

# Setting up the DR Series System as an NFS Target on Amanda Enterprise 3.3.5

## Technical White Paper

Quest Engineering

October 2017



© 2017 Quest Software Inc.

## ALL RIGHTS RESERVED.

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

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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.

Setting Up the DR Series System as an NFS Target on Amanda Enterprise. Updated December 22, 2017

# Contents

<b>Installing and configuring the DR Series system .....</b>	<b>6</b>
<b>Setting up for Unix/Linux environment backup .....</b>	<b>13</b>
Creating the backup set .....	13
Creating the storage devices .....	14
<b>Creating a new backup job with the DR Series system as the target.....</b>	<b>16</b>
Defining the backup set.....	16
Defining where to back up .....	17
Staging a backup .....	19
Defining when to back up.....	19
Defining additional backup settings .....	20
Activating a backup .....	21
<b>Creating a new restore job .....</b>	<b>23</b>
Defining what to restore .....	23
Defining where to restore .....	24
Defining how to restore .....	25
<b>Setting up DR Series native replication and restore from the replication target container .....</b>	<b>27</b>
Configuring the replication relationship between DR Series systems .....	27
Restoring data from the target DR Series system .....	31
<b>Setting up the DR Series system cleaner .....</b>	<b>34</b>
<b>Monitoring deduplication, compression, and performance .....</b>	<b>36</b>

# Revisions

---

Date	Description
January 2014	Initial release
November 2016	Updated the guide with new DR-4.0 GUI screens
November 2017	Updated with Quest-branded DR Series system screenshots (v4.0.3)

# Executive Summary

---

This document provides information about how to set up the DR Series system as a backup target for Amanda.

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>

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

[http://wiki.zmanda.com/index.php/User\\_documentation](http://wiki.zmanda.com/index.php/User_documentation)



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

# Installing and configuring the DR Series system

- 1 Rack and cable the DR Series system, and power it on. In the Quest DR Series System Administrator Guide, see the following sections for information about using the iDRAC connection and initializing the appliance.
  - “iDRAC Connection”,
  - “Logging in and Initializing the DR Series system”
  - “Accessing iDRAC6/Idrac7 Using RACADM”
- 2 Log on to iDRAC using the default credentials (username: root and password: calvin) and either:
  - the default address 192.168.0.120,
  - or the IP address that is assigned to the iDRAC interface

INTEGRATED REMOTE ACCESS CONTROLLER Enterprise

Login ?

iDRAC | Quest DR4000

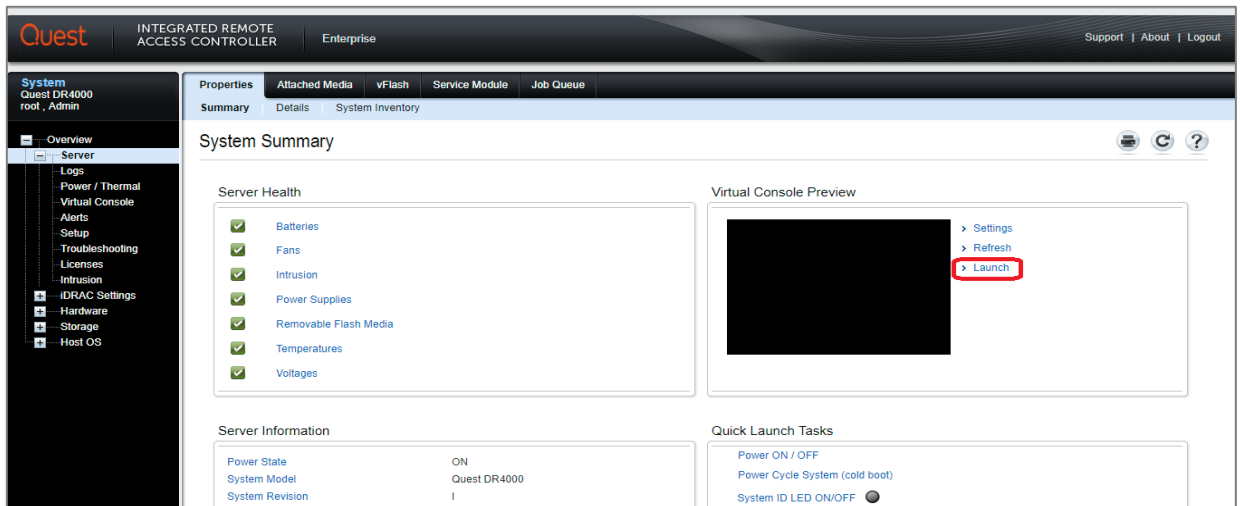
Type the Username and Password and click Submit.

Username: Password:

Domain: This iDRAC

Cancel Submit

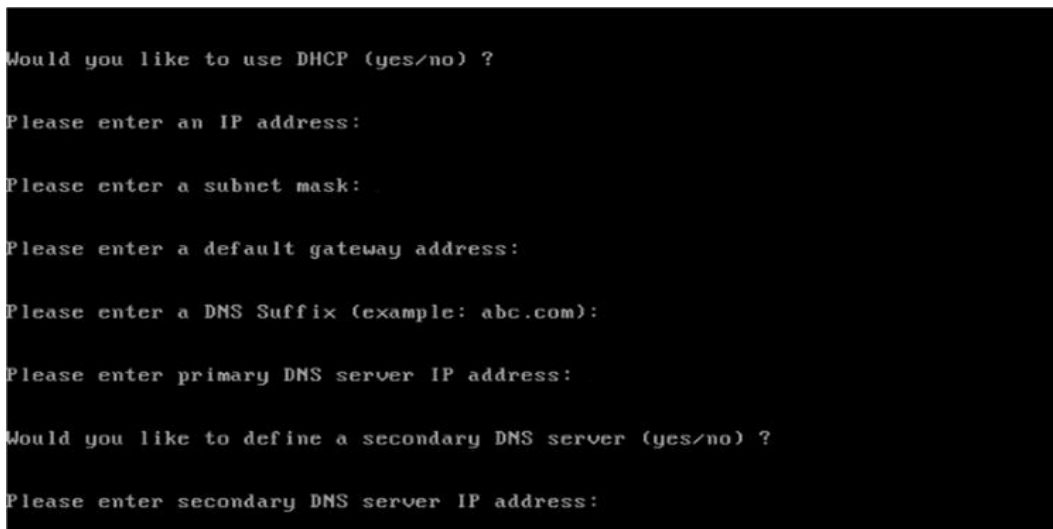
- 3 Launch the virtual console.



- 4 After the virtual console opens, log on to the system (with the username: **administrator** and password: **St0r@ge!** where the "0" in the password is the numeral zero).



- 5 Set the user-defined networking preferences.



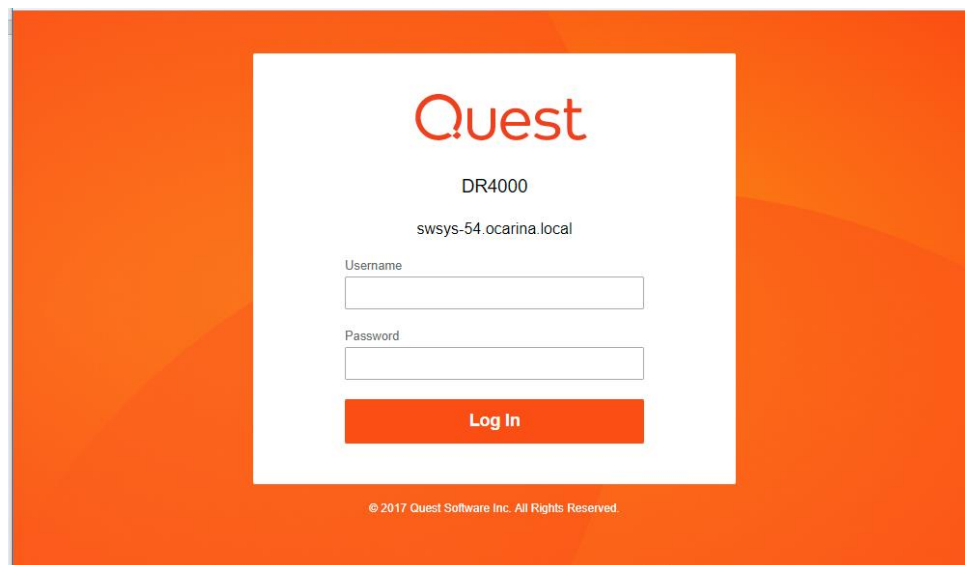
- 6 View the summary of preferences and confirm that it is correct.

```
=====
                        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        : Swsys-54

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.).

The image shows the Quest DR4000 login interface. It has an orange background with a white central box. Inside the box, the Quest logo is at the top, followed by 'DR4000' and 'swsys-54.ocarina.local'. Below this are input fields for 'Username' and 'Password', and a red 'Log In' button. At the bottom of the white box, it says '© 2017 Quest Software Inc. All Rights Reserved.'

- 8 Join the DR Series system to Active Directory.

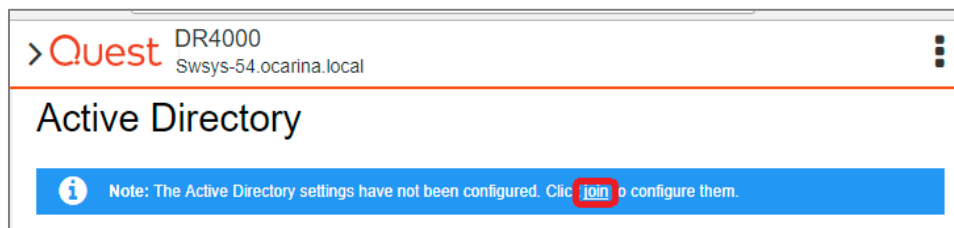
**i** **NOTE:** if you do not want to add the DR Series system to Active Directory, see the *DR Series System Owner's Manual* for guest logon instructions.

- a In the left navigation area of the DR Series system GUI, click **System Configuration** and then select **Active Directory**.





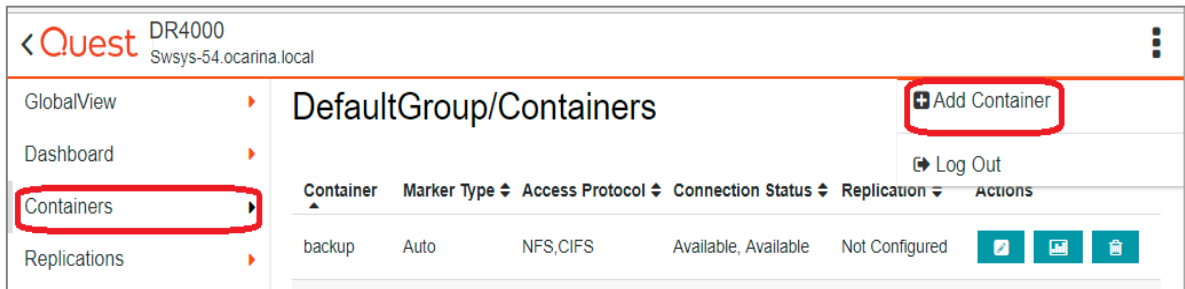
b Click **Join**.



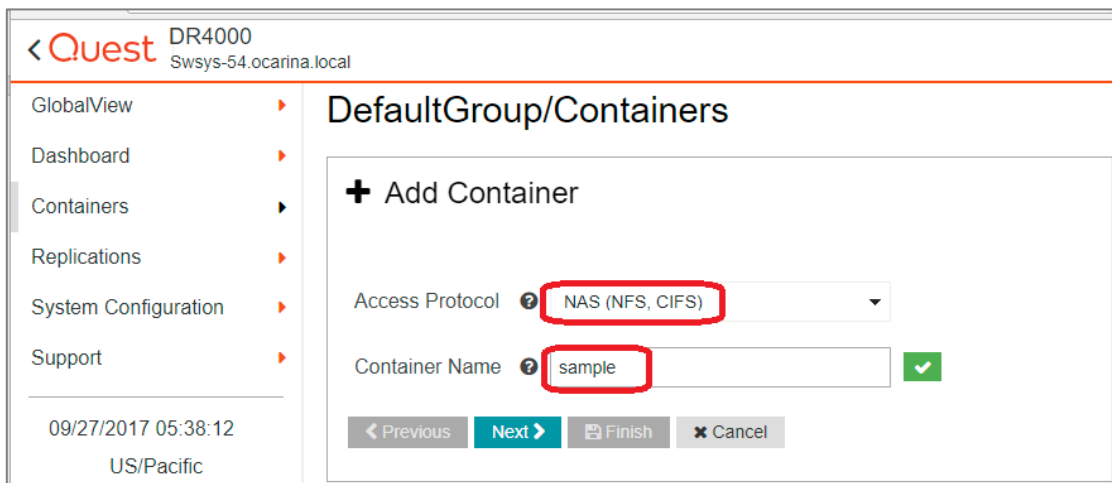
c Enter valid credentials and click **Join**.

The screenshot shows the "Active Directory" configuration page in the Quest DR4000 web interface, specifically the "Join" form. The top navigation bar includes the Quest logo, the text "DR4000", and the URL "Swsys-54.ocarina.local". The page title is "Active Directory". Below the title, the "Join" form is displayed. The form has a title "Join" with a key icon. It contains four input fields: "Domain Name (FQDN)" with a "Required" label, "Username" with a "Required" label, "Password" with a "Required" label, and "Org Unit". At the bottom of the form, there are two buttons: "Join" and "Cancel".

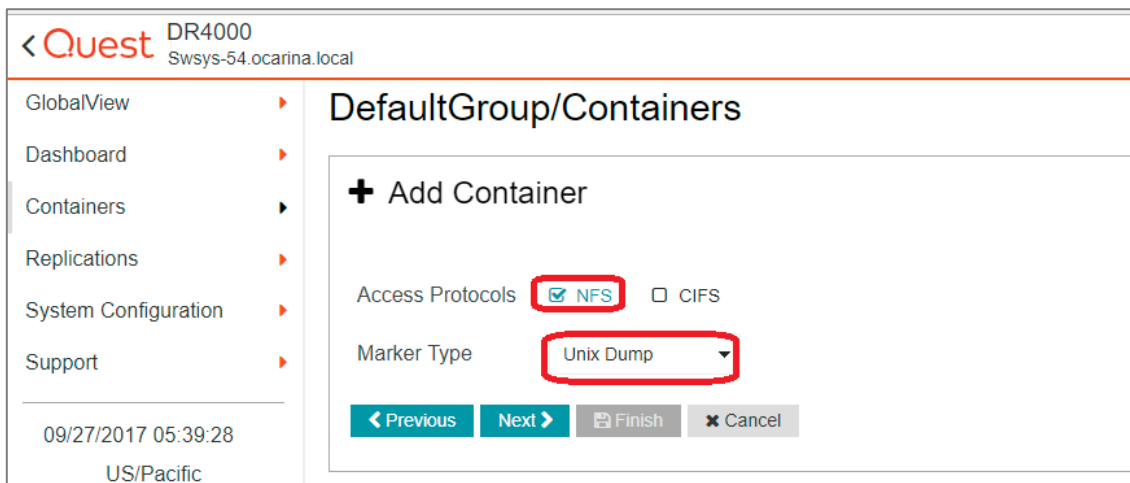
- 9 You now need to create and mount the container. In the left navigation menu, click **Containers > Default Group**, and then, on the Action menu in the upper right corner of the page, Add Container.



- 10 Enter a container name and for the Access Protocol, select **NAS (NFS, CIFS)** and then click **Next**.



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



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

Quest DR4000  
Swsys-54.ocarina.local

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

09/27/2017 05:40:46  
US/Pacific

### DefaultGroup/Containers

#### + Add Container

NFS Options ☒ Read Write Access ☐ Read Only Access

Map Root To

Client Access ☒ Open (allow all clients) ☐ Create Client Access List

Client FQDN or IP Address   
+

Allow Clients

< Previous Next > Finish Cancel

13 Review the summary and then click **Save** to add the container.

Quest DR4000  
Swsys-54.ocarina.local

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

09/27/2017 05:42:08  
US/Pacific

### + Add Container

#### Storage Access Protocol

Access Protocol NAS (NFS, CIFS)

Container Name **sample**

#### Configure NAS Access & Marker

NAS Access Protocol NFS

Marker Type Unix Dump

#### Configure NFS Client Access

NFS Options Read Write Access




Map Root To Root

Client Access Open (allow all clients)

< Previous Next > **Save** Cancel

14 Confirm that the container is added.

The screenshot displays the 'SG1/Containers' management interface. A blue notification banner at the top states: 'Success: Successfully added container "sample1". Container is being established. Information updates may be briefly delayed until the process is fully completed.' Below this, a table lists the containers. The table has columns: Container, Marker Type, Access Protocol, Connection Status, Replication, and Actions. One container named 'sample' is listed, with 'Auto' as the Marker Type, 'NFS,CIFS' as the Access Protocol, and 'Available, Available' as the Connection Status. The Replication status is 'Not Configured'. The Actions column contains three icons: a checkmark, a document, and a trash can. The left sidebar shows navigation options: GlobalView, Dashboard, Containers (selected), Replications, System Configuration, and Support. At the bottom left, the date and time are shown as '09/28/2017 10:49:57' and the time zone as 'US/Pacific'.

Container	Marker Type	Access Protocol	Connection Status	Replication	Actions
sample	Auto	NFS,CIFS	Available, Available	Not Configured	  

1 Item(s) found

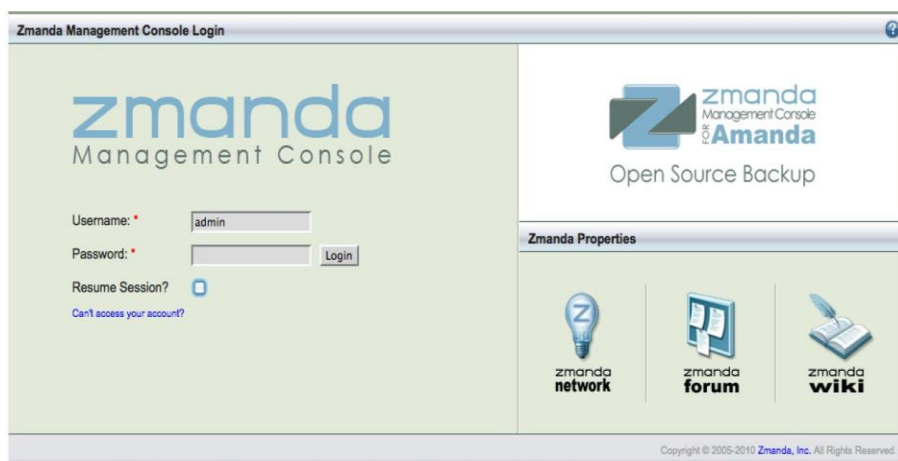
09/28/2017 10:49:57  
US/Pacific

# 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](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>/`



## 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.

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

Administer backup sets - create, edit, view, delete backup sets

Create Backup Set

Backup Set Owner: admin

Backup Set Name: Savings\_DR

Brief Description: Test DR Savings

Report Display Unit: Megabytes

Comments: (clear)

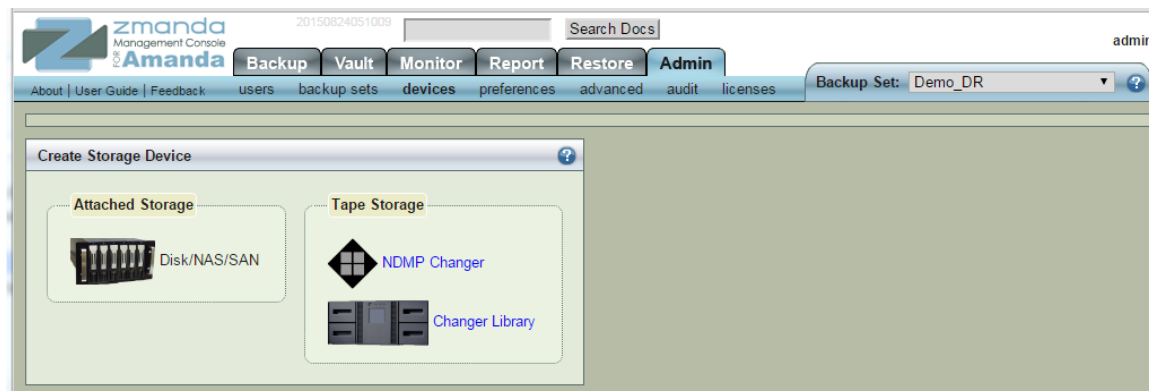
Cancel Add

## Creating the storage devices

Follow these steps to create storage devices:

- 1 Log on to the Amanda server and add the DR Series system NFS mount.
- 2 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/sample /mnt/DR_container_amanda
```
- 3 On the Admin tab, under Attached Storage, click **Disk/NAS/SAN** to add a DR Series system container as a storage device.



- 4 Enter the device name and any comments.
- 5 In the Root Path field, enter the mount point path for the DR Series system container, and click Add.

**Create : Disk/NAS/SAN Device**

Name\*: DR\_device1

Comments:

Root Path\*: /mnt/foldename

Reserved Percent\*: 5 %

Advanced Options

Cancel Add

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

**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

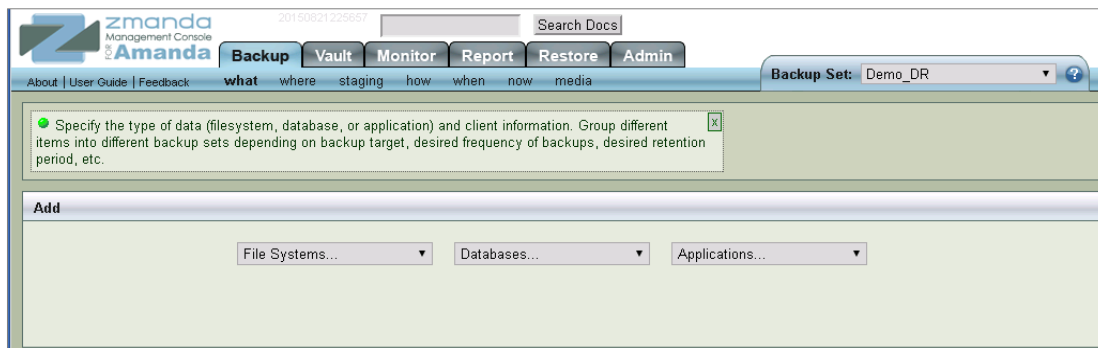
Invert Selection Refresh Table Edit Delete List Expert Use

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

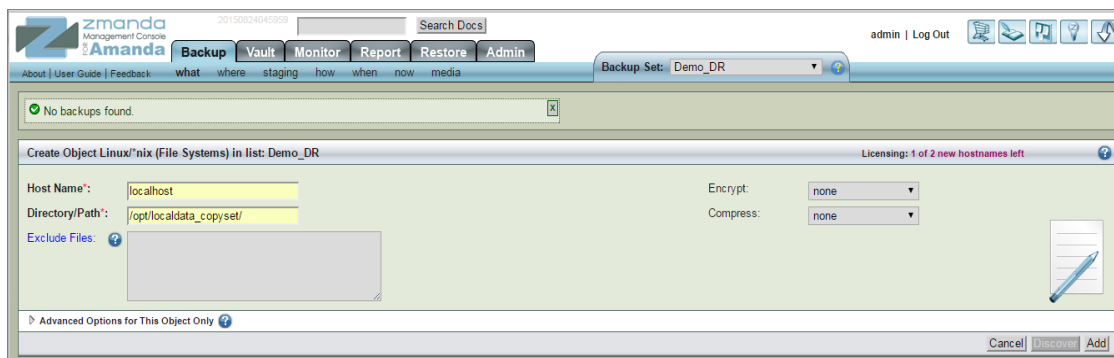
## Defining the backup set

In the Zmanda Management Console, you can define the host system and directories to include in a 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**.

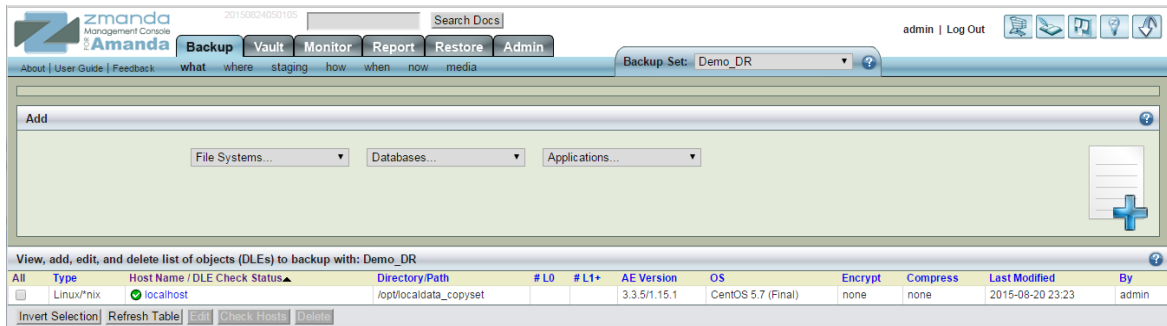






**NOTE:** For better space savings, Quest recommends that the Encrypt and Compress options are set to none

- 3 Upon successful addition, the data set is listed at the bottom of the management console window.



## Defining where to back up

Follow these steps to define 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 screenshot shows the Zmanda Amanda Management Console interface. At the top, there are tabs for Backup, Vault, Monitor, Report, Restore, and Admin. A message box at the top states: "After clicking 'Add/Update', ZMC will try to connect to the device. Depends on the connection, this operation may take some time to finish." Below this, a configuration window titled "Use Demo\_DR configuration for device: DR\_device1" is open. It contains the following fields:

- Device Type: Disk/NAS/SAN (with a plus icon)
- Device Name\*: DR\_device1
- Comments: (empty text area)
- Taperscan: Oldest (dropdown menu)
- Backups stored at\*: /mnt/DR\_container\_amanda (with an info icon)
- Partition Total Space\*: Unknown MiB
- Partition Free Space\*: Unknown MiB (shared free space)
- Media Used Space: 0 MiB (used by this backup set)

At the bottom of the configuration window are "Cancel" and "Add" buttons.

4 After the virtual console opens, log on to the system (with the username: **administrator** and password: **St0r@ge!** where the "0" in the password is the numeral zero). The DR Series system is added.

The screenshot shows the Zmanda Amanda Management Console interface after the device has been added. The configuration window is now titled "Edit Demo\_DR configuration for device: DR\_device1". The fields are the same as in the previous screenshot, but the "Add" button has been replaced with "Update". Below the configuration window, there is a table titled "View, add, and edit how backup sets use devices".

All	Backup Set	Device	Device Name	Endpoint / Changer Path	Storage Device Statistics	Auto Label	Time Last Modified	By
<input checked="" type="checkbox"/>	Demo_DR		DR_device1	/mnt/DR_container_amanda	261.4G 4494.8G	Yes	2015-08-20 23:24:23	admin

# 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. The 'Backup' tab is selected, and the 'staging' sub-tab is active. The 'Edit Staging Configuration for Demo\_DR' dialog is open. The configuration includes:

- Device Name: DR\_device1
- Auto Flush: ☒ automatically flush dumps from staging to media
- Staging Size Limit: Disabled (recommended: 25% of partition)
- Reserved for root: 5% (5% recommended, 10% for Solaris)
- Backup runs staged at: /var/lib/amanda/staging/Demo\_DR
- Live Staging Contents: Space currently used: 0. The staging area of this backup set is currently empty.
- 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.'

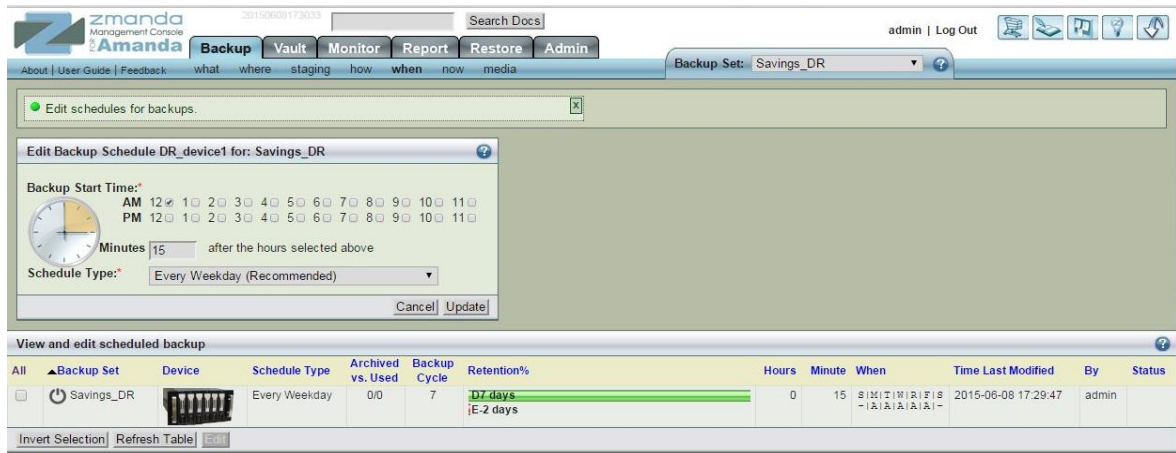
At the bottom, there is a table titled 'View and edit how backup sets use staging areas'.

Backup Set	Device	Flash	Directory	Staging Partition Statistics	Staging Usage Statistics	Time Last Modified	By
Demo_DR	DR_device1	yes	/var/lib/amanda/staging/Demo_DR	Disabled	Disabled	2015-08-20 23:24:23	admin

# Defining when to back up

Follow these steps to define when to back up:

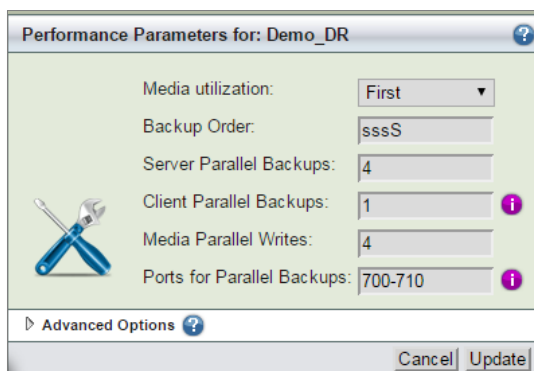
- 1 On the Backup tab, click when to define when to perform backups. The Backup Schedule table shows the list of backup sets and backup schedules. This overall view of the backup schedules provides helpful information about how backup windows overlap, as well as the number of backups running at any time.
- 2 Edit the backup schedule as needed, and then click **Update**.



## 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 Now** page to define key 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 **now** 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**.

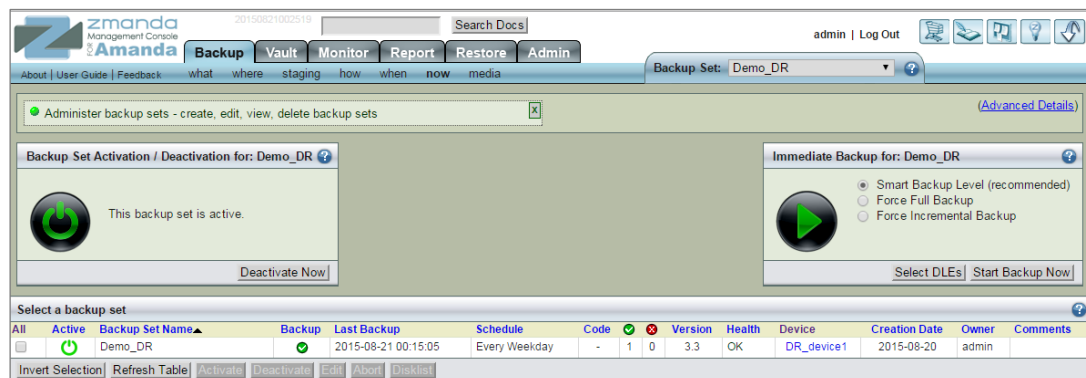
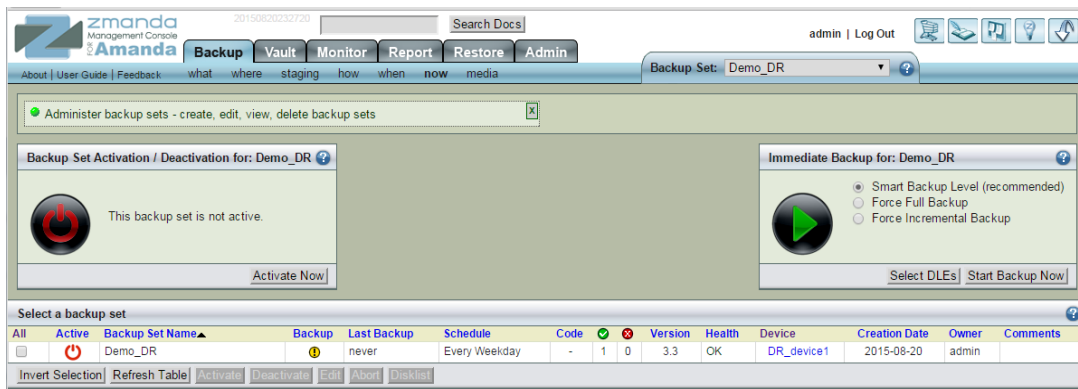


**NOTE:** For information about limits on the number of supported parallel streams or backups to the DR Series system, see the *DR Series System Interoperability Guide*.

# Activating a backup

A backup set must be activated for automatically-scheduled backups to execute, and 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 To execute a backup set immediately, click **Start Backup Now**. 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.

The screenshot displays the Zmanda Management Console interface. The top navigation bar includes tabs for Backup, Vault, Monitor (selected), Report, Restore, and Admin. The user is logged in as 'admin'. The main content area is titled 'Monitor Backups' and shows a status bar indicating the page was refreshed at 2015-08-21 00:25:58 with a 1-second interval.

On the left, the 'Monitor Backups' panel shows filters: 'Show Backups' set to 'newer than 2 days', 'Which Backup Set?' set to 'ALL', and 'Auto Refresh?' checked. It reports 'Total Backups: 1'. A 'Backup Type' table is also visible:

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"/>

On the right, the 'Legend: Backup States' table shows the following:

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

The 'Timeline Monitor Chart' at the bottom displays a table of backup activities:

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	<div></div>	localhost	/opt/localdata_copyset	<div></div>	<div></div>	<div></div>	22032m dumping to tape (21870m done (99.27%)) (0:15:09)	22032m finished (0:20:06)

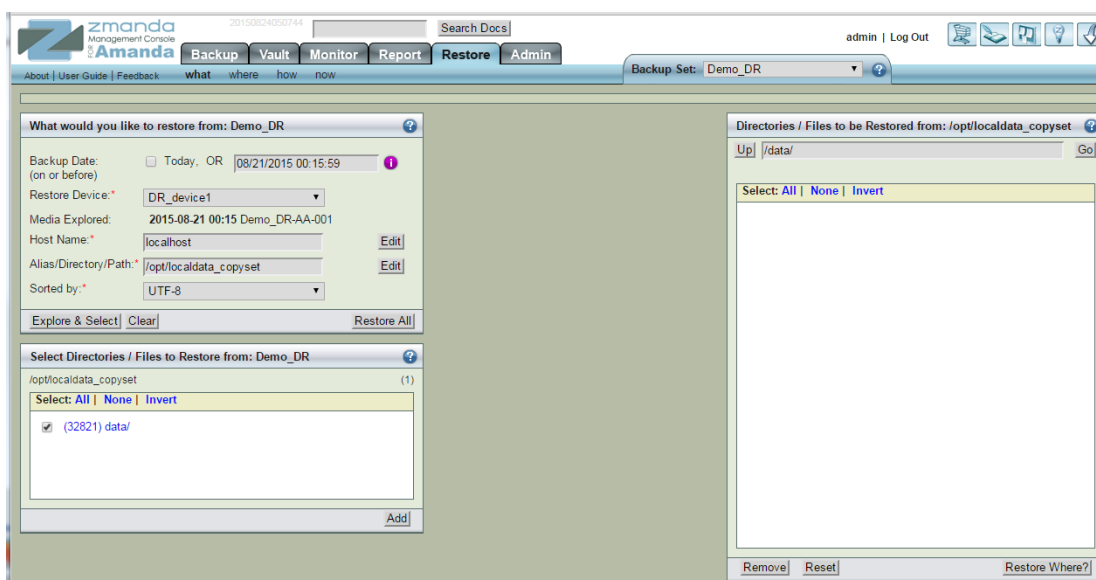
A 'Refresh Table' button is located at the bottom left of the timeline chart.

# Creating a new restore job

## 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
  - 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 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**.

## 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.

Follow these steps to define where to restore.

- 1 On the Restore tab, click **where**.

The Restore From, Restore To, and Tapes Needed panels provide information about the restore job. If the restore is from tape, make sure the required tapes are in the tape changer (in the slots reserved for the backup set).

- 2 Enter information for the Destination Host Name, Destination Location, the other relevant restore settings, and then click **Next**.





**NOTE:** The destination hostname can be a remote machine. The prerequisite for the remote machine is that it have the Zmanda client software installed..

## Defining how to restore

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



**NOTE:** You can select different options for directory and file name conflicts. Quest recommends restoring to a new directory so there will be no conflicts.

Follow these steps to perform the restore:

- 1 On the Restore tab, click **now**.
- 2 Define the settings on this page as needed with the following considerations:
  - **DLE/Object Type** and **Source Host Type** are non-editable fields and are provided for information to fill other fields.
  - **Destination Host Name** refers to the machine(s) where you want to restore the files. It does not have to 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.
  - For **Destination Host Type**, select either Linux/Unix/Mac/Solaris or Windows.
- 3 Click the **Restore** button to start the restore process.

zmanda Management Console  
Amanda

20150824053500 Search Docs admin | Log Out

Backup Set: Demo\_DR

Backup Vault Monitor Report **Restore** Admin

About | User Guide | Feedback what where how now

Restore!how changes applied.  
Restore Mode: Restore All

**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\_copyset

**Restore to Destination**

Destination Host: localhost

Destination Location: /opt/restore\_kotesh/zmc.2015-08-24\_05-MM-SS

**Media Needed**

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

**Demo\_DR Restore Status: Not Started**

Restore not started.

Advanced Options

Restore

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

## Configuring the replication relationship between DR Series systems

This section refers 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.)

< Quest

DR4000

swwsys-49.ocarina.local

GlobalView

DashBoard










Containers

Replications

System Configuration

Support

DefaultGroup/Containers

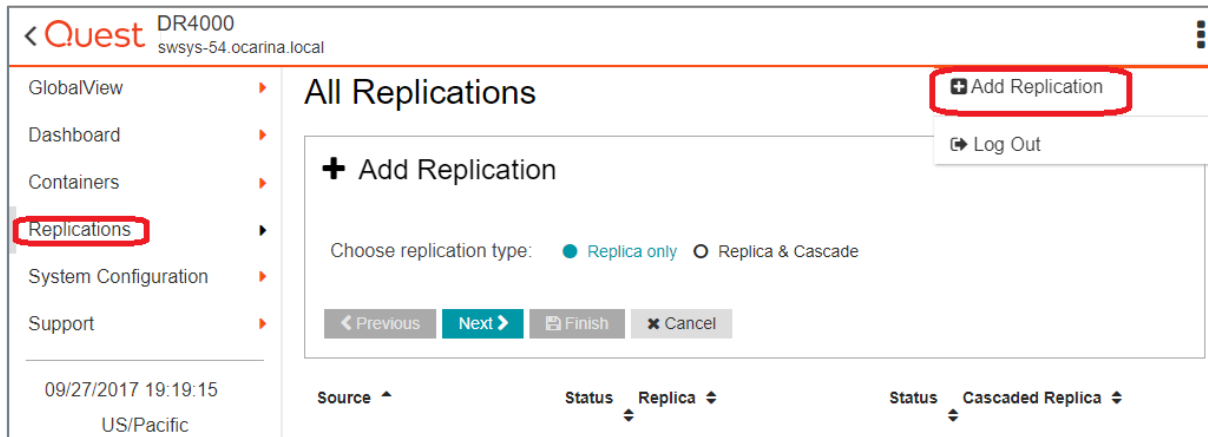
Container ^	Marker Type ^	Access Protocol ^	Connection Status ^	Replication ^	Actions
backup	Auto	NFS,CIFS	Available, Available	Not Configured	  
replication-target	Unix_Dump	NFS	Available	Not Configured	  
sample	Unix_Dump	NFS	Available	Not Configured	  

09/27/2017 19:10:47

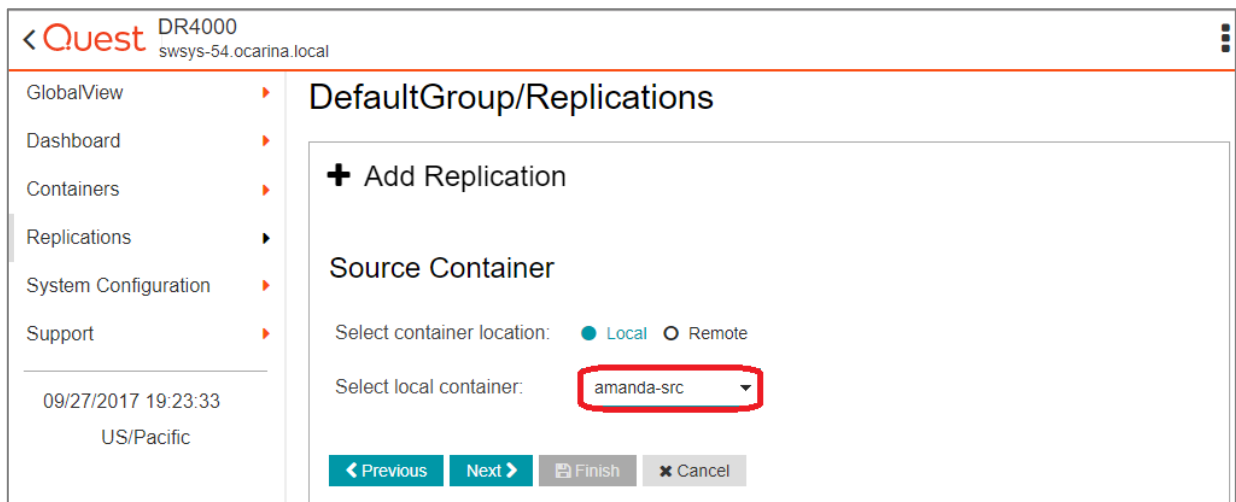
US/Pacific

3 Item(s) found.

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



- 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.

Quest DR4000  
swsys-54.ocarina.local

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

10/31/2017 10:47:28  
US/Pacific

## + Add Replication

### Source Container

*i* Source Container would not accept Cloud DR as a source container.

Select container location: ☐ Local ☒ Remote

Username:

Password:

Remote system:

**Retrieve Remote Container(s)**

Select remote container:

**< Previous** **Next >** **Finish** **Cancel**

- 5 Review the summary and then click **Finish**.

Quest DR4000  
swsys-54.ocarina.local

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

09/27/2017 19:28:13  
US/Pacific

## DefaultGroup/Replications

### + Add Replication

### Summary

**Source Container**

Location: local

Name: **amanda-src**

**Source Container ⇒ Replica Container**

Encryption: Not Enabled

**Replica Container**

Location: remote

Remote System: 10.250.242.135

name: **replication-target**

**< Previous** **Next >** **Finish** **Cancel**

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

Quest DR4000 swsys-54.ocarina.local

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

09/27/2017 20:04:50  
US/Pacific

## All Replications

Local container(s) in bold.

Source	Status	Replica	Status	Cascaded Replica
swsys-54 amanda-src	✓	swsys-49 replication-target	+	

Peer Status: Online

Peer Bandwidth: Default

State: **INSYNC**

Encryption: Not Enabled

Percent done: 100 %

Replication Average Transfer Rate: 0 bytes/sec

Replication Peak Transfer Rate: 0 bytes/sec

Network Average Transfer Rate: 0 bytes/sec

Network Peak Transfer Rate: 0 bytes/sec

Network Bytes Sent: 1.07 K

Pending Bytes: 0

Estimated Time to Sync: 0 sec

Dedupe Network Savings: 0.00 %

Compression Network Savings: 0.00 %

Last INSYNC Time: Wed Sep 27 19:30:12 2017

Time Until Scheduled Run: in Window

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

Quest DR4000 swsys-54.ocarina.local administrator

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

10/31/2017 11:16:36  
US/Pacific

## DefaultGroup/Replications

Local container(s) in bold.

Source	Status	Replica	Status	Cascaded Replica
swsys-54 amanda-src	⏏	swsys-49 replication-target	+	

Peer Status: Stopped

Peer Bandwidth: Default

State: **INSYNC**

Encryption: Not Enabled

Percent done: 100 %

Replication Average Transfer Rate: 0 bytes/sec

Replication Peak Transfer Rate: 0 bytes/sec

Network Average Transfer Rate: 0 bytes/sec

Network Peak Transfer Rate: 13.00 bytes/sec

Network Bytes Sent: 1.07 K

Pending Bytes: 0

# Restoring data from the target DR Series system

Before you begin restoring data from the target DR, ensure the following pre-requisites are met:

- 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, click Replication in the left navigation area.
- 2 Select the replication pair, and click **Stop**.

Quest DR4000  
swsys-54.ocarina.local

GlobalView  
Dashboard  
Containers  
Replications  
System Configuration  
Support

09/27/2017 20:04:50  
US/Pacific

## All Replications

Local container(s) in bold.

Source	Status	Replica	Status	Cascaded Replica
swsys-54 amanda-src	✓	swsys-49 replication-target	+	

Peer Status: Online

Peer Bandwidth: Default

State: INSYNC

Encryption: Not Enabled

Percent done: 100 %

Replication Average Transfer Rate: 0 bytes/sec

Replication Peak Transfer Rate: 0 bytes/sec

Network Average Transfer Rate: 0 bytes/sec

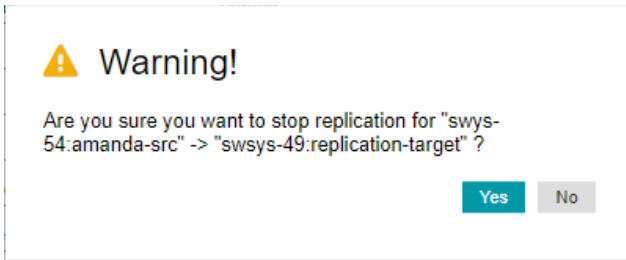
Network Peak Transfer Rate: 0 bytes/sec

Network Bytes Sent: 1.07 K

Pending Bytes: 0

Estimated Time to Sync: 0 sec

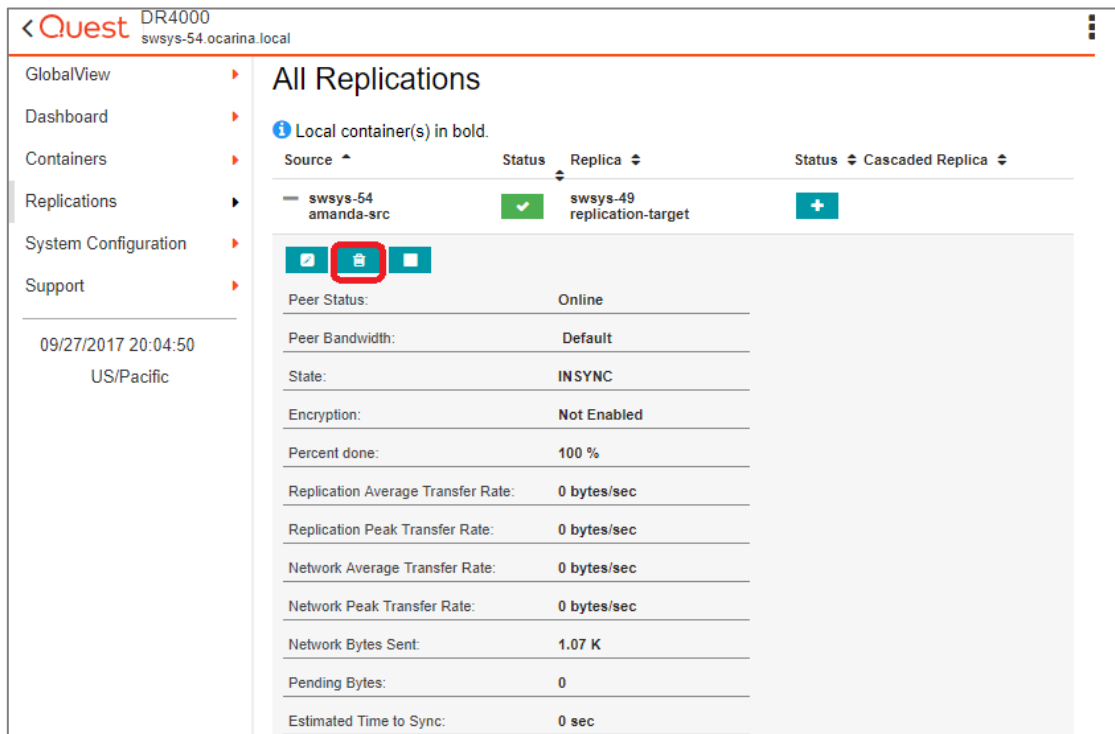
- 3 In the Warning dialog box, click **Yes** to confirm stopping the replication.



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

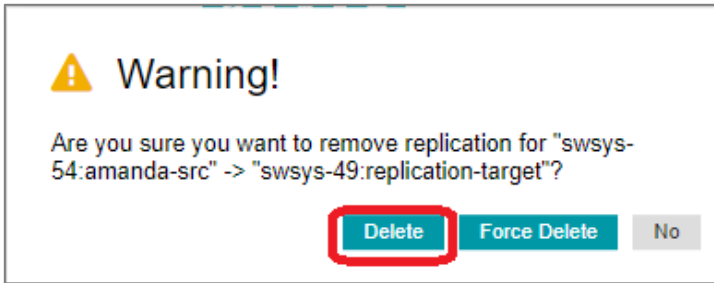


- 4 Delete the replication by selecting the replication pair and clicking **Delete** at the top of the page.

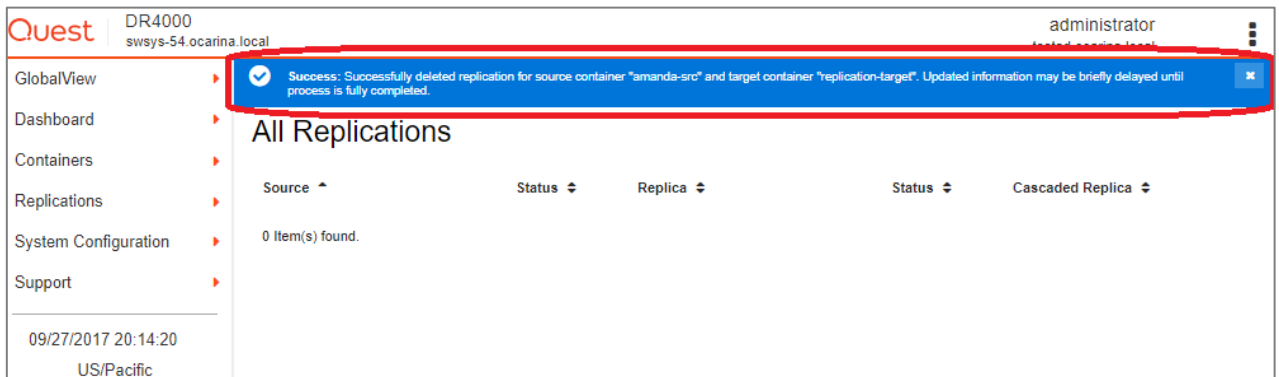




- 5 In the Warning dialog box, click **Yes** to confirm deleting the replication.



A message is displayed when the Replication is successfully deleted.



- 6 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`
- 7 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/DR_container_amanda
```
- 8 For the instructions for restoring, refer to the section in this document, Creating a new restore job.

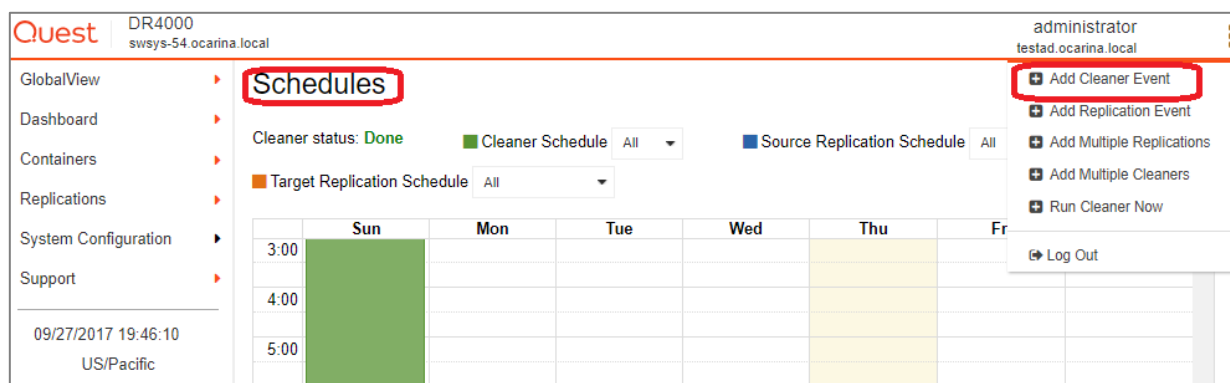
**i** | **NOTE:** The device name and backup set remains the same for restoring data from the replication target.

# 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. Refer to the DR Series Cleaner Best Practices white paper for guidance on setting up the cleaner.

- 1 In the DR Series system GUI, click **System Configuration > Schedules**.
- 2 On the Action menu, click **Add Cleaner Event**.



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

Quest DR4000 swsys-54.ocarina.local administrator testad.ocarina.local

GlobalView Dashboard Containers Replications System Configuration Support

## Schedules

Cleaner status: **Running** ■ Cleaner Schedule All ■ Source Replication Schedule All

■ Target Replication Schedule All

New

**i** Only one cleaner event is allowed per day.

Set event from start day: **Sunday** at: 01 : 00 to end day: **Monday** at: 02 : 00

Save Cancel

The new cleaner event is displayed on the Schedules page.

Quest DR4000 swsys-54.ocarina.local

GlobalView Dashboard Containers Replications System Configuration Support

## Schedules

Cleaner status: **Running** ■ Cleaner Schedule All

|      | Sun                    | Mon                    |
|------|------------------------|------------------------|
| 0:00 |                        |                        |
| 1:00 | 1:00 - 2:00<br>Cleaner | 1:00 - 2:00<br>Cleaner |
| 2:00 |                        |                        |
| 3:00 |                        |                        |

# Monitoring deduplication, compression, and performance

After backup jobs have run, the DR Series system tracks capacity, storage savings, and throughput in 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.

