

Quest DR Series System Container Migration

Technical White Paper

Quest Engineering

November 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.

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

Overview	5
Understanding migration strategies	5
CIFS/NFS containers	6
Veritas Backup Exec	7
Migrating OST containers	7
Migrating VTL containers	11
Veritas NetBackup	15
Migrating OST containers	15
Migrating VTL containers	15
CommVault	19
Migrating VTL containers	19
Quest NetVault	24
Migrating RDA containers	24
Migrating VTL containers	24
Quest vRanger	28
Migrating RDA containers	28

Executive Summary

This paper provides suggested best practices for migrating container types to Quest-branded containers for the DR Series system. Not all backup applications are covered in this document. Please contact technical support if additional assistance is needed.

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 backup application build version and screenshots used in this document might vary slightly, depending on the version of the DR Series system / backup application you are using.

Overview

Understanding migration strategies

Before you begin, you should refer to the following considerations about container migration in the DR Series system.

First, not all containers require migration; for example, CIFS/NFS containers are not “branded,” and, generally, require no additional steps to migrate outside of normal maintenance actions. Second, if a container needs migration there are three ways, in general, by which to migrate it.

In this document, each section describes a data management application and details the suggested way to migrate containers. If your specific data management application is not included in this guide, please note that the general options for migration are the same.

- The first general migration strategy is to create new containers, add them to the backup application, and then allow data on the old containers to reach retention. At that point, you can delete the old container. This requires the least amount of effort generally but depends on the data management application. Because data deduplication occurs between containers of the same storage group on the DR Series system, there will be no increase in storage overhead because of this action. The downside to this might be container limitations, such as four VTL's per DR Series system, and additional action being required once data reaches retention. This strategy applies to all container types.
- The second general migration type is to create and add a new container, but then manually run duplication/copy jobs to move existing data between containers. Once completed, you can delete the old container immediately; however, the duplication/copy process can be time-consuming and difficult, depending on the application. This strategy applies to all container types.
- The third general migration type is to remove the container from the data management application as-is. Re-add it to the data management application as a Quest container, and then run an inventory process on the container. This strategy only works for OST/RDA protocol; it will not work for VTL. Also, the inventory process can range from easy to very difficult/time-consuming, depending on the application.

CIFS/NFS containers

There is no need to migrate a CIFS/NFS container. If Rapid CIFS or Rapid NFS is used, be sure to upgrade to the latest Quest-branded installer for your build of the DR Series system operating system (OS).

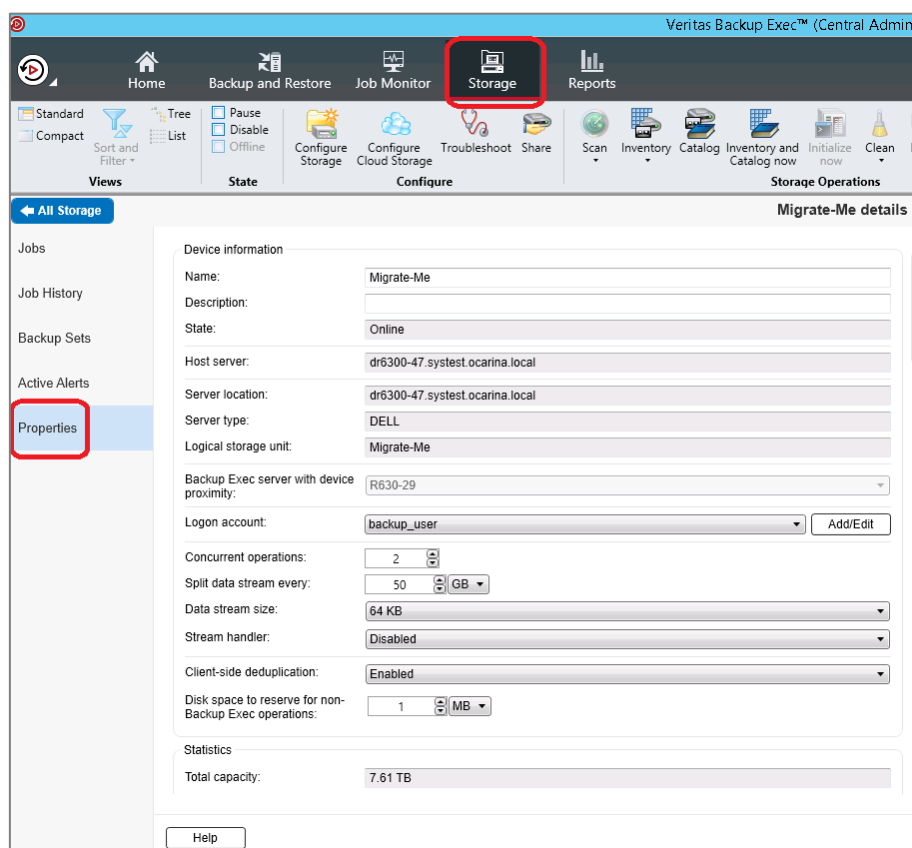
Veritas Backup Exec

Veritas Backup Exec is one of the easier backup applications in which to migrate containers. Generally, migration revolves around an inventory process or running duplication jobs.

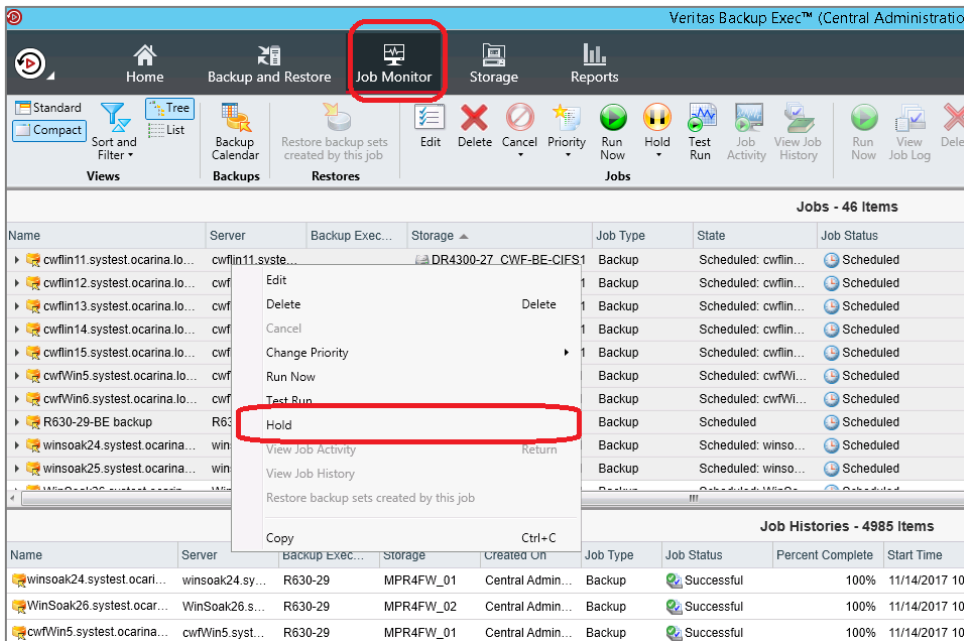
Migrating OST containers

The best strategy for Veritas Backup Exec regarding OST containers is to simply remove the container and re-add it as a Quest-branded container. Once that is complete, you need to run a catalog/inventory to re-import the images and retarget jobs to the Quest-branded container.

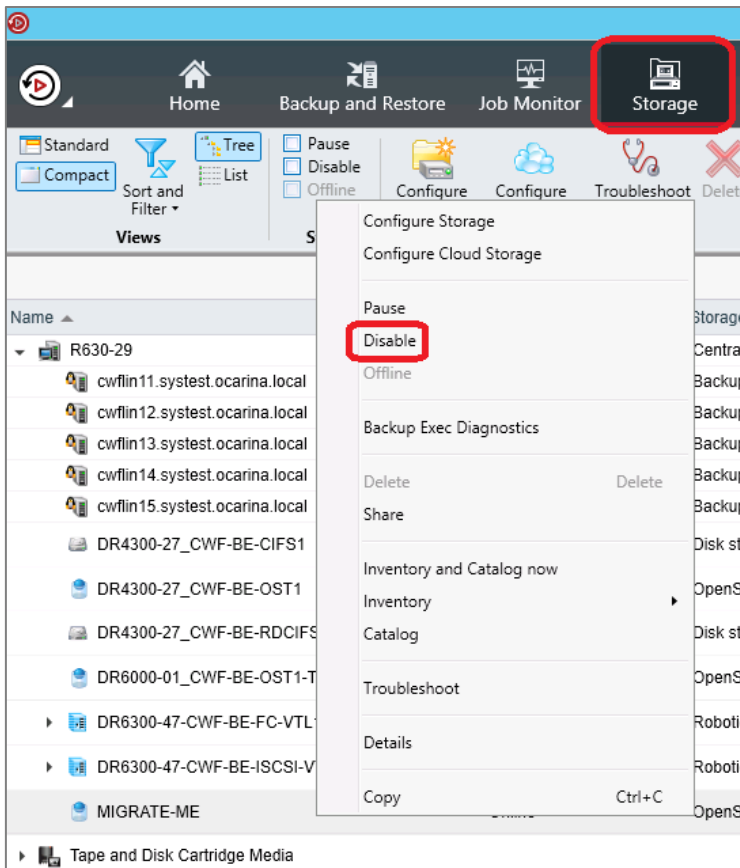
- 1 Start by reviewing your current container settings. Open the Backup Exec console, and navigate to the Storage Tab.
- 2 Double-click the container to be migrated, and then select the Properties tab. Note the current settings.



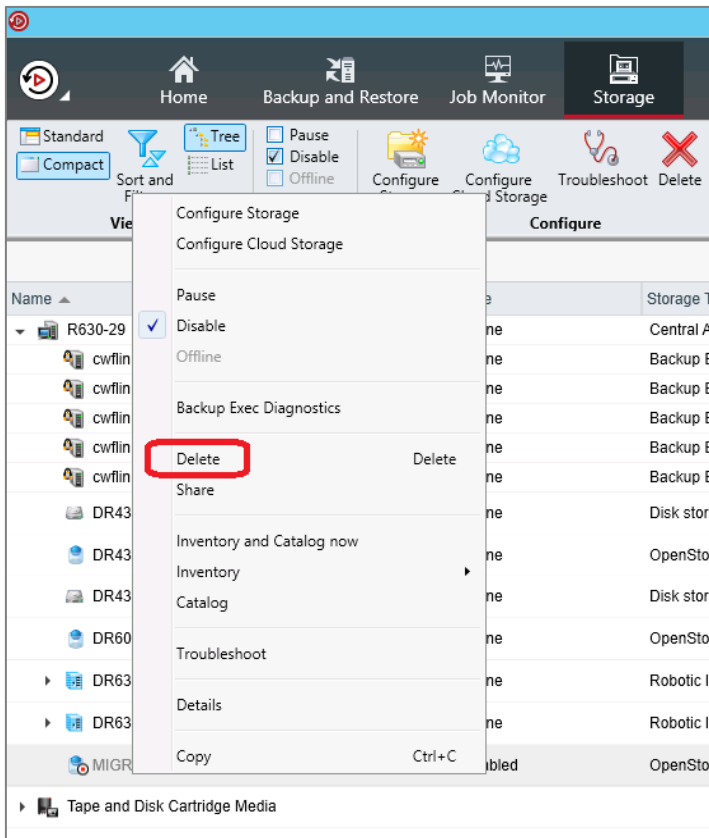
- On the Job Monitor tab, highlight all jobs using the container to be migrated, right-click and select **Hold**.



- On the Storage Tab, right-click the container to be migrated, and select **Disable**.



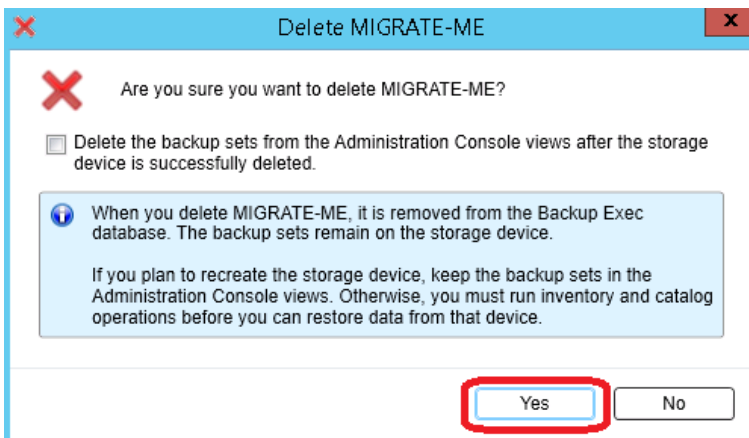
- When the container becomes grey, right-click it again, and select **Delete**.



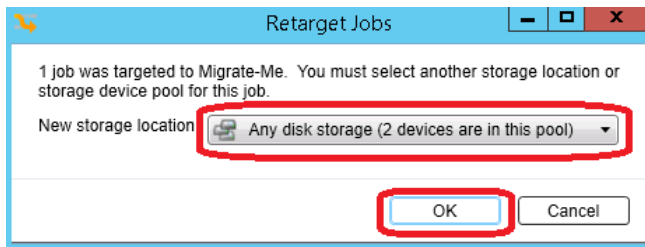
- On the pop-up window, do **not** select any check boxes; only click the **Yes** button.



CAUTION: Do **NOT** select the check box to delete backup sets. If you do all data will be deleted from the container and be unrecoverable

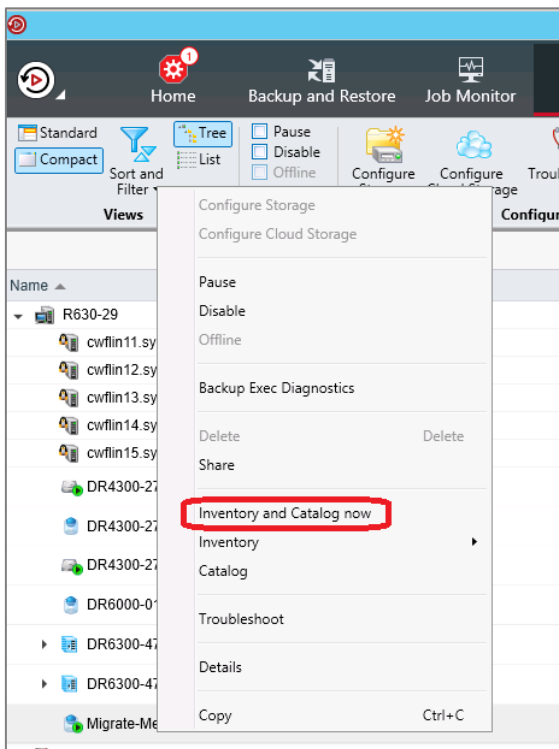


- If jobs are targeted to this container, a Retarget jobs option dialog box appears.
- Select the **Any disk storage** option in the drop-down menu, and click OK.

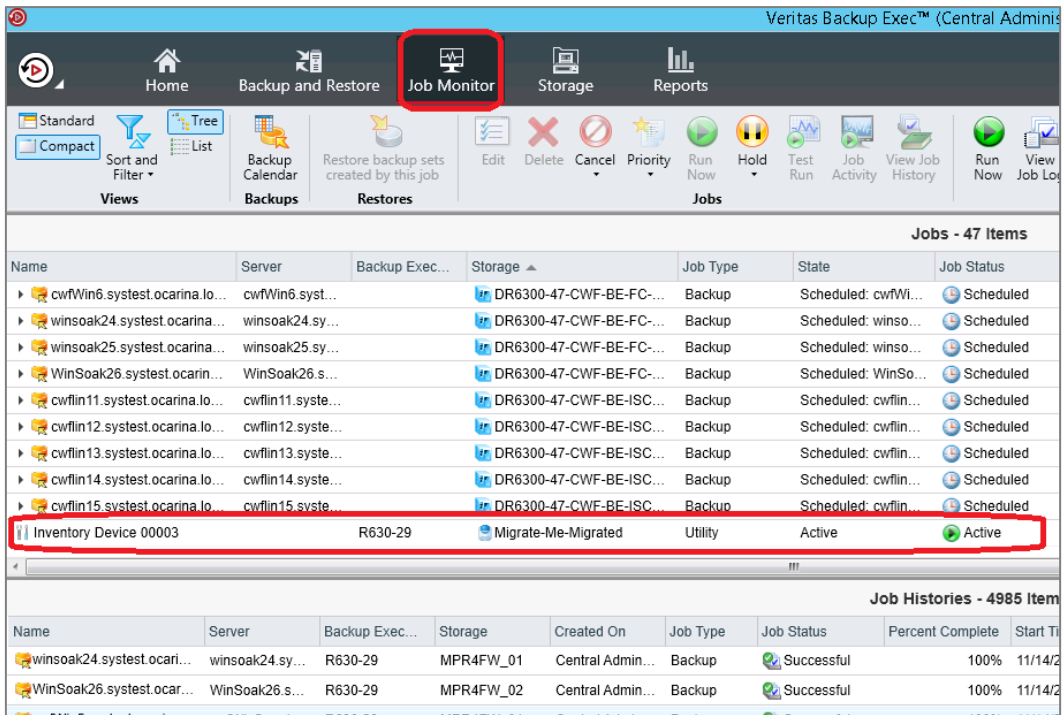


9 Select **Configure Storage** and proceed to add the container again as an OST device using the Quest plugin. If assistance is required, please review the Veritas Backup Exec setup whitepaper located at <http://support.quest.com/DR-Series>. Make sure to configure settings like “concurrent streams”, “split data stream every”, and “data stream size” to their original settings.

10 On the Storage tab, right-click the added container, and click the **Inventory and Catalog now** option.



This will automatically start and can be monitored in your list of jobs under Job Monitor.



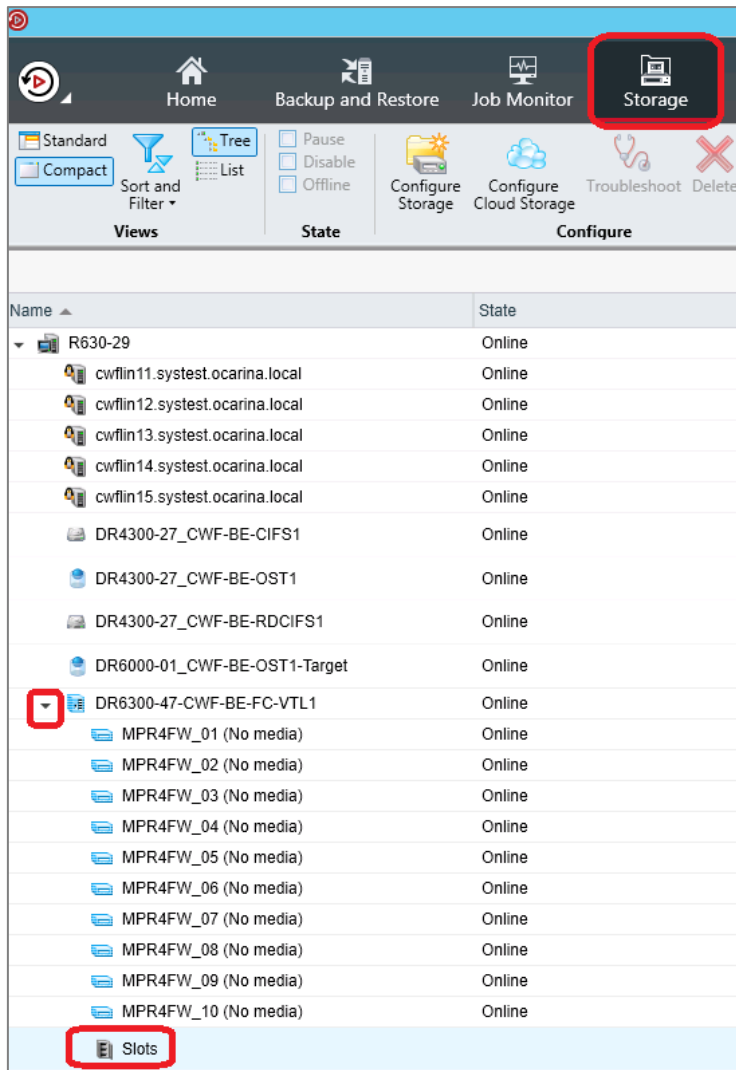
- 11 After the inventory/catalog finishes, highlight the jobs that used to be targeted to the original container.
- 12 Edit them and configure their full, incremental, or duplicate jobs to the newly added container.

Migrating VTL containers

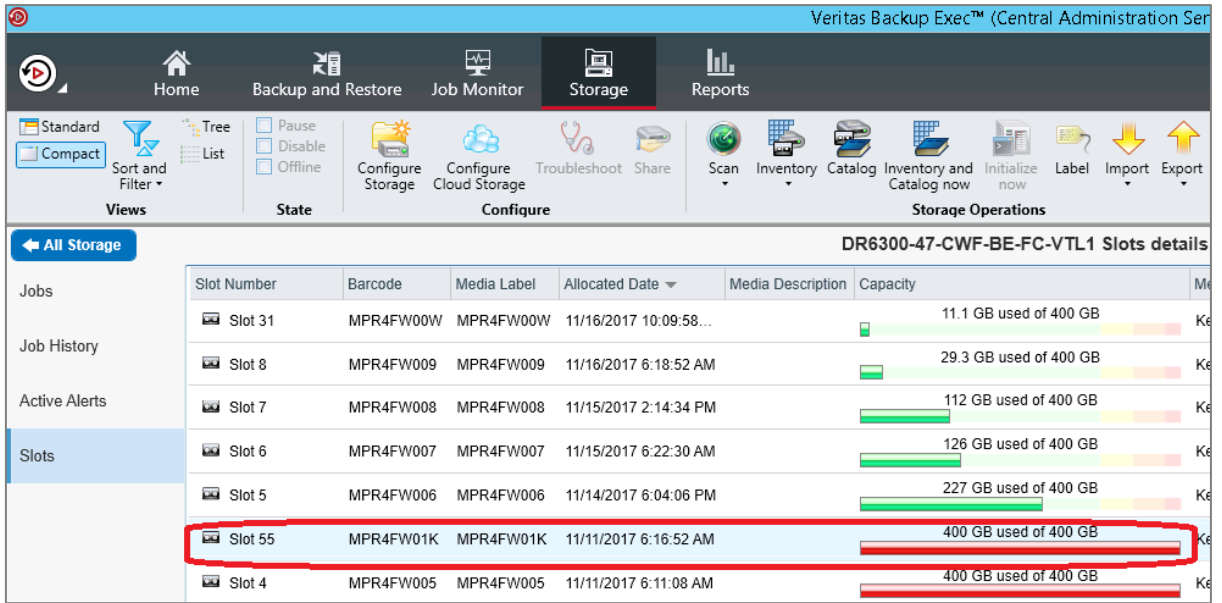
The protocol used to connect the VTL container does not affect the migration process. VTL containers cannot simply be re-added as a different library type, which means that a new container of a Quest type must be created to change library types. Once the new library is added, it is recommended that you allow the old VLT backup sets to expire naturally. Then, remove the library from Backup Exec and the container from the DR appliance once retention is met completely. The only alternative is to run duplicate jobs on backup sets per tape within backup exec.

If you cannot allow retention to meet over time and are forced to duplicate tapes, you can use the following example:

- 1 Create and add the new Quest branded library in Backup Exec. Follow the Backup Exec whitepaper if step-by-step instructions are needed for this process.
- 2 Open the Backup Exec Console, and navigate to the Storage Tab. Find the library to be migrated from and expand it. Find the slots section under that library and double click on it.

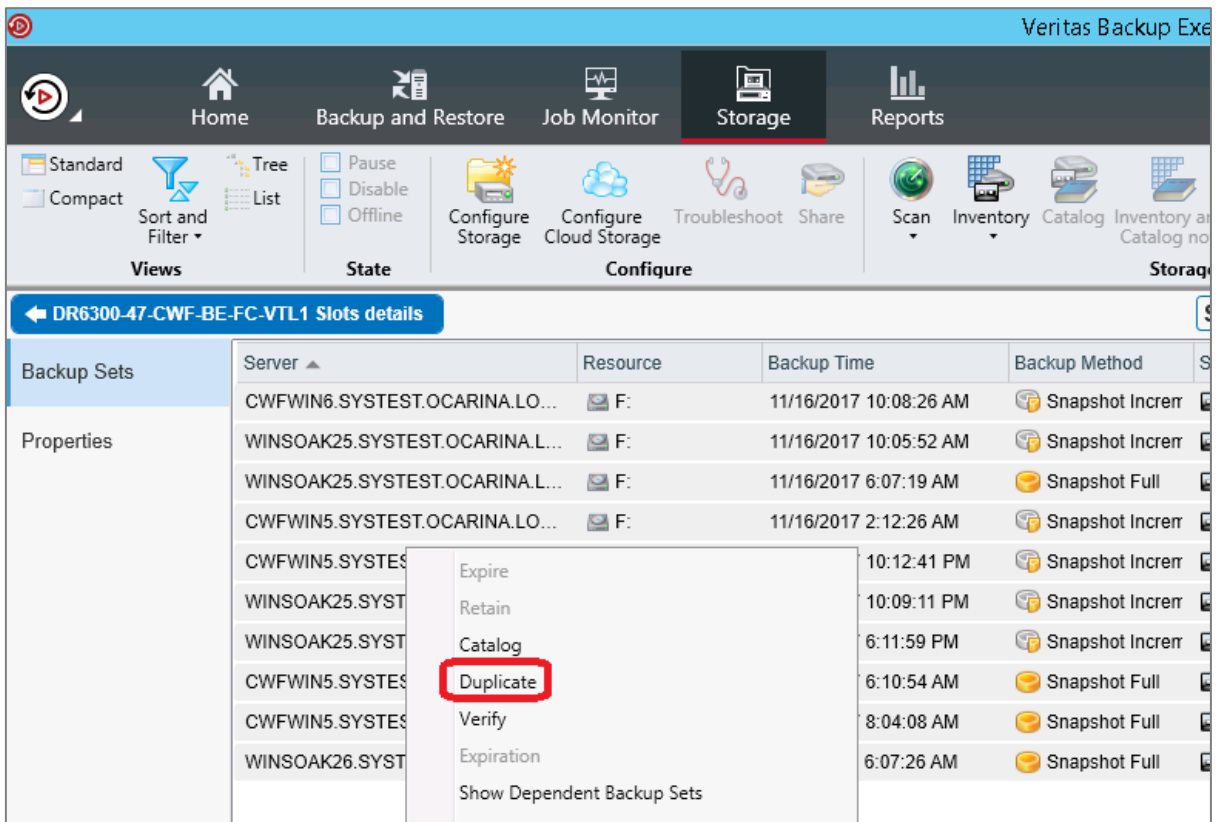


- 3 In the Slots screen it can be useful to organize the media by the “Allocated Date” column, which will bring all the tapes currently under retention to the top. This screen can be useful to define a list of tapes to be copied by barcode. Once this is done pick one of the tapes and double-click it.

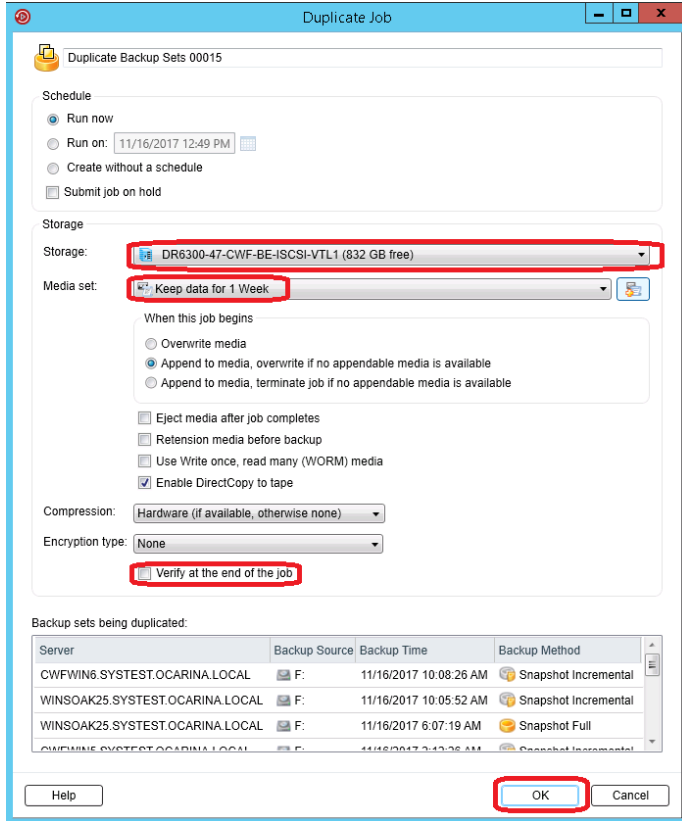


i **NOTE:** In Backup Exec it is usually possible to copy multiple rows via Ctrl-C and paste into a spreadsheet tool. This is also useful for generated a list of tapes to be migrated.

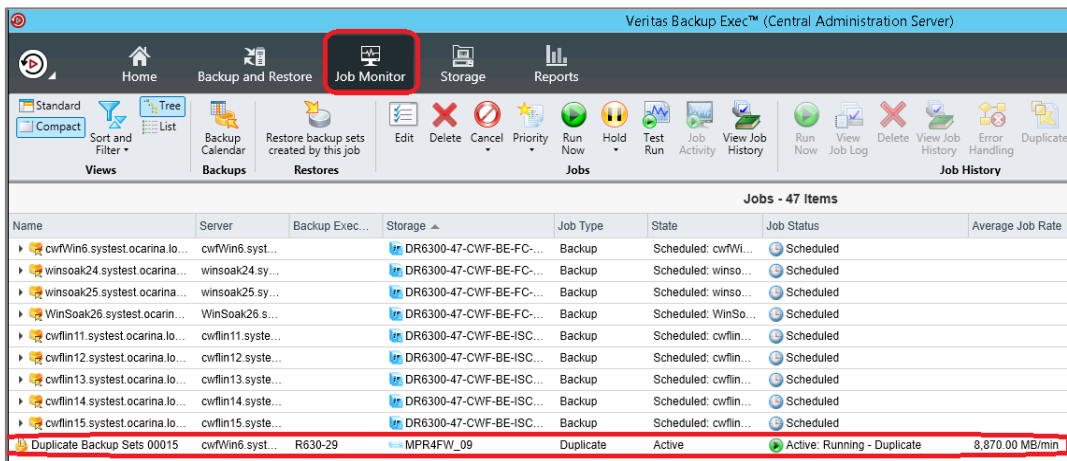
- 4 On this screen highlight **all** the backup sets stored on this tape. This may include multiple backups if this tape was appended to. Right click and select the Duplicate option.



- In the Duplicate Job window, select the newly added Quest Library under the Storage drop-down. Also, select the media set. Remember that in Backup Exec media sets define retention. There is no way to continue the backup set current retention; this action will reset retention to the settings of the new media set. Because of this, you might want to create a newer, short media set. Disabling the “Verify at the end of the job” check box can also save on duplication job runtime. Click OK.



- At this point, you can monitor the duplication under the Job Monitor tab for completion.



- Repeat this process for each tape to be copied. Depending on the number of tapes this can be time consuming.
- After copying all available tapes, do not forget to modify your jobs to point to the newly created library. Then Disable and Delete the old library from Backup Exec and the VTL container from the DR appliance.

Veritas NetBackup

Veritas NetBackup generally requires that a secondary container be created to migrate. For OST, the NetBackup database only allows a Storage Server to be added as one type at a time.

Migrating OST containers

It is not possible to mount the same storage server twice in a NetBackup cell using the same hostname or IP address. This is because these fields are shared and are required to be unique in the NetBackup database. This limitation is the same as adding a NDMP server with the same hostname or IP as a storage server

https://www.veritas.com/support/en_US/article.000018018

The most functional way to migrate involves removing and re-adding the Storage Server then running a manual inventory process, which can be time consuming depending on the number of images. The Storage Server cannot be removed without first removing all the storage units and disk pools associated with the storage server, and this cannot be done with OST images left unexpired. Because of the complicated nature of this it is highly recommended that Veritas NetBackup support personnel assist with the migration, if it is absolutely necessary.

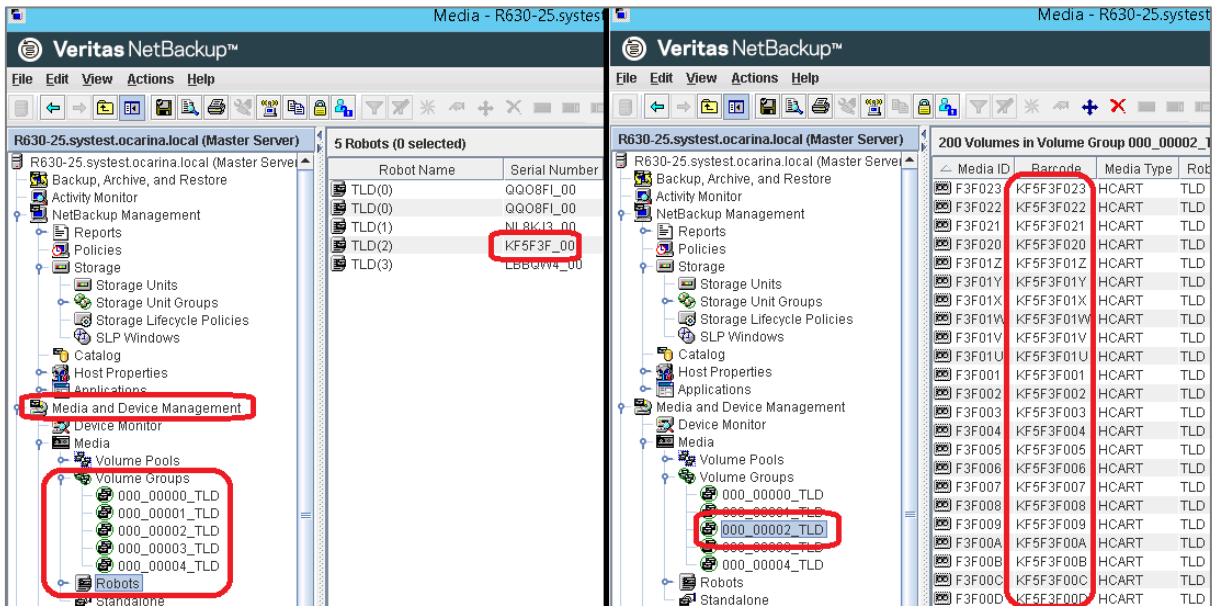
Migrating VTL containers

The protocol used to connect the VTL container does not affect the migration process. VTL containers cannot be re-added as a different library type, which means that a new container of a Quest type needs to be created to change library types. Once the new library is added, it is recommended that you allow the old VLT backup sets to expire naturally. Then remove the old library from NetBackup and the container from the DR appliance once retention is met completely. The only alternative is to run duplicate jobs on backup sets per tape within NetBackup.

If you cannot allow retention to meet over time and are forced to duplicate tapes, you can use the following example:

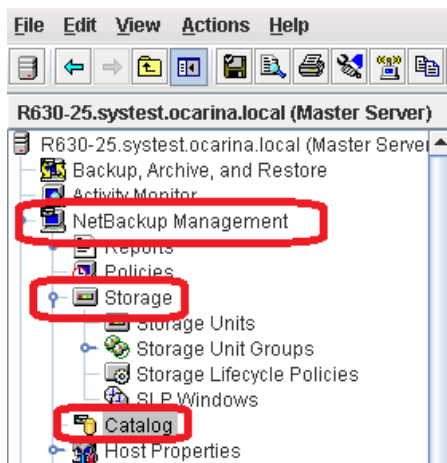
- 1 Create and add the new Quest branded library in NetBackup. Follow the instructions in the Veritas NetBackup setup whitepaper if step-by-step instructions are needed for this process.
- 2 Open the NetBackup Administration Console, expand Media and Device Management, then select Media. Identify the library to be migrated and the Volume Group in which the media resides by checking the

library serial number and the Barcodes listed in the Volume Group. In the example notice how the library starts with a serial number **KF5F** and all of the tapes begin **KF5F**. You can also use the Volume Groups panel to develop a list of tapes to be migrated. Confirm the “Time Assigned” column is not blank, which suggests the media is currently in use.



i **NOTE:** In NetBackup it is usually possible to copy multiple rows via Ctrl-C and paste into a spreadsheet tool. This is also useful for generated a list of tapes to be migrated.

3 Expand the NetBackup Management and Storage sections and then select **Catalog**.



4 Do the following:

- a Set the Action dropdown to **Duplicate**.
- b Select the “Media ID:” radio button and then enter or find the Media ID that matches a barcode to be copied.

- c Select a from and to time range under “Date/Time Range” that covers the complete retention of that tape. There is no harm in setting the from date to an extremely distant date.
- d Leave other options set at the default settings, and click **Search Now**. There may be multiple search results as multiple backups may be appended to the same tape.
- e Select them all and then right-click and select **Duplicate...**

Action:
Duplicate

Media:
 Media ID: F3F023
 Media host: <All Media Hosts>
 Disk Type: BasicDisk
 Disk pool: <All>
 Media server: <All Media Hosts>
 Path: <All>

Copies:
 Primary Copy
 Policy name: <All Policies>
 Policy type: <All Policy Types>
 Type of backup: <All Backup Types>
 Client (host name): <All Clients>

Date/Time Range:
 From: Nov 13, 2004 12:10:24
 To: Nov 14, 2017 11:59:59

Job Priority:
 Override default priority
 Job Priority: 75000
 (higher number is greater priority)

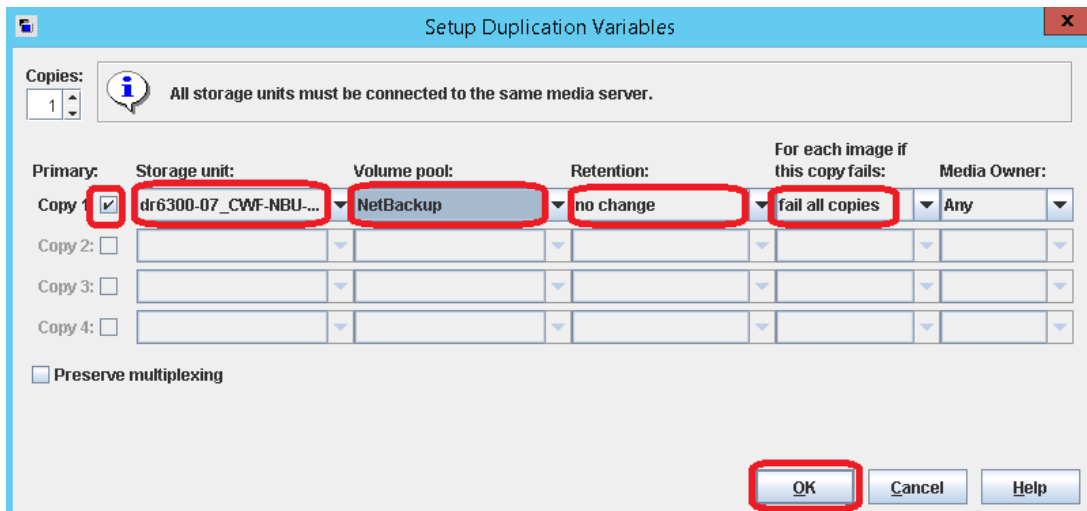
Buttons: Help, Search Now

Search Results: 7 backup image(s) found (7 selected)

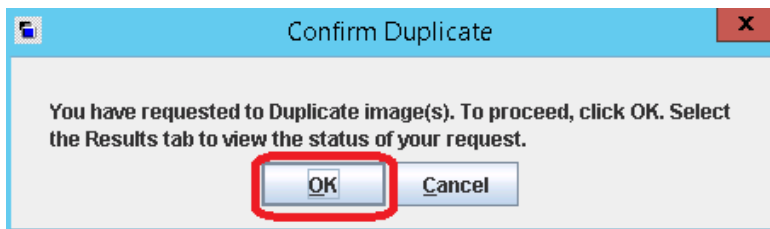
Backup ID	Date	Policy	Schedule Name	Media Server	Media ID	Copy Number	Primary Cop
cwfw3_1510...	Nov 8, 2017 10:...	CWF-FC	Full	r630-25.systemst...	F3F023	1	Yes
cwfw4_1510...	Nov 8, 2017 8:0...	CWF-FC	Full	r630-25.systemst...	F3F023	1	Yes
cwfw4_1510...	Nov 8, 2017 4:0...	CWF-FC	Incr	r630-25.systemst...	F3F023	1	Yes
cwfw4_1510...			Incr	r630-25.systemst...	F3F023	1	Yes
cwfw4_1510...			Incr	r630-25.systemst...	F3F023	1	Yes
cwfw4_1510...			Incr	r630-25.systemst...	F3F023	1	Yes
cwfw4_1510...			Incr	r630-25.systemst...	F3F023	1	Yes

Context menu options: Verify..., Duplicate..., Expire..., Initiate Import...

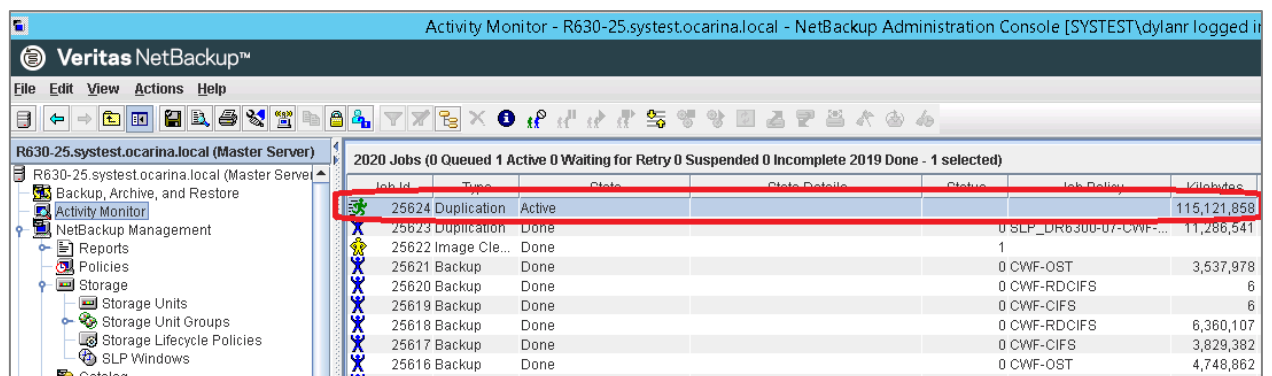
- 5 In the Duplication screen, do the following:
- a Select the Primary Check box.
 - b Select the new Quest VTL storage unit in the Storage Unit drop down.
 - c Set a volume pool to use. Unless manual volume pools have been created the NetBackup volume pool is usually correct.
 - d Select No Change under the Retention drop-down, unless retention modification is needed.
 - e Quest also suggests to use the “Fail all copies” option under “for each image if this copy fails.” This will cause the job to fail if a single backup fails to copy to a new tape.
 - f Click the OK button once finished.



- Click OK on the Confirm Duplicate dialog box.



- You can monitor individual tape duplication in the Activity Monitor section.



- Repeat this process for each tape to be copied. Depending on the number of tapes this can be time consuming.
- After copying all available tapes do not forget to modify your policies to point to the newly created library. Then, delete the old library from NetBackup and the VTL container from the DR Series system appliance.

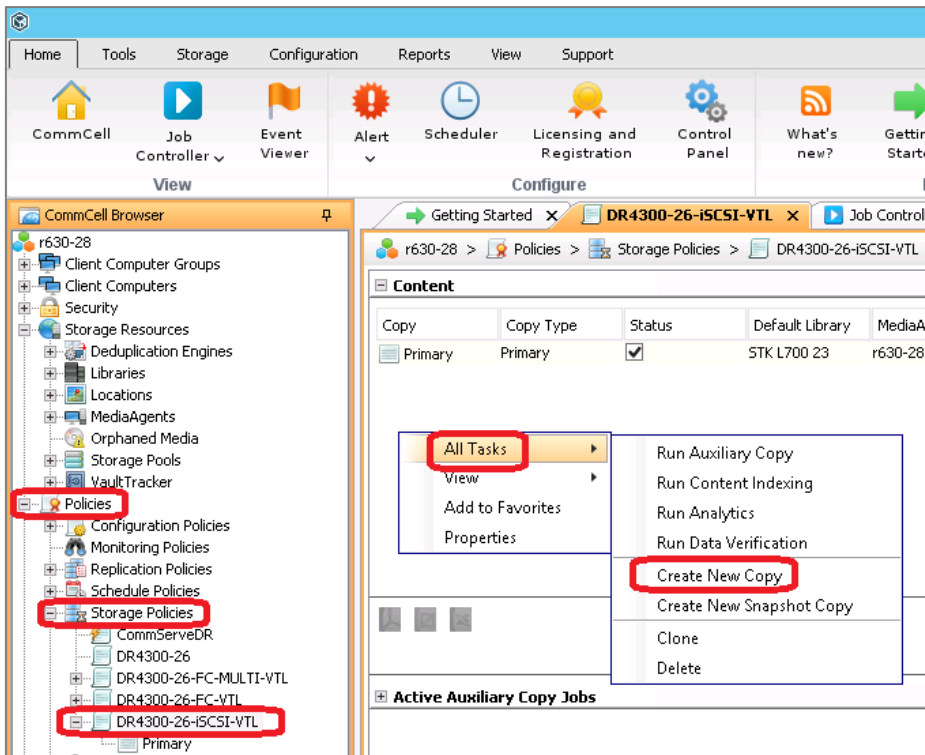
CommVault

Migrating VTL containers

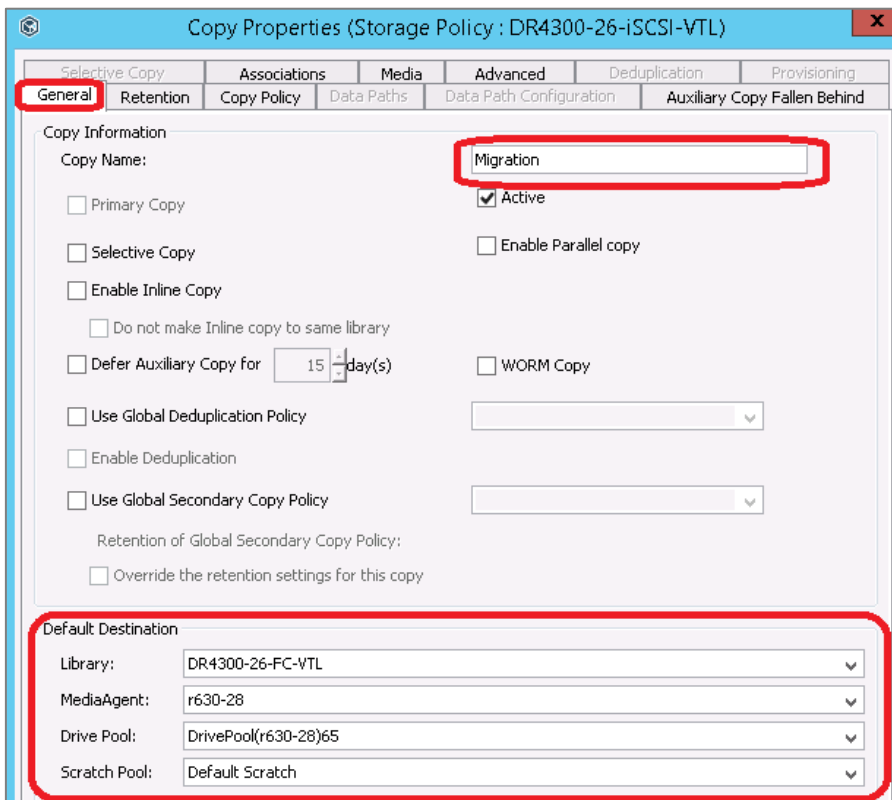
The protocol used to connect the VTL container does not affect the Migration process. VTL containers cannot simply be re-added as a different library type. This means that a new container of a Quest type needs to be created to change library types. Once the new library is added it is recommended that you allow the old VLT backup sets to expire naturally. Then remove the old library from CommVault and the container from the DR appliance once retention is met completely. The only alternative is to run a Synchronous Copy per Storage Policy utilizing the VTL to be migrated. Other actions, like Media Refresh, cannot work because they're intended to be used within the same library instead of copying between libraries.

If you cannot allow retention to meet over time and are forced to Synchronous Copy tapes you can use the following example:

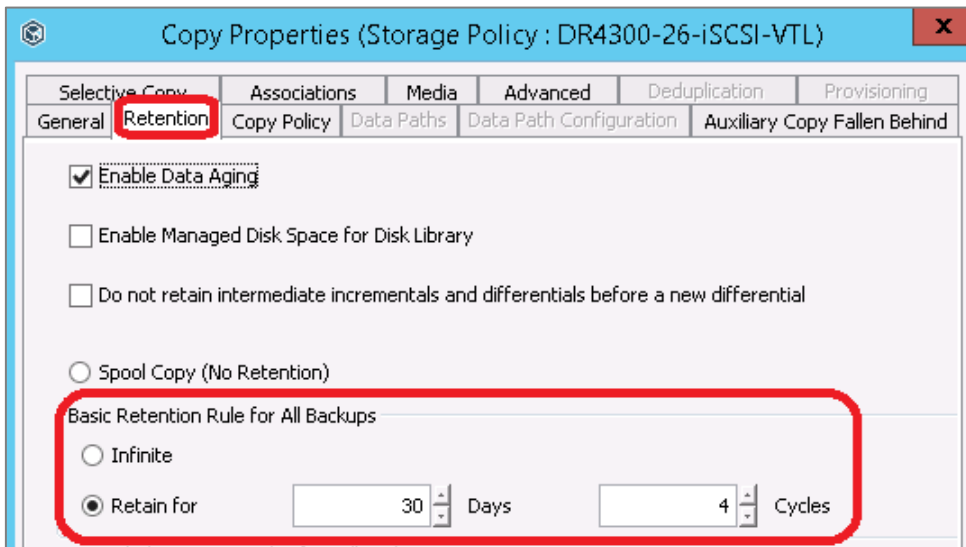
- 1 Create and add the new Quest branded library in CommVault. Follow the CommVault whitepaper if step by step instructions are needed for this process.
- 2 Open the CommCell Console, and do the following:
 - a Expand Polices and then Storage Polices.
 - b Find a policy currently using the VTL to be migrated.
 - c Select that policy and in the content tab, right-click the white space below your copies.
 - d Select "All Tasks" and click "Create New Copy."



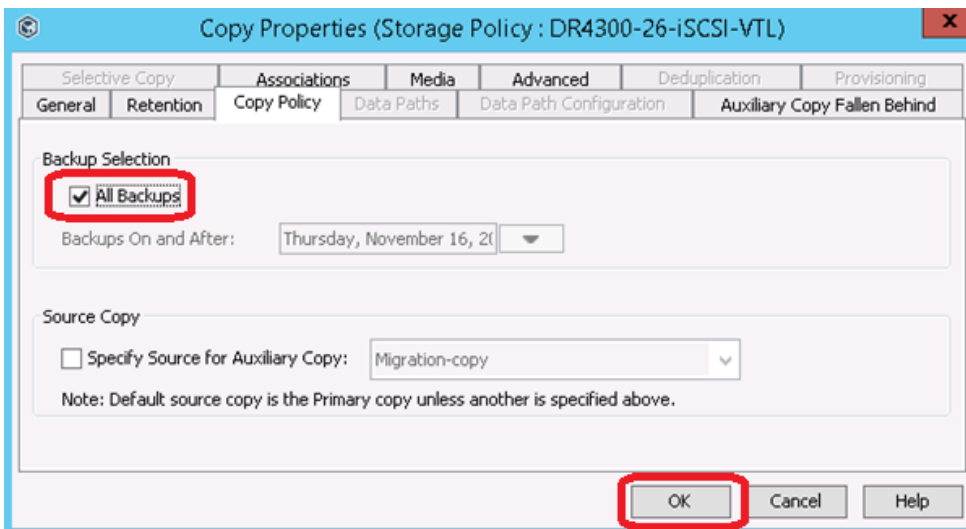
- 3 On the General tab, do the following: (but do not select any of the copy type check boxes).
 - a Set the Default Destination library to the newly added Quest VTL, making sure to pick the appropriate Media Agent, Drive Pool, and Scratch Pool.
 - b You will also need to enter a Copy Name.



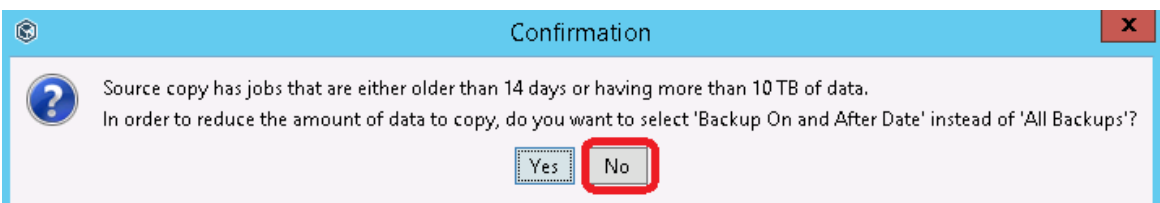
- 4 Under the Retention tab, select the desired retention for the copied backups. Note that you cannot continue the previous retention used by the backup. Because of this, it might be logical to get this retention to shorter than normally required.



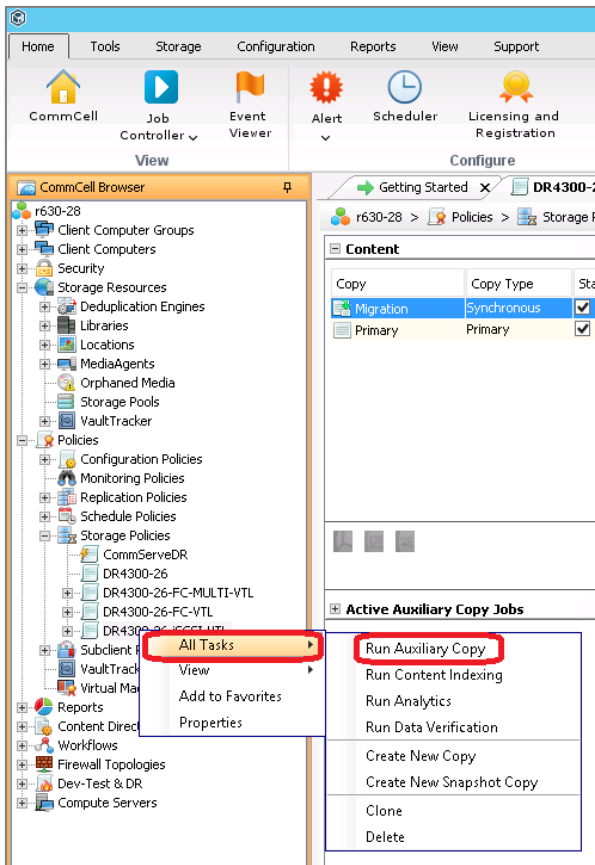
- 5 In the Copy Policy section, select the check box for “All Backups,” unless you specifically need a different range, and click the OK button.



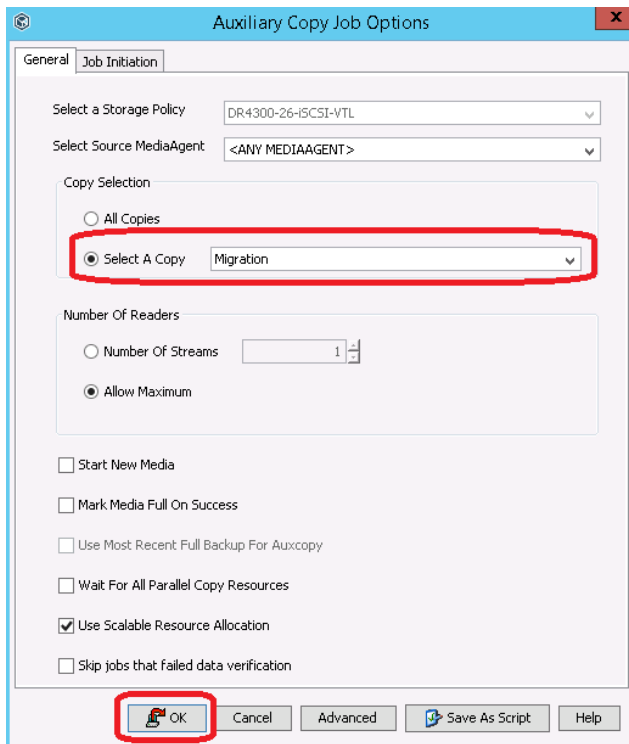
- 6 If the policy is large enough, a confirmation notice might appear, suggesting the jobs are older than 14 days or it will be copying more than 10TB. Click “No” to proceed with the current settings.



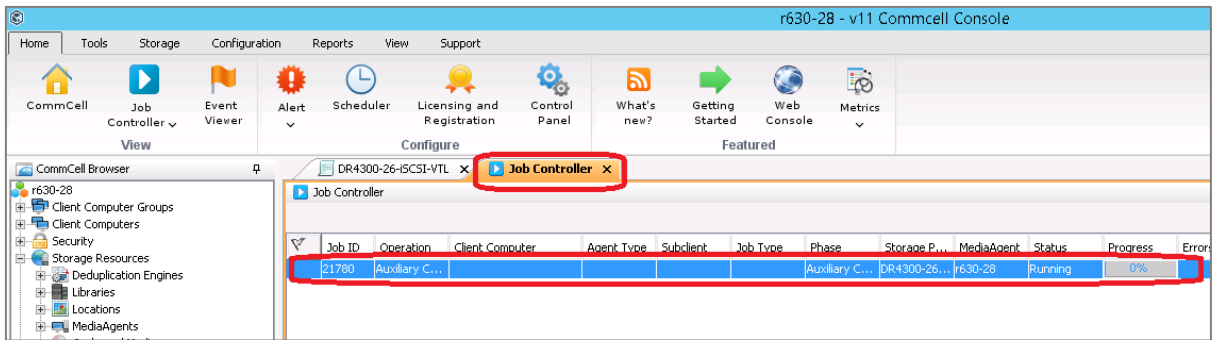
7 Right-click the Storage Policy, select “All Tasks,” and then click “Run Auxiliary Copy.”



8 Click the “Select a Copy” radio button, select the newly created synchronous copy by name in the drop down, and then click OK.



9 You can view the status of the copy from the Job Controller.



- 10 Repeat this process for each policy to be copied. Depending on the number of policies and the total amount of data this can be time consuming.
- 11 After copying all the policies, do not forget to modify your primary copies to point to the newly created library. Then, delete the old library from CommVault and the VTL container from the DR Series appliance.

Quest NetVault

Migrating RDA containers

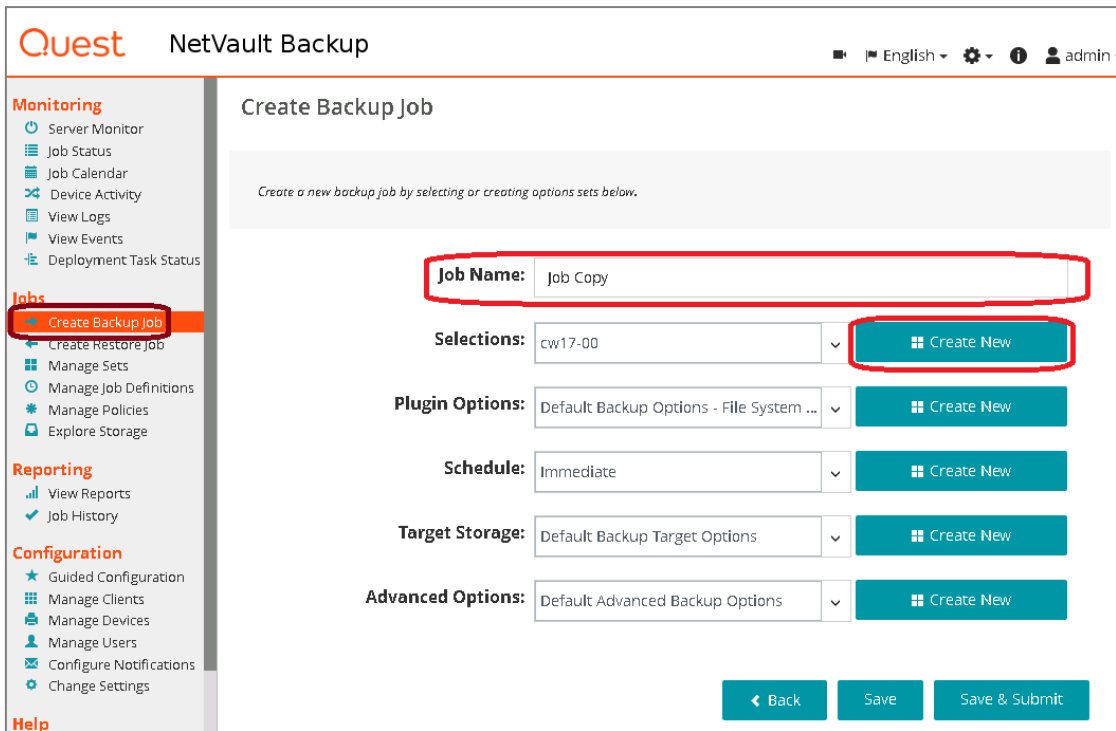
There is no need to migrate data in RDA containers. After upgrading the DR Series system appliance and upgrading to NetVault 11.4.5.11 or later, all previous RDA devices will be converted to Quest branding automatically. Just ensure that you update both the DR Series system operating system (OS) and the NetVault server.

Migrating VTL containers

The protocol used to connect the VTL container does not affect the migration process. VTL containers cannot be re-added as a different library type, which means that a new container of a Quest type needs to be created to change library types. Once the new library is added, it is recommended that you allow the old VLT backup sets to expire naturally. Then, remove the old library from NetVault and the container from the DR Series appliance once retention is met completely. The only alternative is to run a Data Copy Job per Saveset with the VTL to be migrated.

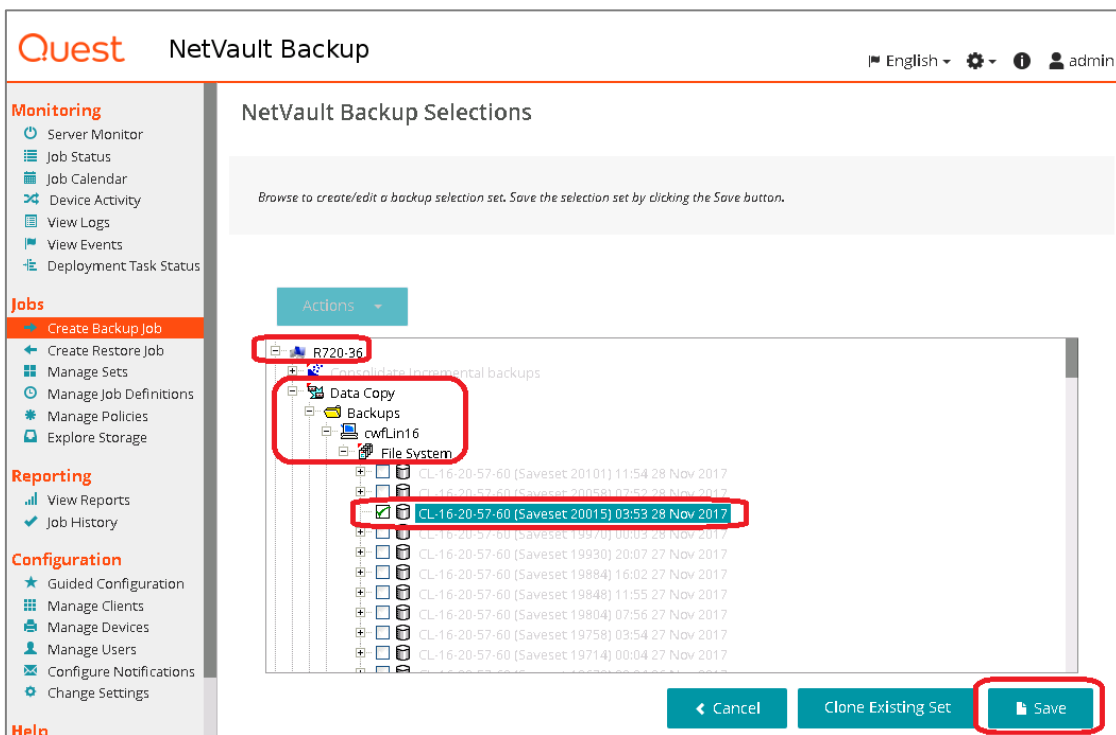
If you cannot allow retention to meet over time and are forced to do Data Copy Jobs, you can use the following example:

- 1 Create and add the new Quest branded library in NetVault. Follow the instructions in the DR Series system NetVault setup whitepaper if step-by-step instructions are needed for this process.
- 2 Open the NetVault web GUI, and click **Create Backup Job**. Enter a name for the Job and click **Create New**.



3 Do the following:

- a Expand the server/smart client with the libraries attached.
- b Expand the Data Copy plugin, and then the Backups folder.
- c Expand the client that was backed up and the plugin used to do the backup, in this case, File System.
- d Select one of the savesets (only one can be selected at a time), and click the Save button.



- 4 Name the selection set, and click **Save**.

Create New Set

data copy

Confirm set creation

Cancel Save

- 5 Set the Target Storage device to the newly created VTL and the Advanced Options to a retention set you prefer. The retention for this copied job will start over, and the retention is defined here. If you do not want to restart the full retention, a shorter than normal retention can be defined in a new Advanced Options set. For information on creating sets, refer to the DR Series system NetVault setup whitepaper and the NetVault specific documentation.
- 6 Click **Save & Submit**.

Quest NetVault Backup

English

admin

Create Backup Job

Create a new backup job by selecting or creating options sets below.

Job Name: Job Copy

Selections: data copy **Create New**

Plugin Options: Default Backup Options - Data Copy - ... **Create New**

Schedule: Immediate **Create New**

Source Storage: Any Device **Create New**

Target Storage: DR4300-04-FC-VTL **Create New**

Advanced Options: 1-month **Create New**

Navigation: < Back Save **Save & Submit**

- Monitoring**
 - Server Monitor
 - Job Status
 - Job Calendar
 - Device Activity
 - View Logs
 - View Events
 - Deployment Task Status
- Jobs**
 - Create Backup Job**
 - Create Restore Job
 - Manage Sets
 - Manage Job Definitions
 - Manage Policies
 - Explore Storage
- Reporting**
 - View Reports
 - Job History
- Configuration**
 - Guided Configuration
 - Manage Clients
 - Manage Devices
 - Manage Users
 - Configure Notifications
 - Change Settings
- Help**

7 You can now monitor the Data Copy progress in the job Status page.

The screenshot shows the Quest NetVault Backup interface. On the left is a navigation menu with sections: Monitoring (Server Manager, Job Status, Job Instance, Device Activity, View Logs, View Events, Deployment Task Status), Jobs (Create Backup Job, Create Restore Job, Manage Sets, Manage Job Definitions, Manage Policies, Explore Storage), Reporting (View Reports, Job History), Configuration (Guided Configuration, Manage Clients, Manage Devices, Manage Users, Configure Notifications, Change Settings), and Help (Documentation, Video and Tutorials). The main area shows 'Job Activity' with three charts: 'Current Activity' (Active, Pending, Scheduled), 'Policies' (Healthy, Warnings, Errors), and 'Regular Jobs' (Healthy, Warnings, Errors). Below the charts is a table titled 'Showing: All waiting jobs' with a search filter. The table has the following columns: Start Time, Job Title, Client, Type, ID / Instance / Phase, Next runtime, Progress, Current Status, and Last Exit Status. The first row is highlighted with a red border.

Start Time	Job Title	Client	Type	ID / Instance / Phase	Next runtime	Progress	Current Status	Last Exit Status
11/28/2017 1:28 ...	Job Copy	R72D-36	Backup	201 (Instance 1, P...	Never	0.00 MB (0.00 GB)	Running; Wait...	Not Known
11/24/2017 3:00 ...	CL-41-56 (D9430...	cwLin56	Backup	139 (Instance 191...	11/28/2017 3:00 ...	99.25 GB (99 GB)	Running; Wait...	Backup Compl...
11/24/2017 3:00 ...	CL-41-56 (D9430...	cwLin53	Backup	142 (Instance 191...	11/28/2017 3:00 ...	100.65 GB (101 ...)	Running; Wait...	Backup Compl...
11/24/2017 3:00 ...	CL-41-56 (D9420...	cwLin45	Backup	134 (Instance 191...	11/28/2017 3:00 ...	100.34 GB (100 ...)	Running; Wait...	Backup Compl...
11/24/2017 3:00 ...	CL-41-56 (D9430...	cwLin46	Backup	135 (Instance 191...	11/28/2017 3:00 ...	100.57 GB (100 ...)	Running; Wait...	Backup Compl...
11/24/2017 3:00 ...	CL-41-56 (D9430...	cwLin47	Backup	136 (Instance 191...	11/28/2017 3:00 ...	99.95 GB (100 ...)	Running; Wait...	Backup Compl...
11/24/2017 3:00 ...	CL-41-56 (D9430...	cwLin52	Backup	141 (Instance 191...	11/28/2017 3:00 ...	100.00 GB (100 ...)	Running; Wait...	Backup Compl...

8 Repeat this process for each Saveset to be copied. Depending on the number of Savesets, this can be time consuming.

9 After copying all available data do not forget to modify your jobs to point to the newly created library. Then, delete the old library from NetVault and the VTL container from the DR Series appliance.

Quest vRanger

Migrating RDA containers

There is no need to migrate data in RDA containers. After upgrading the DR Series system appliance and upgrading to vRanger 7.6.4.0 or later, all previous RDA devices will be converted to Quest branding automatically. Just be sure to update both the DR Series operating system and the vRanger server.