



Setting Up the Dell™ DR Series System as an NFS Target on Amanda Enterprise 3.3.5

Dell Engineering
September 2015

Revisions

Date	Description
June 2015	Initial release
September 2015	Screenshot improvements and various editorial changes.

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2015 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever, without the express, written permission of Dell, Inc., is strictly forbidden. For more information, contact Dell.

PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: <http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector> Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, and PowerVault™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. 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. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.



Table of contents

Executive summary	4
1 Installing and configuring the DR Series system	5
2 Setting up for Unix/Linux environment backup	11
2.1 Creating the backup set.....	11
2.2 Creating the storage devices	12
3 Creating a new backup job with the DR Series system as the target	14
3.1 Defining the backup set.....	14
3.2 Defining where to back up.....	15
3.3 Staging a backup	17
3.4 Defining when to back up.....	17
3.5 Defining additional backup settings.....	18
3.6 Activating a backup.....	19
4 Creating a new restore job.....	21
4.1 Defining what to restore.....	21
4.2 Defining where to restore	22
4.3 Defining how to restore.....	23
4.4 Performing the restore.....	23
5 Setting up DR Series system native replication and restore from the replication target container.....	25
5.1 Building a replication relationship between DR Series systems.....	25
5.2 Restoring data from the target DR Series system	27
6 Setting up the DR Series system cleaner.....	30
7 Monitoring deduplication, compression and performance.....	31



Executive summary

This paper provides information about how to set up the Dell DR Series system as a backup target for Amanda Enterprise 3.3.5.

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>

For more information about Amanda, refer to the Amanda documentation at:

http://docs.zmanda.com/Project:Amanda_Enterprise_3.3/ZMC_Users_Manual

Note: The DR Series system/ Amanda build version and screenshots used in this document may vary slightly, depending on the version of the DR Series system/ Amanda Software version you are using.

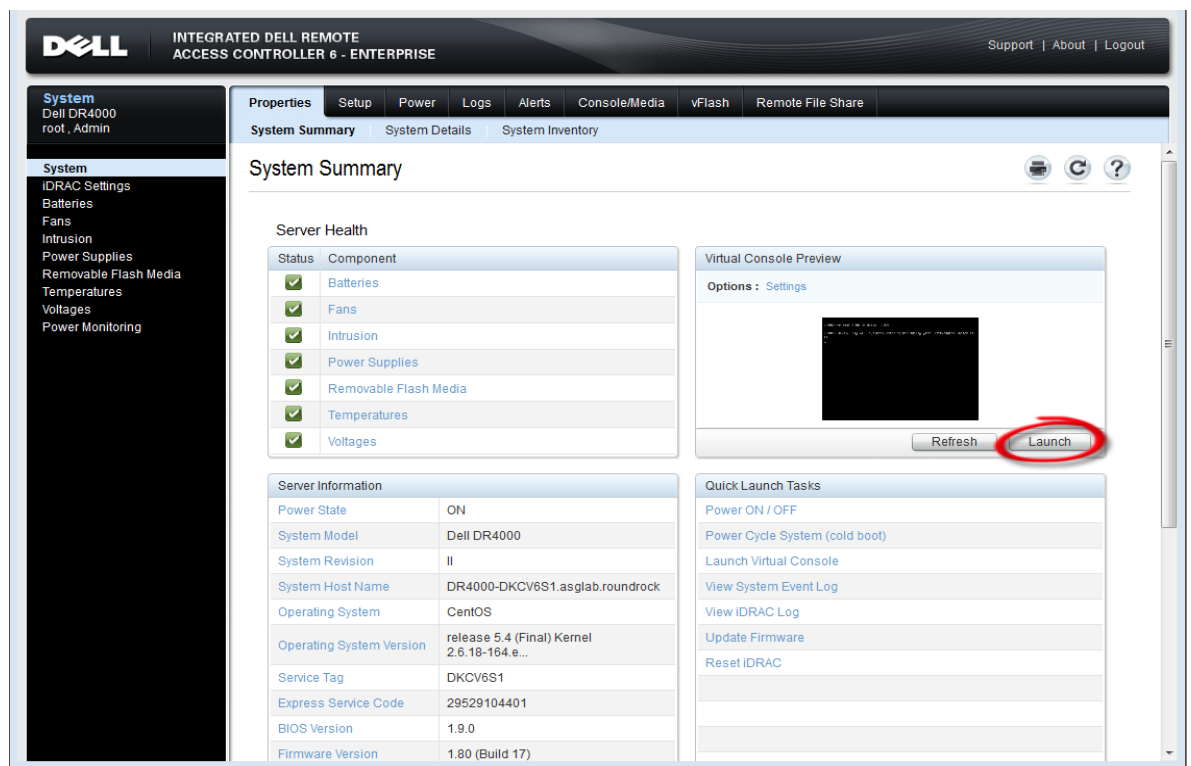


1 Installing and configuring the DR Series system

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

In the *Dell DR Series System Administrator Guide*, see the sections, "iDRAC Connection", "Logging in and Initializing the DR Series system", and "Accessing iDRAC6/iDRAC7 Using RACADM," for information about using the iDRAC connection and initializing the appliance.

2. Log on to iDRAC using the default address **192.168.0.120**, or the IP address that is assigned to the iDRAC interface by using the user name and password of "**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).

```
Debarina release 1 (EAR-1.00.00) Build: 32858
Kernel 2.6.18-164.el5 on an x86_64

localhost login: administrator
Password: St0r@ge!
```

5. Set the user-defined networking preferences.

```
Would you like to use DHCP (yes/no) ?
Please enter an IP address:
Please enter a subnet mask:
Please enter a default gateway address:
Please enter a DNS Suffix (example: abc.com):
Please enter primary DNS server IP address:
Would you like to define a secondary DNS server (yes/no) ?
Please enter secondary DNS server IP address:
```

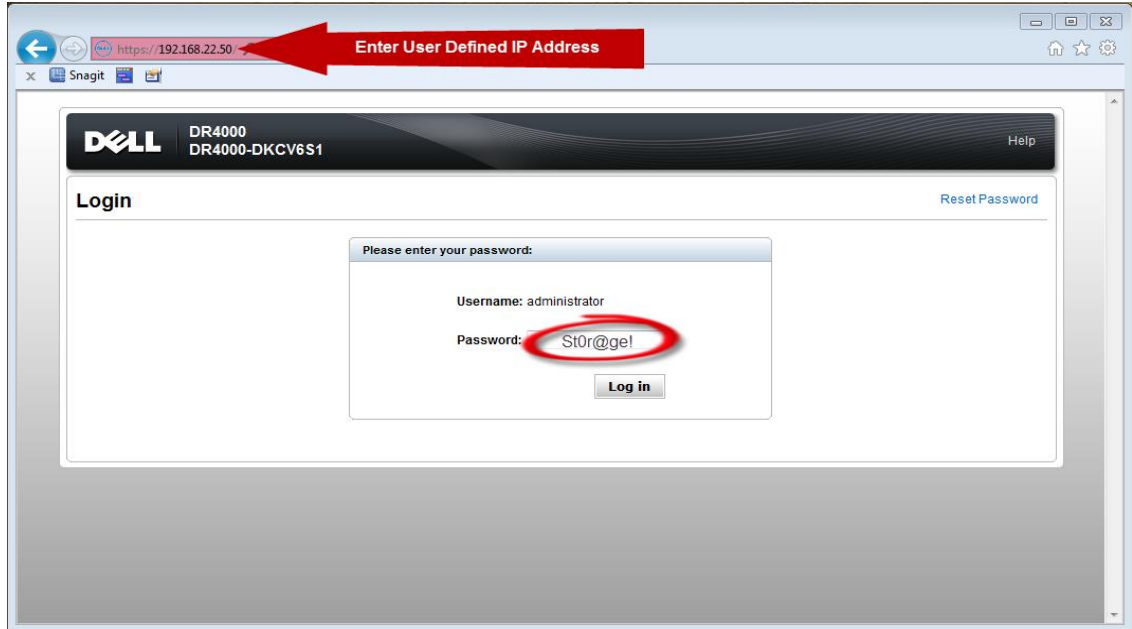
6. View the summary of preferences and confirm that it is correct.

```
=====
                        Set Static IP Address
=====
IP Address           : 10.10.86.108
Network Mask         : 255.255.255.128
Default Gateway      : 10.10.86.126
DNS Suffix           : idmdemo.local
Primary DNS Server   : 10.10.86.101
Secondary DNS Server : 143.166.216.237
Host Name            : DR4000-5

Are the above settings correct (yes/no) ? _
```



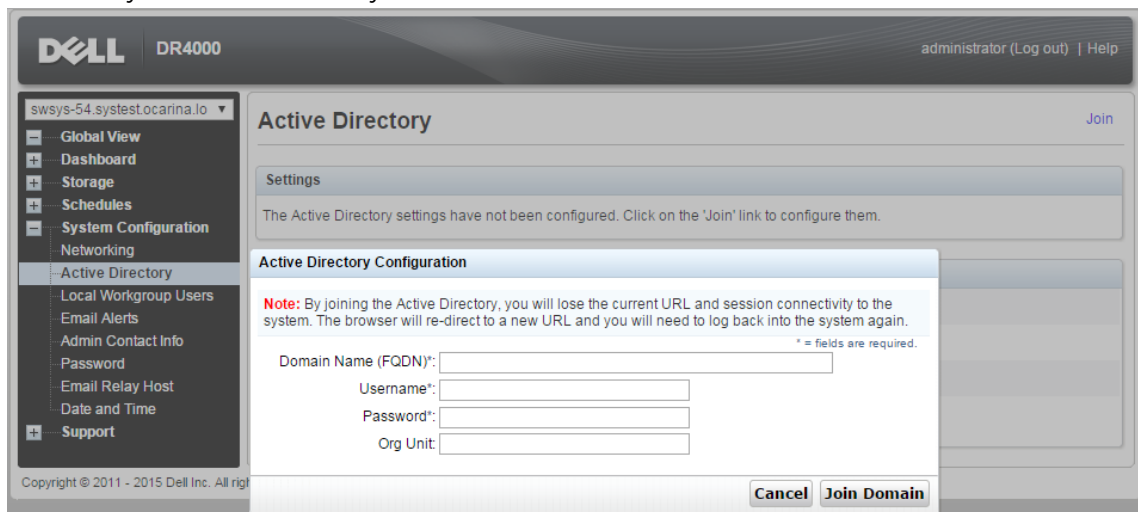
7. Log on to the DR Series system administrator console, using the IP address with username **administrator** and password **St0r@ge!** (The "0" in the password is the numeral zero).



8. 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. Under System Configuration, select **Active Directory** from the left navigation area of the DR Series system GUI.
- b. Enter your Active Directory credentials, and click **Join Domain**.



9. Create and mount the container by selecting **Containers** in the left navigation area, and then clicking the **Create** link at the top of the page.

The screenshot shows the Dell DR4000 web interface. The top navigation bar includes the Dell logo, 'DR4000', and 'administrator (Log out) | Help'. The left sidebar shows a navigation menu with 'Containers' selected. The main content area is titled 'Containers' and includes a 'Create' link, 'Edit', 'Delete', and 'Display Statistics' options. Below this, it shows 'Number of Containers: 8' and 'Container Path: /containers'. A table lists the containers:

Containers	Files	Marker Type	Access Protocol Enabled	Replication	Select
backup	5011	Auto	NFS, CIFS	Not Configured	<input type="radio"/>

10. Enter a container name and click **Next**.

The screenshot shows the 'Container Wizard - Create New Container' dialog box. It has a title bar and a close button. The main area contains the following fields and options:

- Container Name**: A text input field with the value 'sample'. Above the field is a note: 'Max 32 characters, including only letters, numbers, hyphen, and underscore. Name must start with a letter.'
- Virtual Tape Library (VTL)**: A checkbox that is currently unchecked.

At the bottom right of the dialog, there are two buttons: 'Cancel' and 'Next >'.



11. Select the protocol as **NAS (NFS, CIFS)** and then click **Next**.

Container Wizard - Create New Container

Select Access Protocols

Storage Access Protocol*: Dell Rapid Data Storage (RDS) Symantec OpenStorage (OST) NAS (NFS, CIFS)

Container Name and Type
sample

< Back Cancel Next >

12. Select **NFS** as the access protocol and the Marker Type as **Unix Dump**, and then click **Next**.

Edit Container: amandasavings

Configure NAS Access

Enable Access Protocols: NFS (Use NFS to backup UNIX or LINUX clients) CIFS (Use CIFS to backup MS Windows clients)

Marker Type*: None Auto Networker Unix Dump BridgeHead Time Navigator

Container Name and Type
amandasavings

Access Protocols
NAS (NFS, CIFS)

Cancel Next >

13. Configure the NFS client access settings and click **Next**.

The screenshot shows the 'Container Wizard - Create New Container' dialog box, specifically the 'Configure NFS Access' step. The dialog has a title bar with the text 'Container Wizard - Create New Container' and a small icon on the right. Below the title bar, the text 'Configure NFS Access' is displayed, followed by a small asterisk and the text '* = required fields'. The main content area is divided into several sections. On the left, under 'NFS Options *:', there are two radio buttons: 'Read Write Access' (which is selected) and 'Read Only Access'. To the right of these is a checked checkbox labeled 'Insecure'. Below this is a 'Map root to:' label followed by a dropdown menu showing '-select-'. A horizontal line separates this section from the 'Client Access:' section below. In the 'Client Access:' section, there are two radio buttons: 'Open (allow all clients)' (selected) and 'Create Client Access List'. Below this is a 'Client FQDN or IP:' label followed by a text input field and an 'Add' button. Below the input field is a list box labeled 'allow access client(s)' with an empty list and a 'Remove' button. On the right side of the dialog, there is a section titled 'Container Name and Type' with the text 'sample' below it. Below that is a section titled 'Access Protocols' with the text 'NAS (NFS, CIFS)' and 'Auto' below it. At the bottom of the dialog, there are three buttons: '< Back', 'Cancel', and 'Next >'. The 'Next >' button is highlighted, indicating it is the next step in the wizard.

14. Review the summary and then click **Create a New Container**.

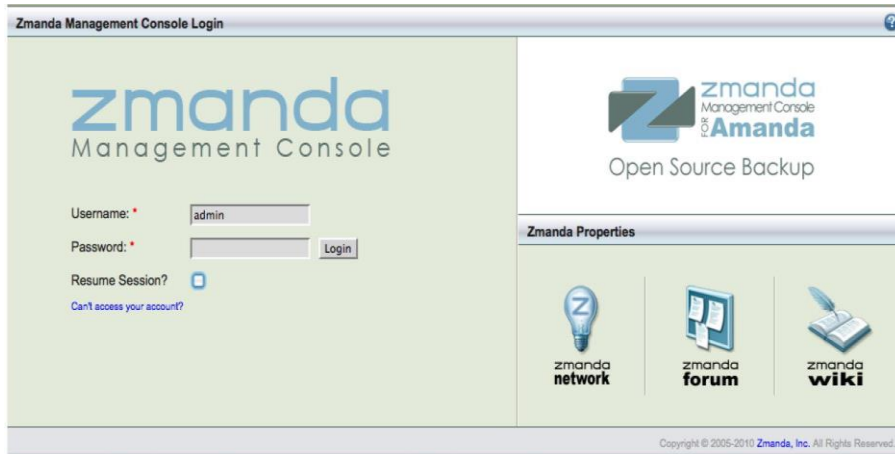
15. Confirm that the container is added.



2 Setting up for Unix/Linux environment backup

NOTE: Before you begin, ensure that you can mount/verify the NFS share from the UNIX/Linux client system. For more details, please refer to the Amanda documentation at: http://docs.zmanda.com/Project:Amanda_Enterprise_3.3/ZMC_Users_Manual

You can access the zmanda Management Console for Amanda in a Web browser by navigating to and logging on at the following location:
https://<host name of the Amanda server>:<port number>/



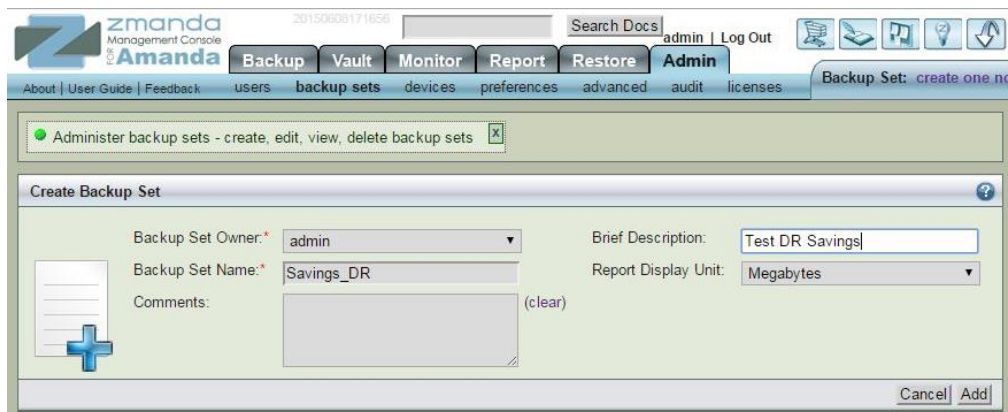
2.1 Creating the backup set

A backup set is a uniquely-named record of backup policies, including:

- Hosts, directories, and files to exclude.
- Backup target, which can be a tape device or disk (via holding disk or virtual tape)
- Type of backup to perform (such as, full or incremental); schedules are automatically configured.

Follow these steps to create a backup set.

1. On the Admin tab, click **backup sets**, enter the name and other details for the backup set as needed, and then click **Add**.



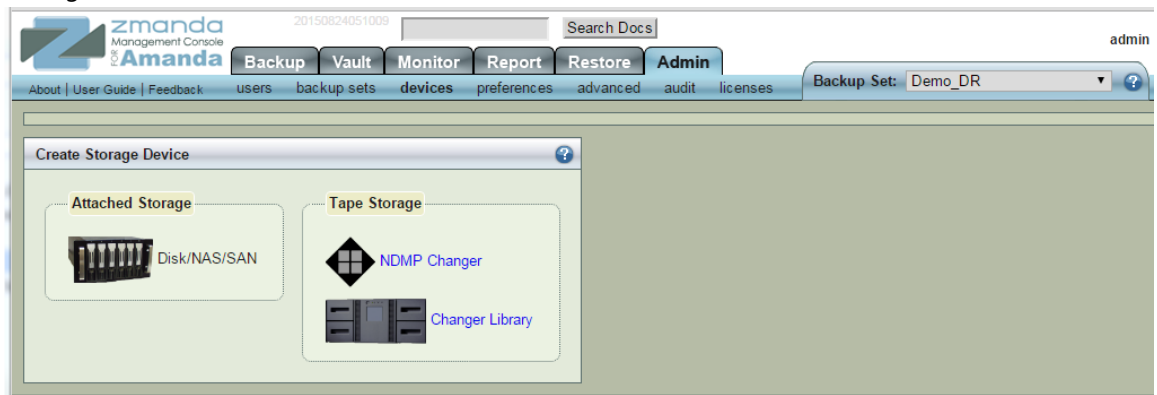
2.2 Creating the storage devices

Before you begin, log on to the Amanda server and add the DR Series system nfs mount. Run the following commands to use the DR Series system container as a backup target in the Amanda backup server:

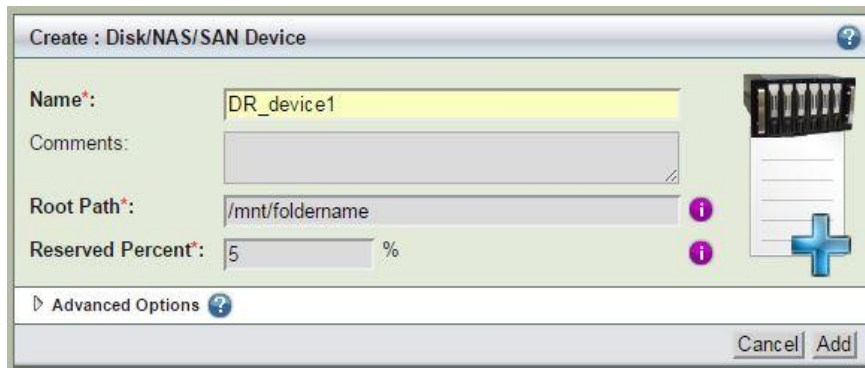
```
mkdir -p /mnt/DR_container_amanda
chmod -R 700 '/mnt/DR_container_amanda'
chown -R amandabackup:disk '/mnt/DR_container_amanda'
mount -t nfs <DR FQDN>:/containers/amanda-src /mnt/DR_container_amanda
```

Then, follow these steps to create the storage devices.

1. On the **Admin** tab, under Attached Storage, click **Disk/NAS/SAN** to add a DR container as a storage device.



2. Enter the device name and any comments, enter the DR Series container mount point path in the **Root Path** field, and then click **Add**.



After the storage devices are successfully added, you can see the storage device in the list of backup set devices.


zmanda Management Console for Amanda 20150824051009 Search Docs admin | Log Out

Backup Vault Monitor Report Restore Admin

About | User Guide | Feedback users backup sets devices preferences advanced audit licenses Backup Set: Demo_DR


Create Storage Device

Attached Storage




Disk/NAS/SAN

Tape Storage




NDMP Changer



Changer Library

View and edit backup set devices

All	Type	Device Name	Status	Path	Comments	Used With	Last Modified	By
<input checked="" type="checkbox"/>		DR_device1	OK	/mnt/DR_container_amanda		Demo_DR	2015-08-20 23:23:14	admin

Invert Selection | Refresh Table | Edit | Delete | List | Expert | Use

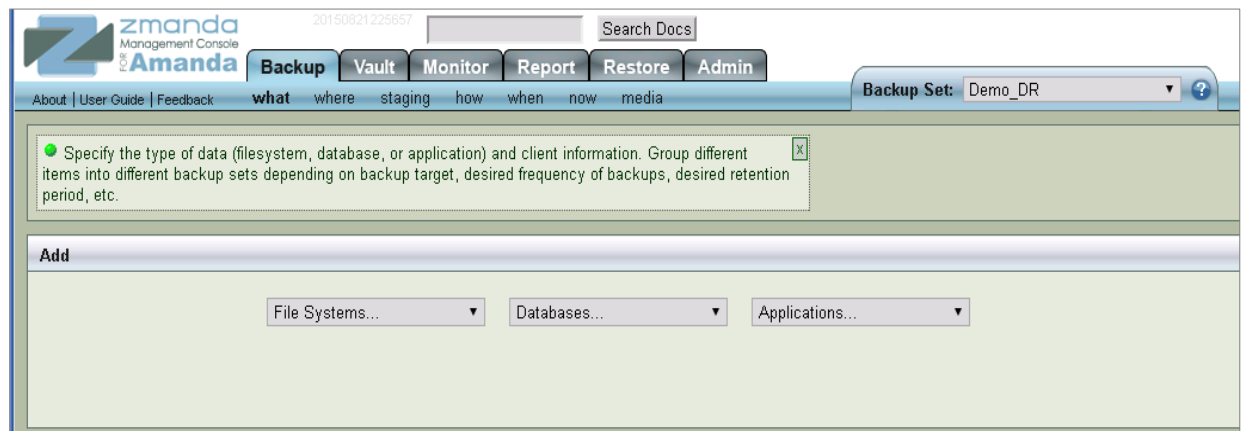


3 Creating a new backup job with the DR Series system as the target

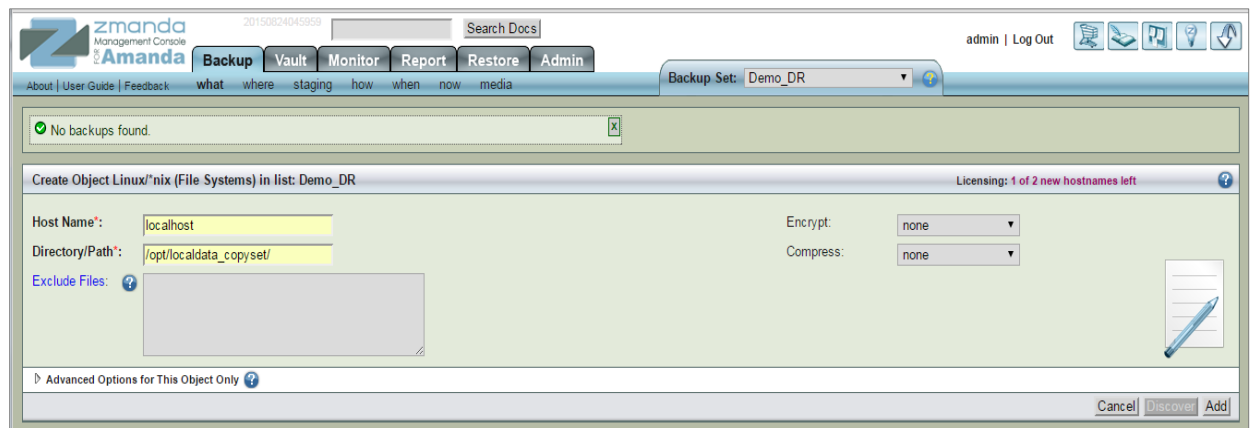
3.1 Defining the backup set

In the zmanda Management Console, *Backup what* defines the host system and directories to include in the backup set.

1. On the Backup tab, click **what**, and on the File Systems drop-down menu, select **Linux**.



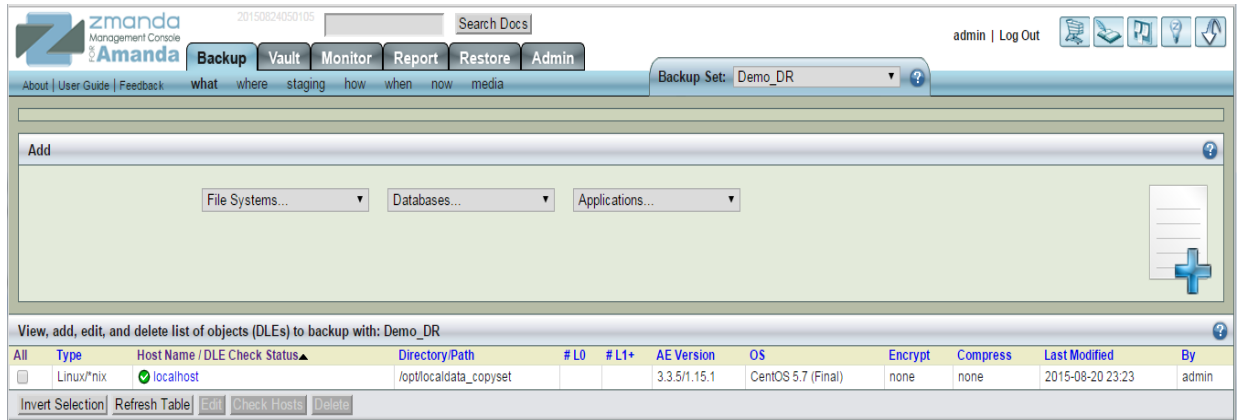
2. Enter the host name and location of the folder to back up, and then click **Add**.



Note: For better space savings, Dell recommends that the Encrypt and Compress options be set to **none**.



Upon successful addition, the data set will be listed at the bottom of the management console window.

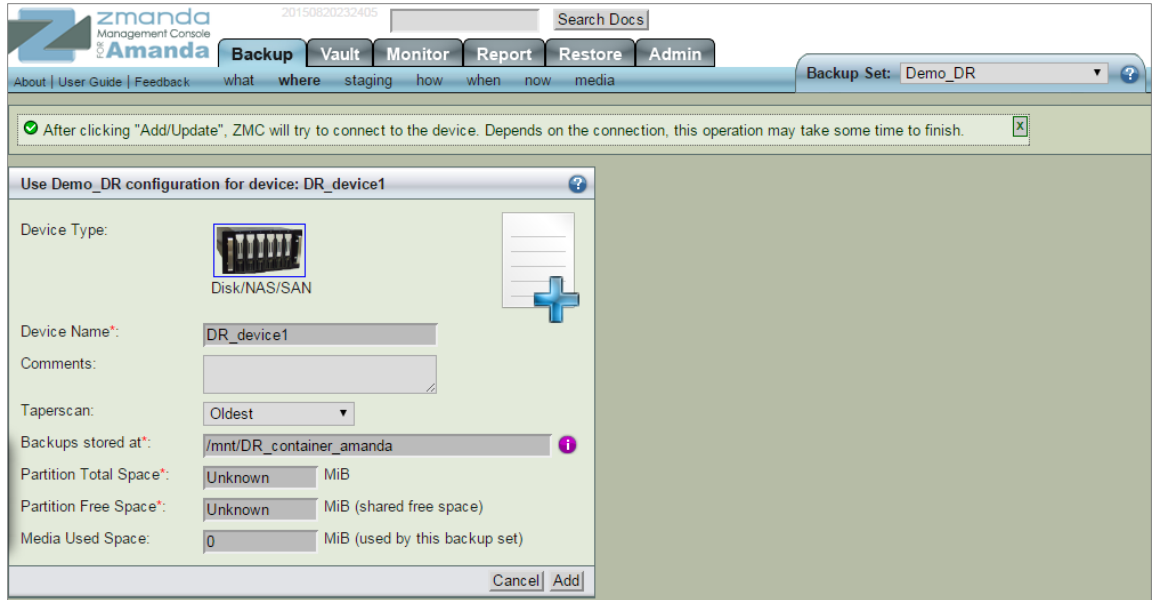


3.2 Defining where to back up

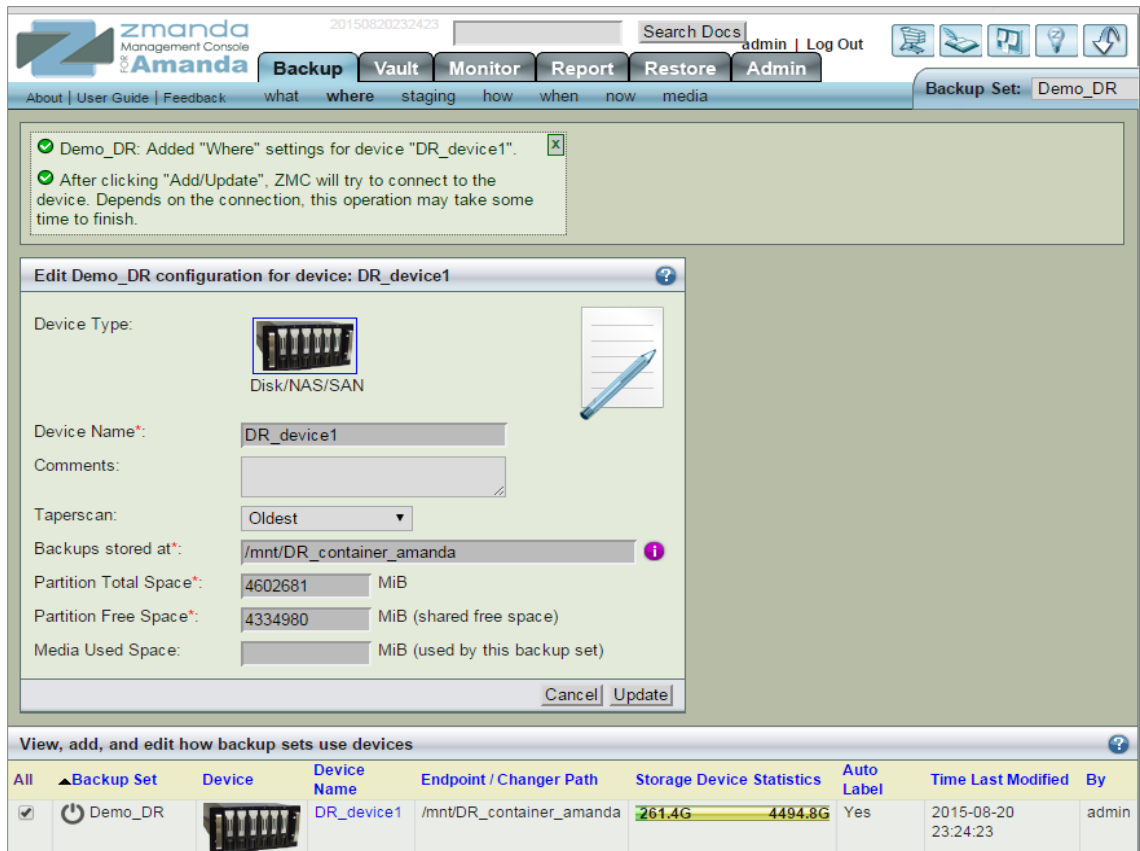
1. On the Backup tab in the zmanda Management Console for Amanda, click **where**.
2. Select the storage device that you created previously (that is, the DR Series system), and then click **Use**.



3. Click **Add**.



The DR Series system is added.



3.3 Staging a backup

In the zmanda Management Console you can define a staging area (an optional write-cache mechanism), which stores the backup image on the server's hard disk. Because backups can be written in parallel to the staging area, backups can be completed in smaller windows than if writing directly to the device.

To set up a staging configuration, on the Backup tab, click **staging**. You can change the default options as needed. For more information, see the Amanda documentation.

The screenshot shows the zmanda Management Console interface. At the top, there are navigation tabs: Backup, Vault, Monitor, Report, Restore, and Admin. The 'Backup' tab is selected. Below the navigation, there is a search bar and a 'Backup Set: Demo_DR' dropdown. The main content area is titled 'Edit interim staging areas for backup data.' and contains a dialog box for 'Edit Staging Configuration for: Demo_DR'. The dialog has several fields and options:

- Device Name*: DR_device1
- Auto Flush: automatically flush dumps from staging to media
- Staging Size Limit: Disabled (recomm) | 25 % of partition
- Reserved for root: 5 % (5% recommended; 10% for Solaris)
- Backup runs staged at: /var/lib/amanda/staging/Demo_DR
- Live Statistics: Partition total space*: 71434, Partition free space*: 13116, Partition used space*: 58318. A note states: "Space for each backup is pre-allocated before starting the backup, unless staging has been disabled."

At the bottom of the dialog, there are 'Cancel' and 'Update' buttons. Below the dialog, there is a table titled 'View and edit how backup sets use staging areas'.

All	Backup Set	Device	Flush	Directory	Staging Partition Statistics	Staging Usage Statistics	Time Last Modified	By
<input type="checkbox"/>	Demo_DR		yes	/var/lib/amanda/staging/Demo_DR	Disabled	Disabled	2015-08-20 23:24:23	admin

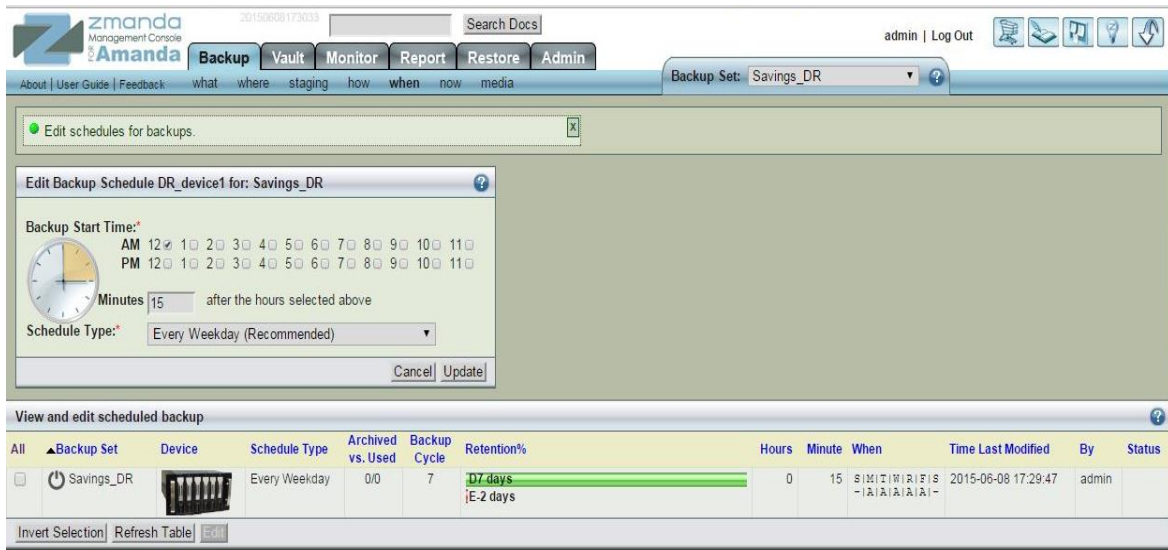
3.4 Defining when to back up

On the Backup tab, click **when** to define when to perform backups.

The Backup Schedule table shows the list of backup sets and backup schedules. This overall view of the backup schedules provides helpful information about how backup windows overlap and the number of backups running at any time.

- Edit the backup schedule as needed, and then click **Update**.

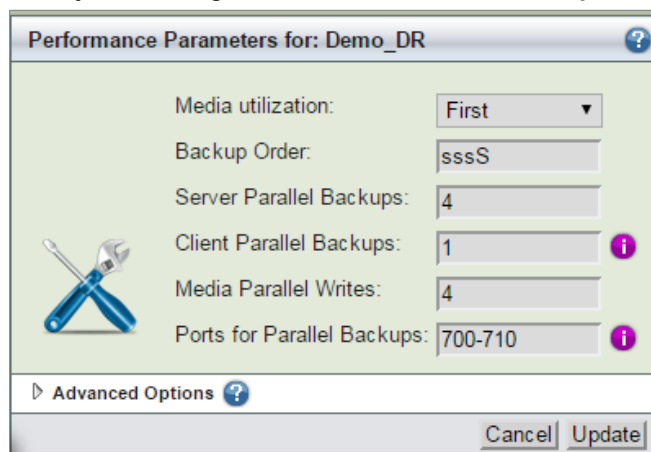




3.5 Defining additional backup settings

After you have defined what, where, and when for the backup set in the zmanda Management Console, you can use the **Backup How** page to define key internal parameters that control how the backup set will run after it has been activated. In most situations, the default settings are appropriate. Before adjusting these settings, advanced users should study the logs and reports of previous backups, and modify parameters for each backup set as needed.

1. On the Backup tab, click **how** to define backup settings.
2. Select a backup set at the bottom of the management console page.
3. Modify the settings as needed, and then click **Update**.



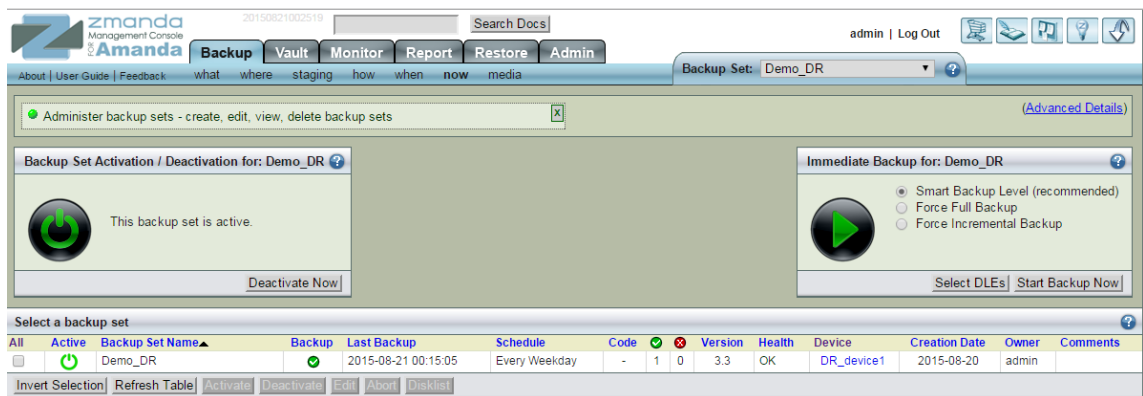
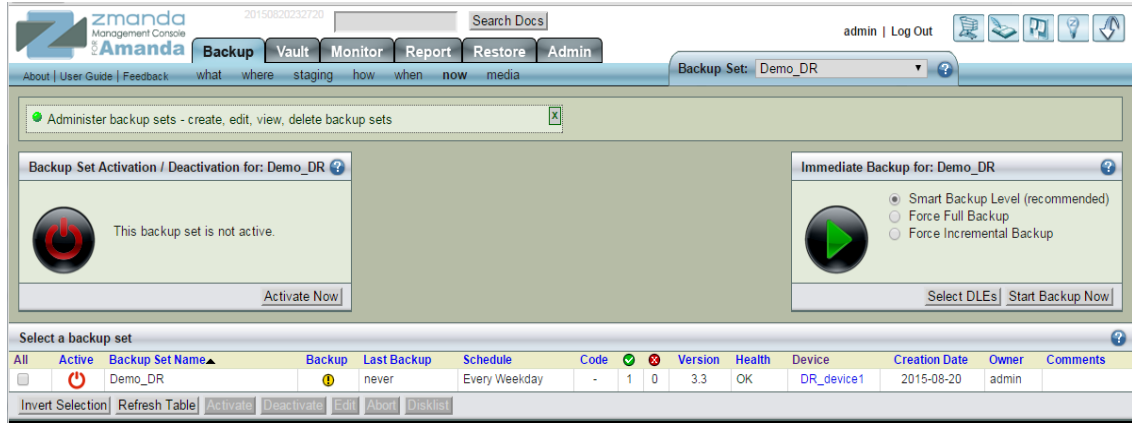
Note: For information about limits on the number of parallel streams supported or backups to the DR Series system, see the *Dell DR Series System Interoperability Guide*.



3.6 Activating a backup

A backup set must be activated for automatically-scheduled backups to execute. Backup sets must be activated individually.

1. On the Backup tab, click **now**.
2. In the Backup Set Activation section, click **Activate Now** to activate a backup set.
3. For immediate execution of a backup set, click **Start Backup Now** in the Immediate Backup section. You can execute an immediate backup at any time.



When an Immediate Backup is run, you can observe the progress of the backup in the **Monitor** page.



zmanda Management Console
 20150821002558 Search Docs admin | Log Out

Backup Vault Monitor Report Restore Admin

About | User Guide | Feedback backups alerts events Backup Set: Demo_DR

Refreshed at: 2015-08-21 00:25:58 (1 second refresh interval)

Monitor Backups

Show Backups: newer than 2 days

Which Backup Set?: ALL

Auto Refresh?: ...

Total Backups: 1

Backup Type	Hide?
Completed: 1	<input type="checkbox"/>
In Staging: 0	<input type="checkbox"/>
Failed: 0	<input type="checkbox"/>
In Progress: 0	<input type="checkbox"/>
Older Backups: 0	<input type="checkbox"/>
Details	<input type="checkbox"/>

Refresh

Legend: Backup States

Backup Level	Full	1	>=2
Success			
Warning			
Failure			
In Progress			

Timeline Monitor Chart

Date and Time	Backup Set	Type	Level	Host Name	Directory/Path	State	Clearing Staging Area	Checking Backup Plan	Transferring Backup to Server	Writing to Backup Media
2015-08-21 00:15	Demo_DR	Linux/nix		localhost	/opt/localdata_copysset				22032m dumping to tape (21870m done (99.27%)) (0:15:09)	22032m finished (0:20:06)

Refresh Table

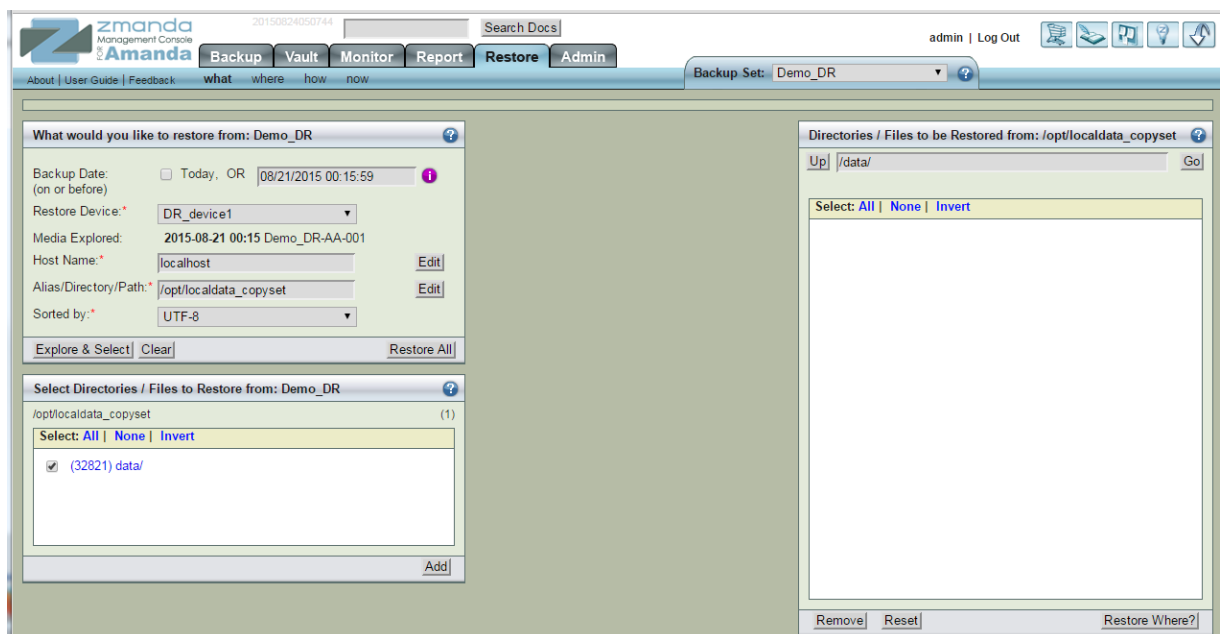


4 Creating a new restore job

4.1 Defining what to restore

On the Restore What page you can define the data to restore. You can select a single file or a single directory or all directories/files under a single directory.

1. On the Restore tab, click **what**.
2. In the **What would you like to restore from** pane, specify which backup image is to be restored.
3. Do one of the following:
 - Click the **Explore & Select** button to specify more detailed information about what is to be restored
 - Or, click the **Express Restore** button to restore the complete backup image.



4. If you clicked Explore & Select, select the directories/files to be restored by clicking left and right arrows. Selected entries appear in the right pane.

Note: The Explore process can take some time depending on the number of entries in the Amanda index for the Host Name and the Directory.

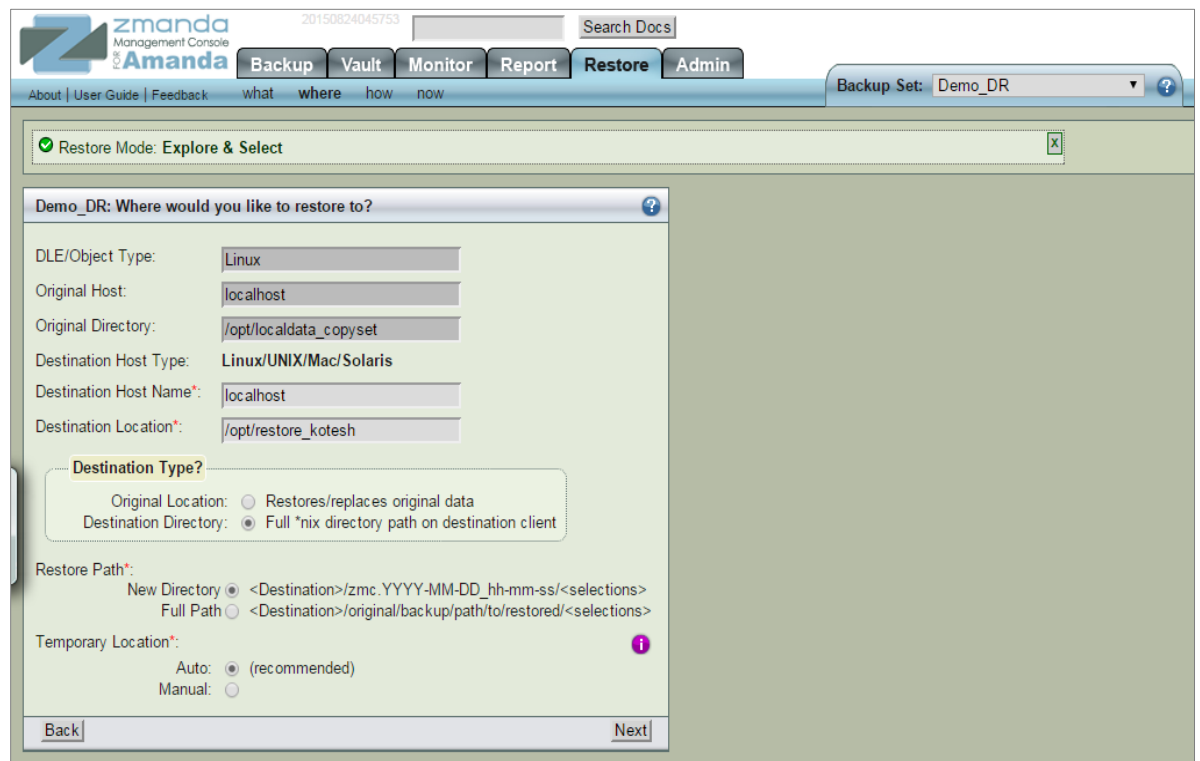
5. When you have selected all required directories/files, click **Restore Where**.

4.2 Defining where to restore

The Run Restore process is the last step in the recovery process. In the Run Restore page, you can review the restore options you have specified, start the actual restore process, and monitor progress.

Note: Only one restore process can be performed for a backup set in the zmanda Management Console.

1. On the Restore tab, click **where**.
The Restore From, Restore To, and Tapes Needed panels provide information about the restore job. Make sure the required tapes are in the tape changer (in the slots reserved for the backup set) if the restore is from a tape.
2. Enter information for the Destination Host Name, Destination Location, and select the other restore settings and then click **Next**.



The screenshot shows the zmanda Management Console interface. The top navigation bar includes 'Backup', 'Vault', 'Monitor', 'Report', 'Restore', and 'Admin'. The 'Restore' tab is active, and the 'where' sub-tab is selected. The main content area displays a dialog box titled 'Demo_DR: Where would you like to restore to?'. The dialog contains the following fields and options:

- DLE/Object Type: Linux
- Original Host: localhost
- Original Directory: /opt/localdata_copysset
- Destination Host Type: Linux/UNIX/Mac/Solaris
- Destination Host Name*: localhost
- Destination Location*: /opt/restore_kotesh
- Destination Type?**
 - Original Location: Restores/replaces original data
 - Destination Directory: Full *nix directory path on destination client
- Restore Path*:
 - New Directory <Destination>/zmc.YYYY-MM-DD_hh-mm-ss/<selections>
 - Full Path <Destination>/original/backup/path/to/restored/<selections>
- Temporary Location*:
 - Auto: (recommended)
 - Manual:

Buttons for 'Back' and 'Next' are located at the bottom of the dialog.

Note: The destination hostname can be a remote machine. The prerequisite for the remote machine is to install the zmanda client software.

4.3 Defining how to restore

On the Restore tab, click **how**. On this page you can configure the conflict resolution policies during restoration of file system.

The screenshot shows the Zmanda Management Console interface. The top navigation bar includes 'Backup', 'Vault', 'Monitor', 'Report', 'Restore', and 'Admin'. The 'Restore' tab is active, and the 'how' sub-tab is selected. The main content area displays the 'Restore Mode: Explore & Select' and a modal window titled 'How to restore, if already exists?'. The modal contains the following fields and options:

- DLE/Object Type: Linux
- Original Host: localhost
- Original Path: /opt/localdata_copyset
- If the Destination Location already has a file or directory with the same name:
 - Directory Conflicts**
 - Merge directory
 - File Conflicts**
 - Restore & Replace
 - Do not Restore
 - Restore, but keep both files

At the bottom of the modal, there are 'Back' and 'Next' buttons.

Note: You can select different options for directory and file name conflicts. Dell recommends to restore to a new directory so there will be no conflicts.

4.4 Performing the restore

1. On the Restore tab, click **now**.
2. Define the settings on this page as needed. When defining the settings on this page, keep the following in mind:
 - **DLE/Object Type** and **Source Host Type** are non-editable fields and are provided for information to fill other fields.
 - **Destination Host Name** -The Destination Host is the machine(s) where you want restore the files. It need not be the same machine that originally contained the backed up data.
 - If no **Destination Host** is specified, the files are restored to the Amanda server machine.
 - **Destination Host Type:** Choose either Linux/Unix/Mac/Solaris or Windows.

3. Click the **Restore** button to start the restore process.

The screenshot shows the Zmanda Management Console interface for the 'Restore' tab. The top navigation bar includes 'Backup', 'Vault', 'Monitor', 'Report', 'Restore', and 'Admin'. The 'Restore' tab is active, and the 'Backup Set' is 'Demo_DR'. The interface displays the following sections:

- Restore from Backup Image of:** Backup made before: August 21, 2015, 12:15 am. DLE/Object Type: Linux. Original Host: localhost. Original Directory: /opt/localdata_copysset.
- Restore to Destination:** Destination Host: localhost. Destination Location: /opt/restore_kotesh/zmc.2015-08-24_05-MM-SS.
- Media Needed:** A table showing the media requirements for the restore operation.
- Demo_DR Restore Status: Not Started:** A status section with a large green play button and a 'Restore' button.

Level	Size	%	Date	Time	Label
0	22032M	1	2015-08-21	00:15:05	Demo_DR-AA-001



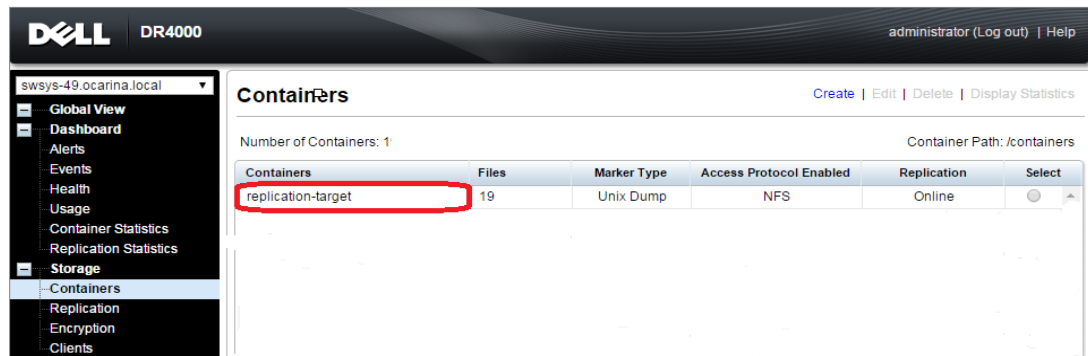
5 Setting up DR Series system native replication and restore from the replication target container

5.1 Building a replication relationship between DR Series systems

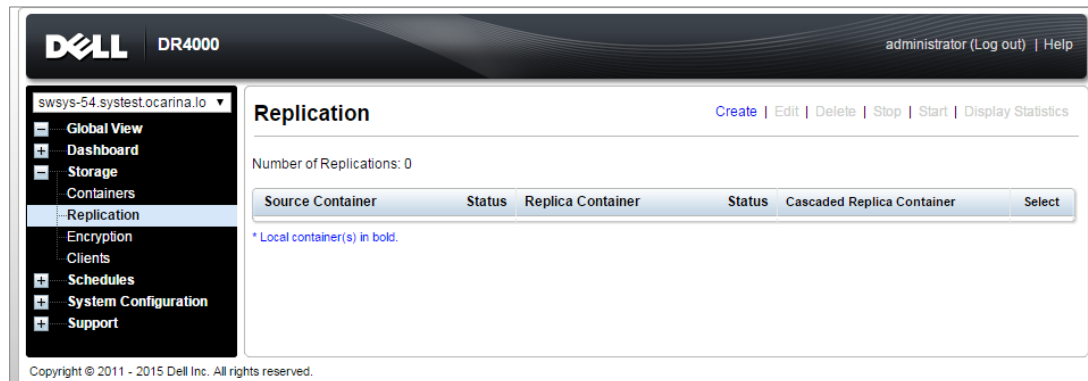
This section will refer to the example DR Series system and container *amand-src* as the source DR and replication source respectively.

Replication can be set up when no backups have been taken on the source or after the source has some backups.

1. Create an NFS container on the target DR Series system to be configured as the replication target. (Follow the same steps used for creating the container as in section 1 of this document.)



2. On the source DR Series system, click **Replication** on the left navigation menu, and then click **Create**.



3. In the Create Replication dialog box, on the **Select container from Local System** drop down menu, select a source container.
4. Configure the Replica Container as follows:
 - a. Select the option, **Select container from remote system**
 - b. Enter the target DR Series system logon credentials.
 - c. Click **Retrieve Remote Containers**, and then select the target container from the list.

- Click **Create Replication**.

- Verify that the replication is created successfully, and that the Status column shows a check box for the replication session.

Message

- Successfully added replication for container 'amanda-src' - 'replication-target'.
- NOTE: Replication connection(s) are being established. Information updates may be briefly delayed until the connection is completed.

Number of Replications: 1

Source Container	Status	Replica Container	Status	Cascaded Replica Container	Select
swsys-54 amanda-src	<input checked="" type="checkbox"/>	swsys-49 replication-target	<input checked="" type="checkbox"/>	Not Configured	<input type="checkbox"/>

* Local container(s) in bold.

Copyright © 2011 - 2015 Dell Inc. All rights reserved.



7. Select the replication session, and then click **Start** to start the replication. Once replication has completed, the Status column will display the status, **INSYNC**.

The screenshot shows the Dell DR4000 GUI. The top navigation bar includes the Dell logo, 'DR4000', and user information 'administrator (Log out) | Help'. A left-hand navigation menu is visible with options like 'Global View', 'Dashboard', 'Storage', 'Containers', 'Replication', 'Encryption', 'Clients', 'Schedules', 'System Configuration', and 'Support'. The main content area is titled 'Replication' and includes a 'Number of Replications: 1' indicator. A table displays the replication session details:

Source Container	Status	Replica Container	Status	Cascaded Replica Container	Select
swsys-54 amanda-src	✓	swsys-49 replication-target	✓	Not Configured	<input type="radio"/>

Below the table, there is a note: '* Local container(s) in bold.' At the top right of the Replication page, there are buttons for 'Create | Edit | Delete | Stop | **Start** | Display Statistics', with the 'Start' button highlighted by a red box. The footer of the GUI reads 'Copyright © 2011 - 2015 Dell Inc. All rights reserved.'

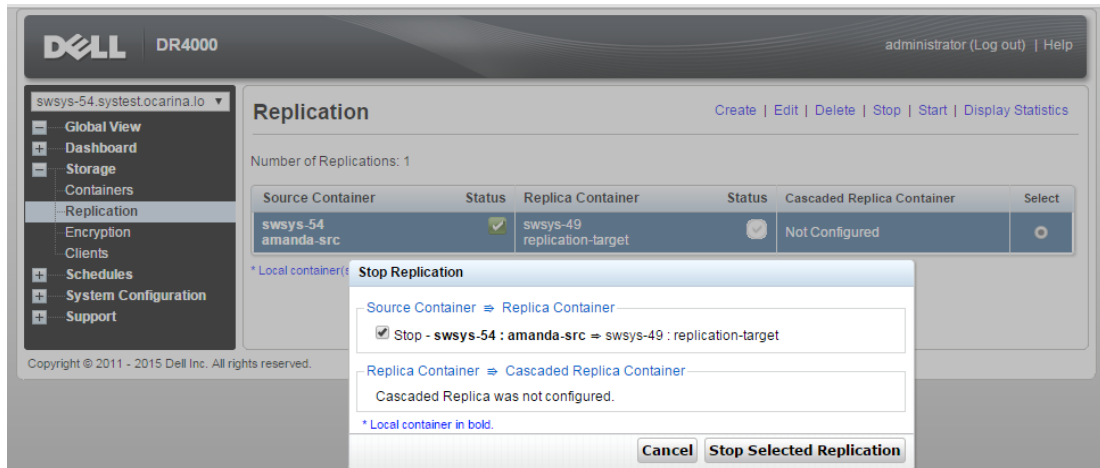
5.2 Restoring data from the target DR Series system

Before you begin, ensure the following:

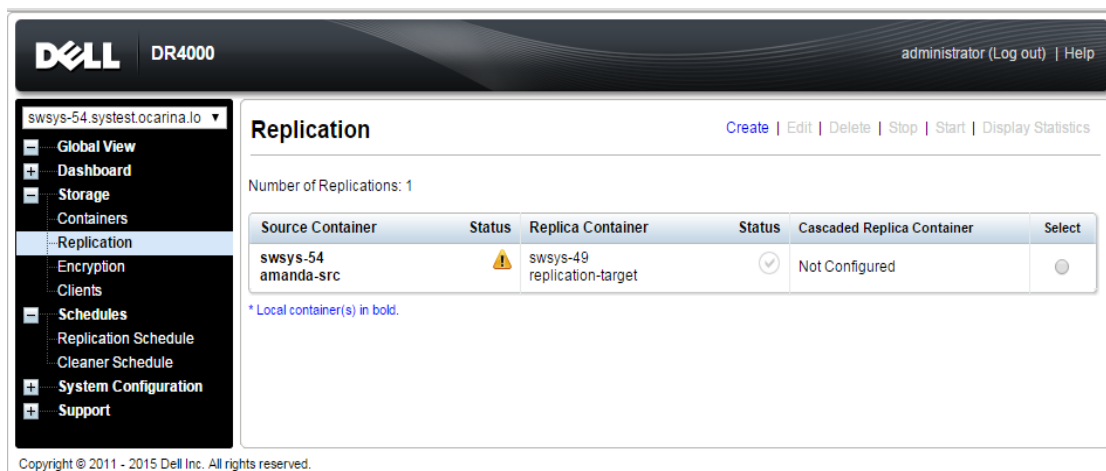
- The replication session has a Peer Status of **Online** if restoring from the replication target is needed,
- The replication is in an **INSYNC** state from the Replication Statistics menu before Stopping/Deleting the replication.
- The replication target has an **NFS** connection enabled to restore from the container using Amanda.
- When restoring the data from a replication target, the replication relationship between the source and target containers must be removed.

Follow these steps to restore data from a target DR Series system.

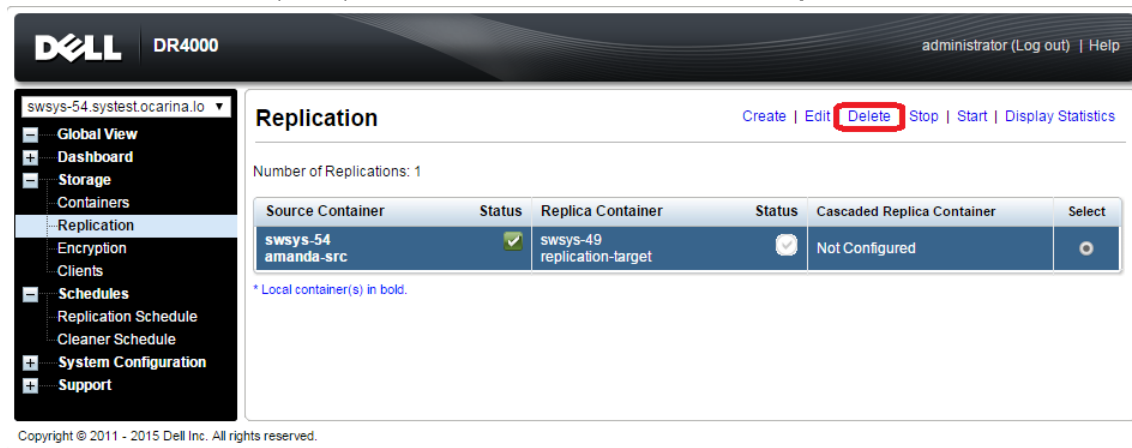
1. In the DR Series system GUI, navigate to the Replication page by selecting **Replication** in the left navigation area.
2. Select the replication pair, and click **Stop**. Follow the on-screen prompts and click **Stop Selected Replication**.

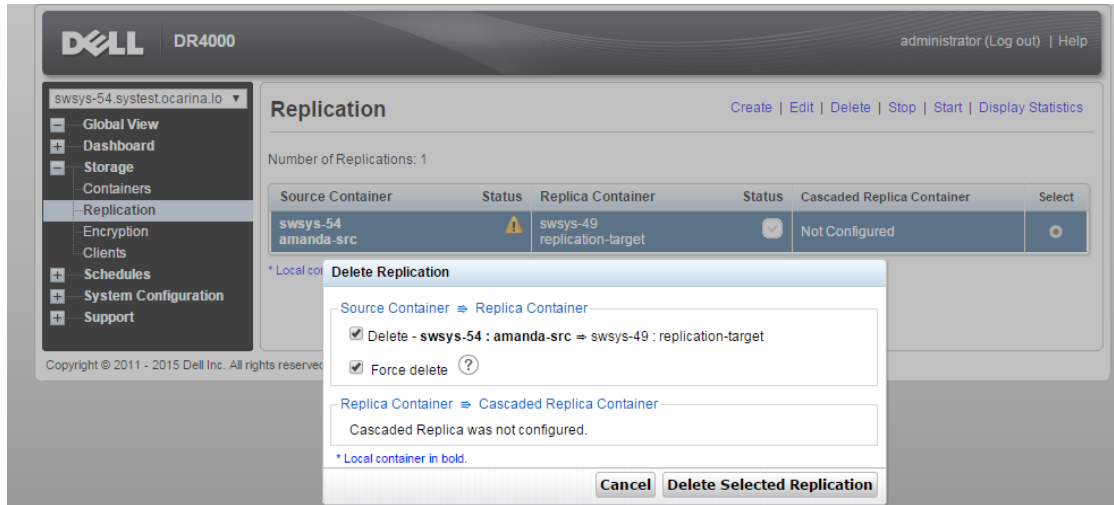


The Status will change to a warning when the replication stops.

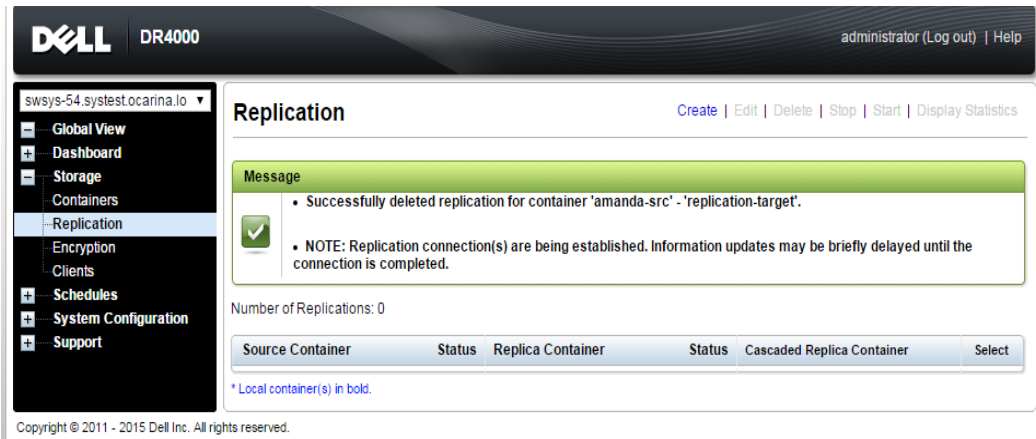


3. Delete the replication by selecting the replication pair and clicking **Delete** at the top of the page. Follow the on-screen prompts and then click **Delete Selected Replication**.





A message is displayed when the Replication is successfully deleted.



4. Log on to the Amanda Server, and unmount the DR Series system source container, for example amanda-src, mounted at **/mnt/DR_container_amanda**:

```
umount /mnt/DR_container_amanda
```

5. On the same mount point, mount the DR Series system replication target container, for example:

```
mount -t nfs <Replication Target DR FQDN>:/containers/replication-target /mnt/DRNFSTarget
```

6. For the instructions for restoring, refer to the section in this document, *Creating a new restore job*.

NOTE: The device name and backup set remains the same for restoring data from the replication target.

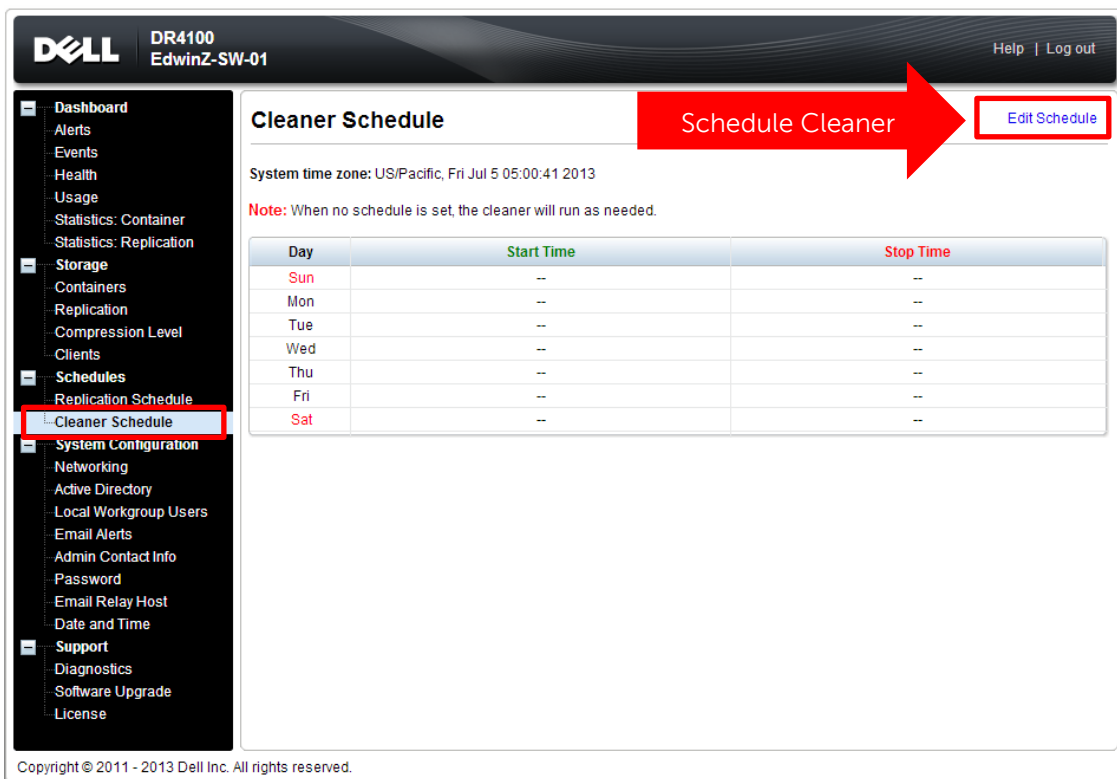


6 Setting up the DR Series system cleaner

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



The screenshot shows the Dell DR Series system cleaner configuration interface. The sidebar menu on the left includes sections for Dashboard, Storage, Schedules, System Configuration, and Support. The 'Cleaner Schedule' option is highlighted in the Schedules section. The main content area displays the 'Cleaner Schedule' configuration page. The page title is 'Cleaner Schedule'. Below the title, there is a 'System time zone' field set to 'US/Pacific, Fri Jul 5 05:00:41 2013'. A note states: 'Note: When no schedule is set, the cleaner will run as needed.' Below the note is a table with columns for Day, Start Time, and Stop Time. The table contains rows for Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all with '--' in the Start Time and Stop Time columns. A red arrow points to the 'Schedule Cleaner' button, and a red box highlights the 'Edit Schedule' button.

Day	Start Time	Stop Time
Sun	--	--
Mon	--	--
Tue	--	--
Wed	--	--
Thu	--	--
Fri	--	--
Sat	--	--



7 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.

