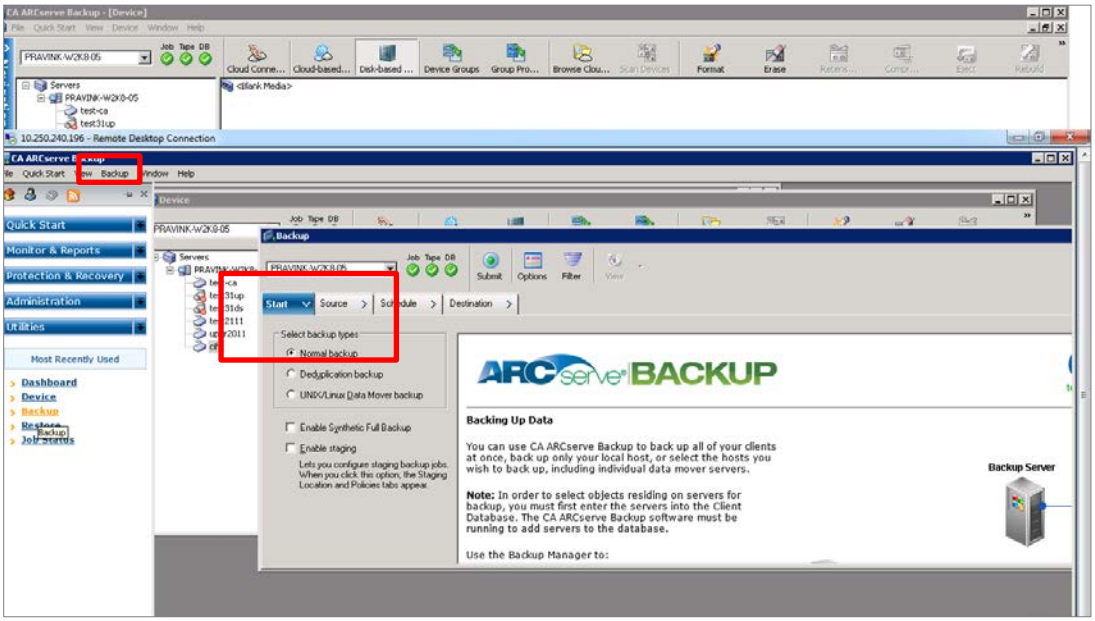
Note: Ensure that you can mount/verify the NFS share from the UNIX/Linux client system. See **Appendix A.1** for information about how to mount/verify the NFS share.

The procedure for the Unix/Linux environment is similar to the procedure for the Windows environment. The only difference is that DR container NFS export path is used instead of a UNC path, as described below, for **Data File Location**. For details, please refer to the preceding procedure for the Windows environment.

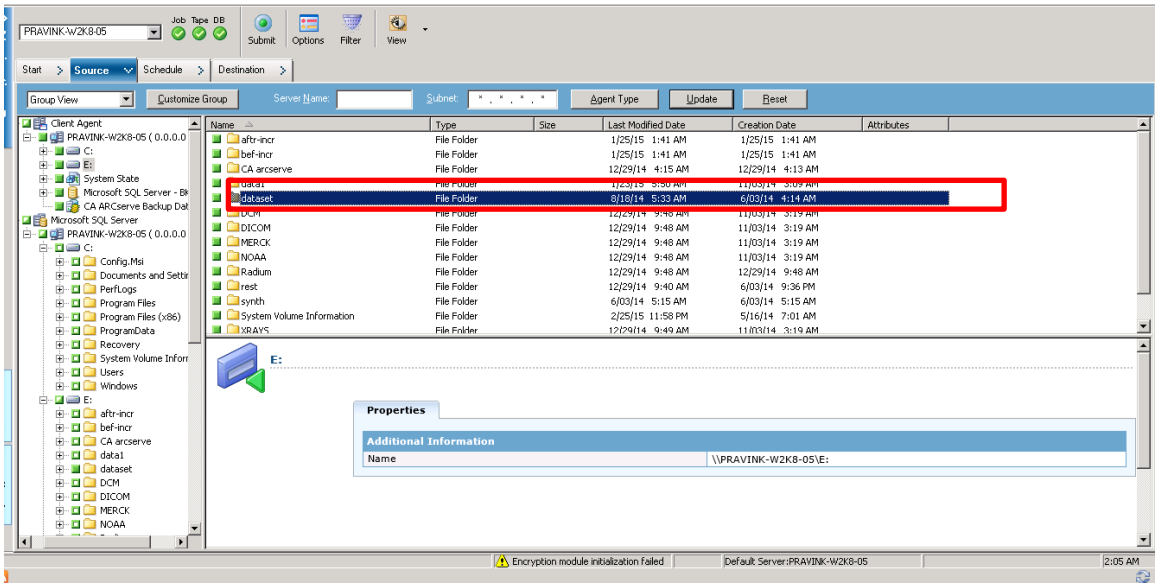


3 Creating a new backup job with the DR Series system as the target

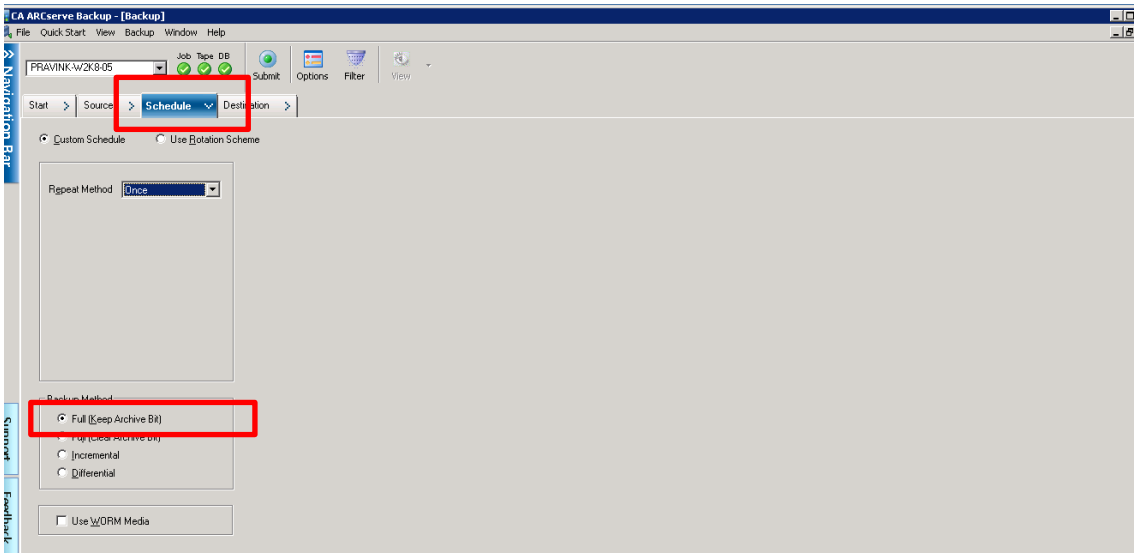
1. In the Navigation pane, click **Quick start** -> **Backup**. Then, in the right panel, on the **Start** tab set **Select backup types** as **Normal backup** for both CIFS and NFS backup.



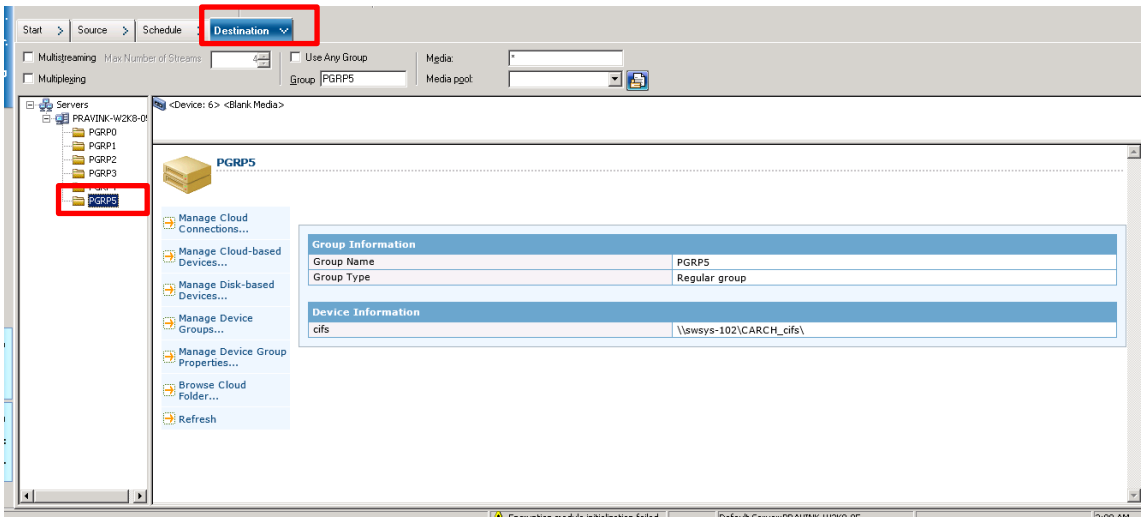
2. On the **Source** tab, select the backup source files.



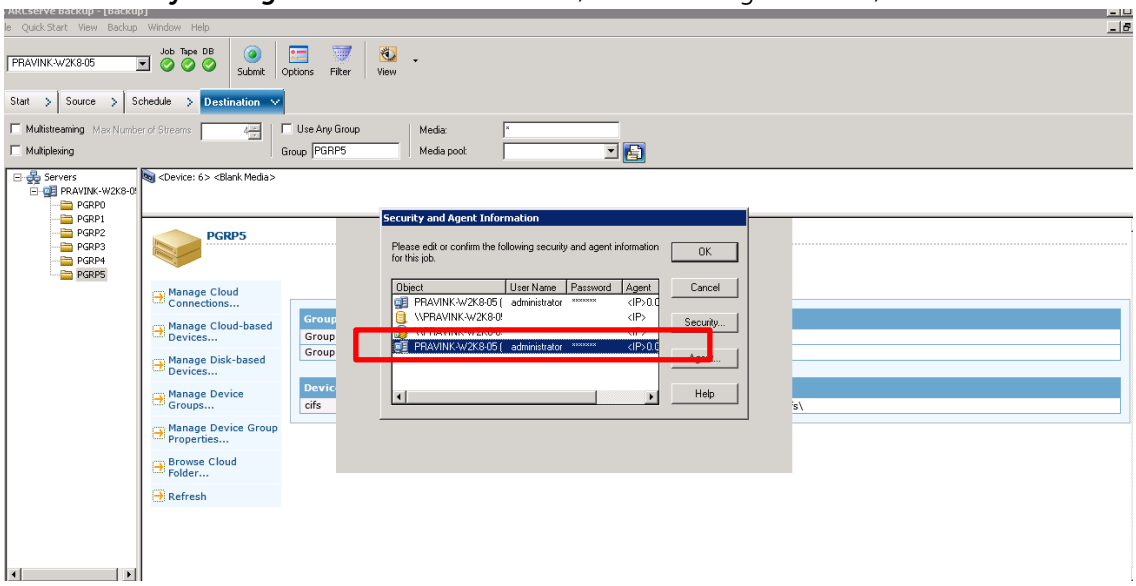
3. On the Schedule tab, set a Custom Schedule or Use Rotation Schema, and Backup Method.



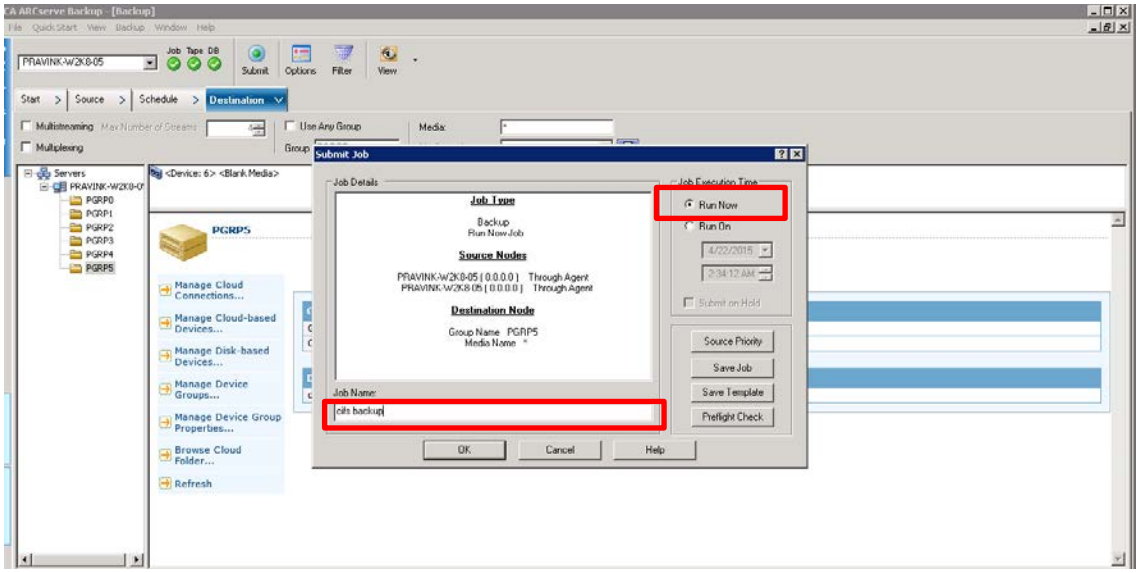
4. On the **Destination** tab, select destination device that is created on DR. Click **Submit**.



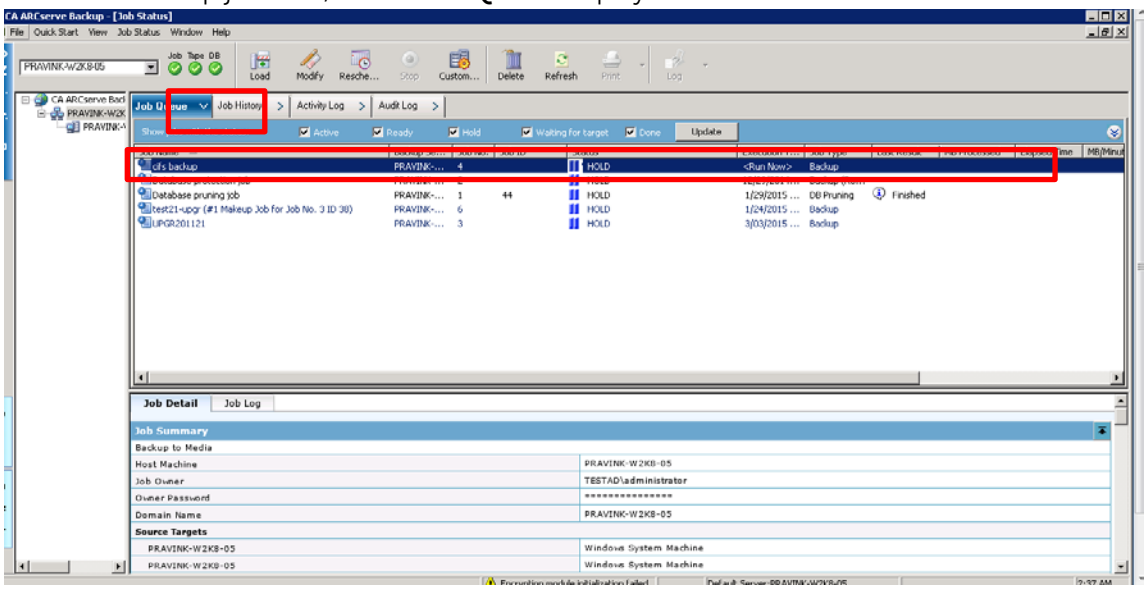
6. In the **Security and Agent Information** window, choose an agent server, and click **OK**.



7. Enter the backup **Job Name**, select **Job Execution Time**, and then click **OK.**



9. When the backup job runs, check **Job Queue** display in **Job Status** window.

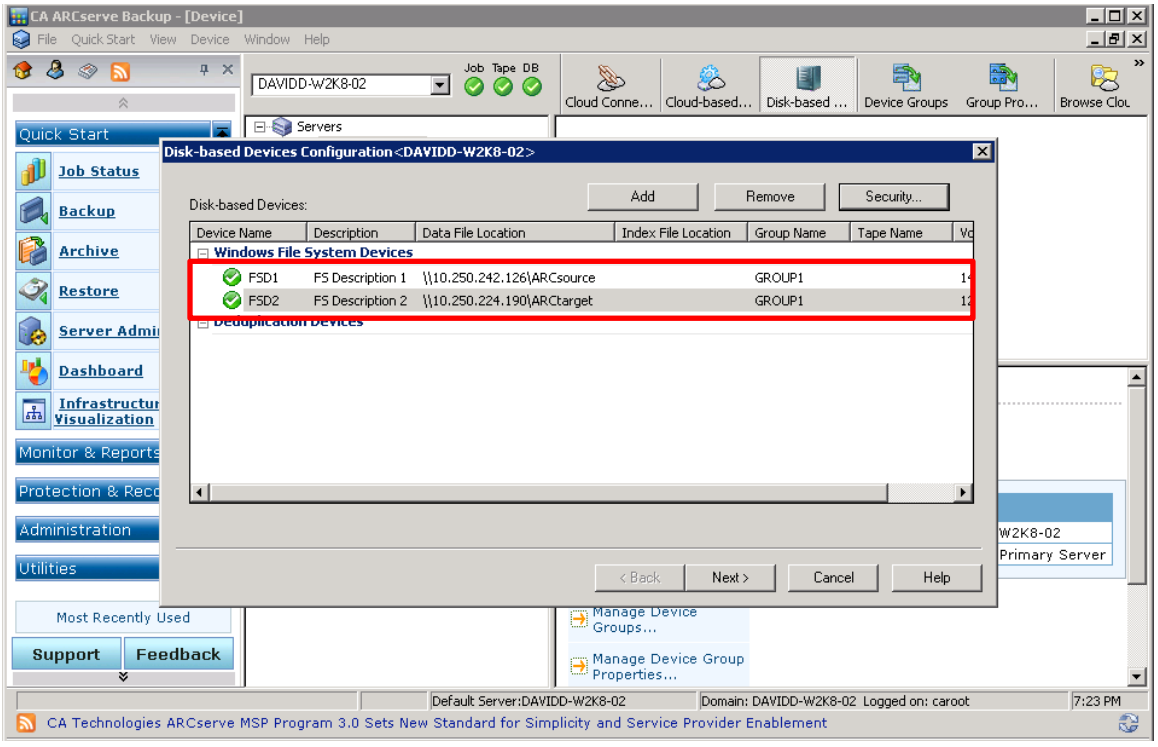


4 Setting up DR native replication and restore from replication target

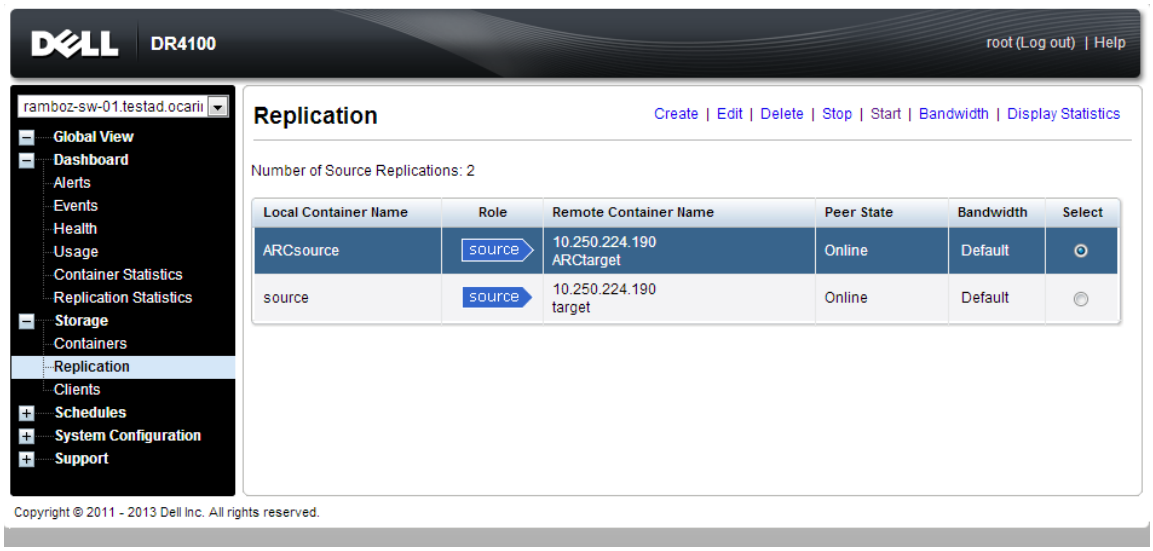
Note: The example used in this procedure assumes DR1 is the replication source DR Series system and DR2 is the replication target DR Series system. 'ARCsource' is the replication source container, and 'ARCtarget' is the replication target container.

4.1 Creating a DR native replication session

1. Create a CIFS container 'ARCsource' on DR1; create a second CIFS container 'ARCtarget' on DR2. For each of the containers, on the ARCServe server, configure Windows File System Devices within the same group.

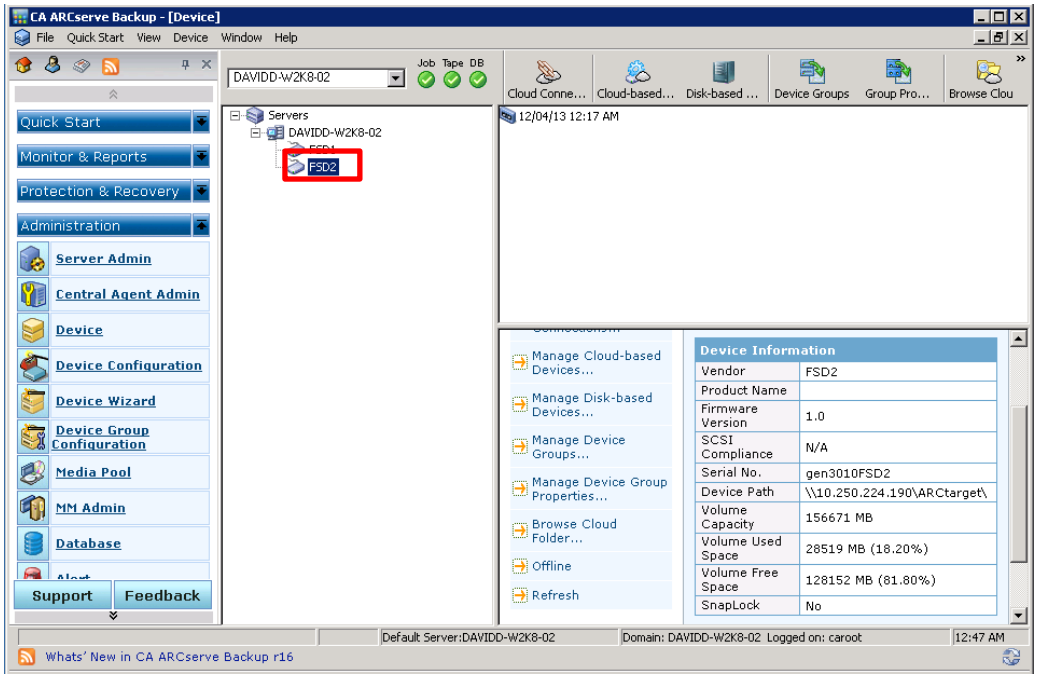


2. From DR1's GUI, on the **Replication** page, click **Create**. Set 'ARCsource' container as the replication source, and set DR2 'ARCtarget' container as the replication target. **Start** the replication session, or make sure the replication session is **Online**. You can **Stop** and/or **Delete** the replication whenever it is in INSYNC mode.

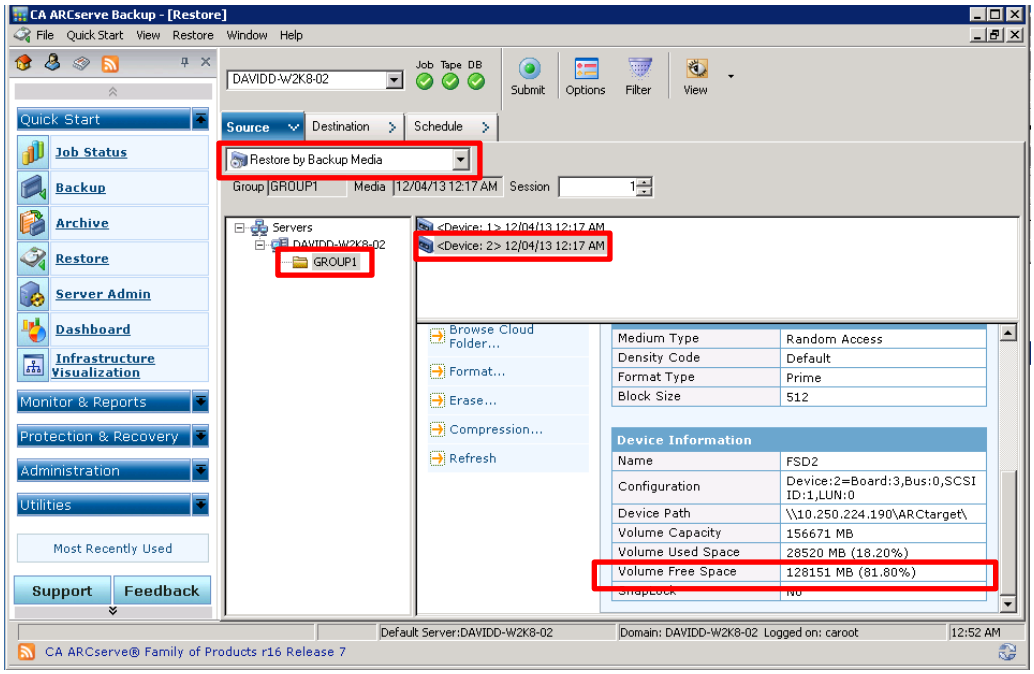


4.2 Restoring from the replication target

1. Restart ARCserve services. Go to **Administration** -> **Device**. Check and verify the target device.



2. Go to **Quick Start** -> **Restore**. Configure a restore job. Run the job to restore from the target device.

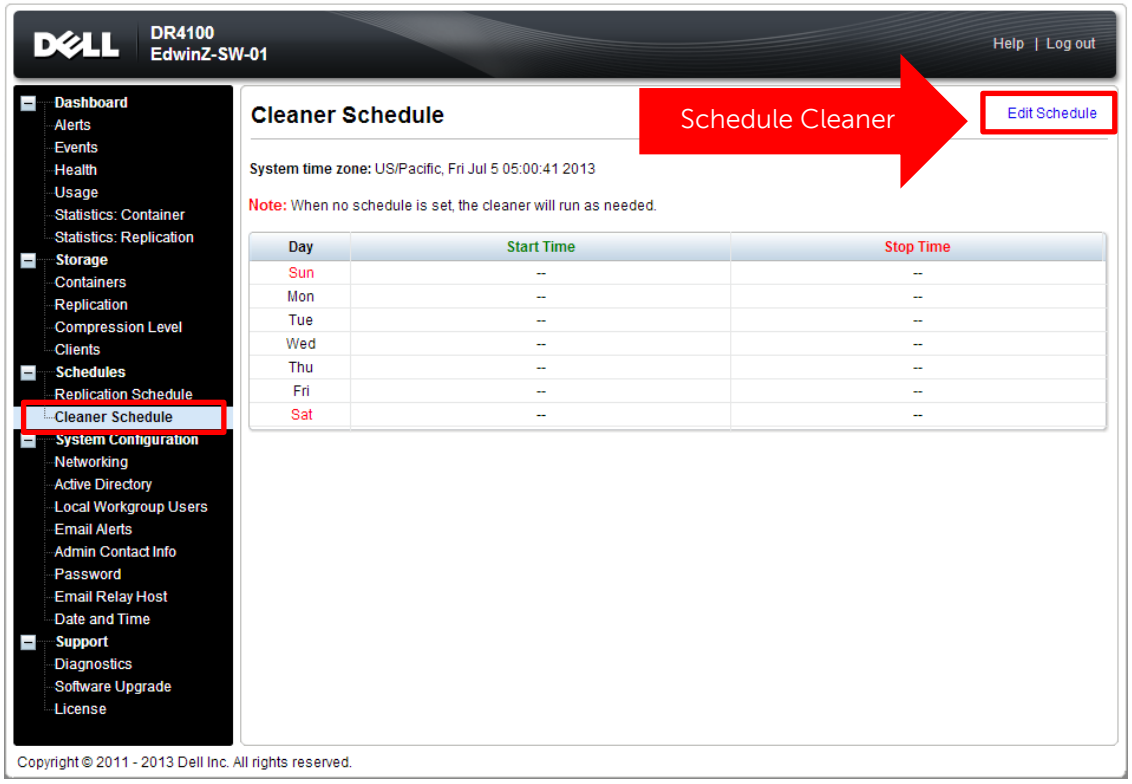


5 Setting up the DR Series system cleaner

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 screenshot 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 six hours per week when backups are not taking place, and generally after a backup job has completed.



6 Monitoring deduplication, compression, and performance

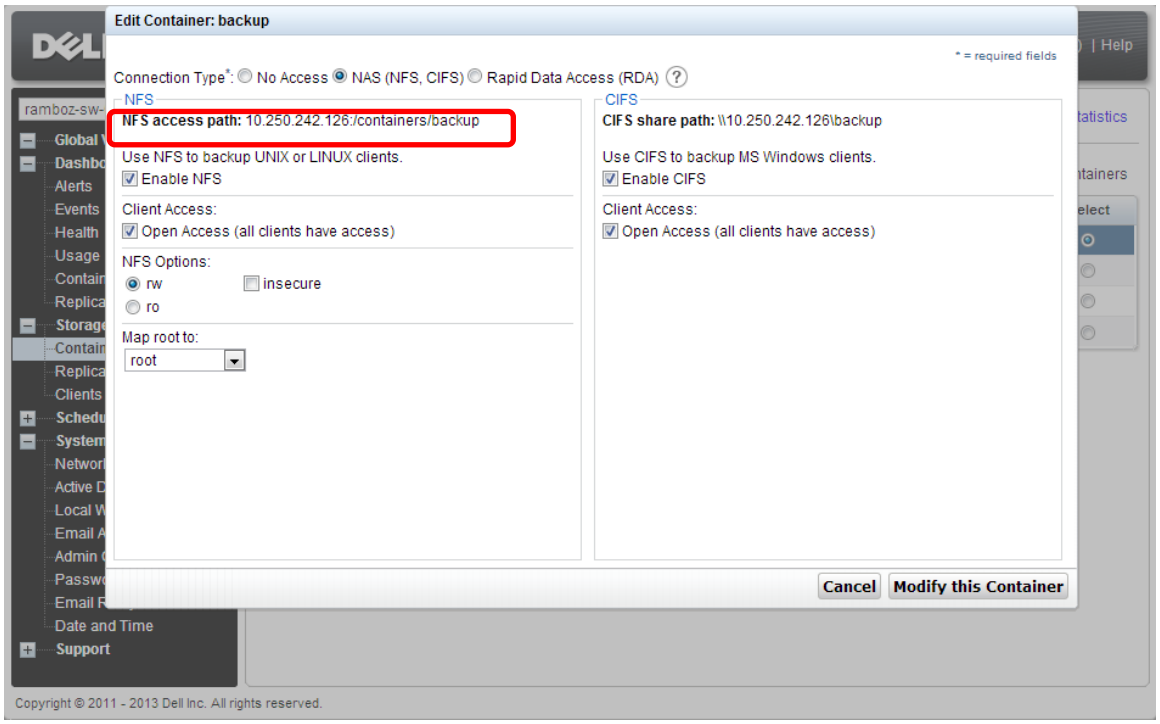
After backup jobs have run, the DR Series system tracks capacity, storage savings, and throughput on the DR Series system dashboard. This information is valuable in understanding the benefits of the DR Series system.

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 Creating a storage device for NFS

For NFS backup using CA ARCserve, 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 CA ARCserve. Check the NFS access path:



2. Mount the NFS access path in the Linux agent server.
   Example:

```
[root@IvanW-RHEL6-01 mnt]# mount 10.250.242.126:/containers/backup /mnt/nfs
```