

Setting Up QoreStor as a CommVault Backup Target

Technical White Paper

Quest Engineering

February 2023



© 2023 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>. 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 QoreStor as a CommVault Backup Target

Updated – February 16, 2023

Contents

Configuring QoreStor as a CIFS/NFS Magnetic Library	5
Creating a CIFS container for use with CommVault	5
Adding the QoreStor CIFS container as a Magnetic Library in CommVault	7
Creating a NFS container for use with CommVault	9
Adding the QoreStor NFS container as a Magnetic Library in Commvault	11
Configuring Rapid CIFS with CommVault.....	13
Windows prerequisites.....	13
Installing Rapid CIFS on a CommVault Windows media agent	13
Configuring Rapid NFS with Commvault	16
Linux prerequisites	16
Installing Rapid NFS on a CommVault Linux media agent.....	16
Setting up QoreStor system replication	18
Creating a CIFS/NFS replication session.....	18
Setting up a CommVault Replica Library	20
Using QoreStor as a Cloud Storage in CommVault	28
Creating an Object Container(S3) in QoreStor.....	28
Adding the QoreStor Object Container(S3) to CommVault	31
Performance Tier.....	32
Setting up Performance Tier with QoreStor	33
Cloud/Archive Tier	35
Cloud Tier.....	35
Important Considerations for Cloud Tier with CommVault.....	35
Setting up Cloud Tier.....	37
Archive Tier.....	40
Important Considerations for Archive Tier with CommVault.....	40
Setting Up Archive Tier	40
Setting up the QoreStor system cleaner	43
Monitoring deduplication, compression and performance	45

Executive Summary

This document provides information about how to set up QoreStor software with CommVault, including:

- Configuring the QoreStor system as a CIFS/NFS storage unit for CommVault 10 and 11.

For additional information, see the QoreStor documentation and other data management application best practices whitepapers at:

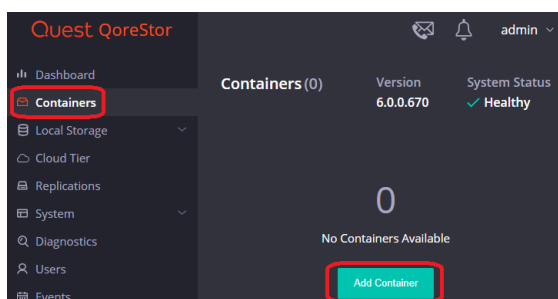
<https://support.quest.com/qorestor/>

i | **NOTE:** The QoreStor/CommVault build version and screenshots used for this paper may vary slightly, depending on the version of QoreStor/CommVault software you are using.

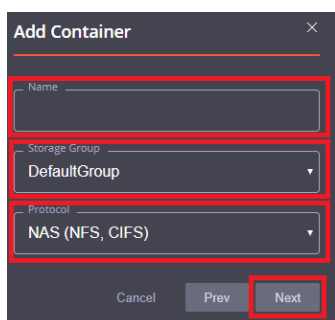
Configuring QoreStor as a CIFS/NFS Magnetic Library

Creating a CIFS container for use with CommVault

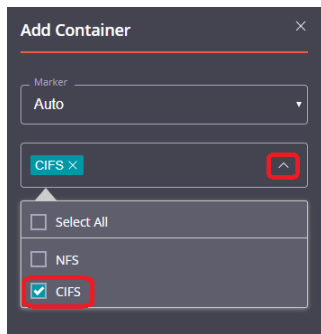
- 1 Select the **Containers** tab, then click **Add container**.



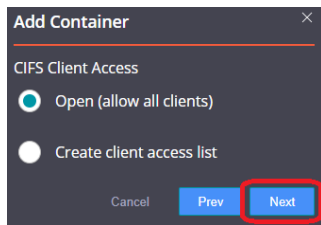
- 2 Enter a container **Name**, select a **Storage Group** or leave the **DefaultGroup** option selected, and select **NAS (NFS, CIFS)** from the **Protocol** dropdown menu. Click **Next**.

A screenshot of the 'Add Container' dialog box. It has a title bar with 'Add Container' and a close button. There are three input fields: 'Name' (a text box), 'Storage Group' (a dropdown menu with 'DefaultGroup' selected), and 'Protocol' (a dropdown menu with 'NAS (NFS, CIFS)' selected). At the bottom, there are three buttons: 'Cancel', 'Prev', and 'Next' (highlighted with a red box).

- 3 Click the dropdown on the **Protocols** field then select the check mark for **CIFS**. Leave **Marker Type** on **Auto**, then click **Next**.

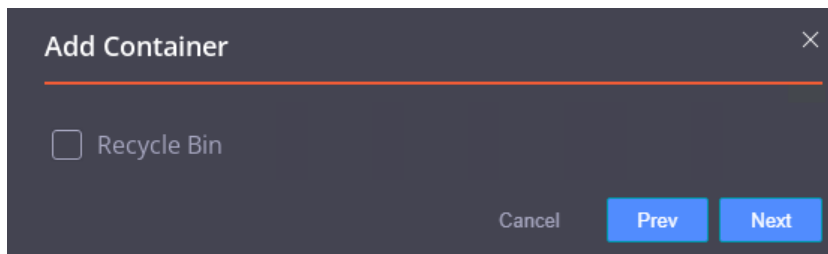


- 4 Fill in the **CIFS Client Access** options if needed then click **Next**.

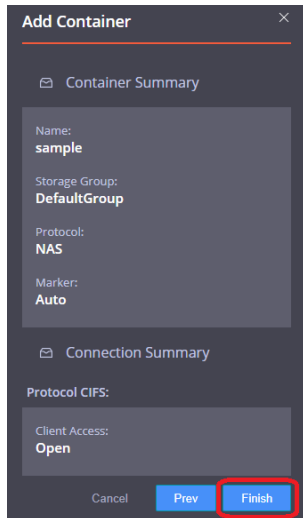


i **NOTE:** For improved security, Quest recommends adding IP addresses for only CommVault media servers.

- 5 On this page, the Recycle Bin feature may be enabled, please check the user guide for more information. Click **next**.



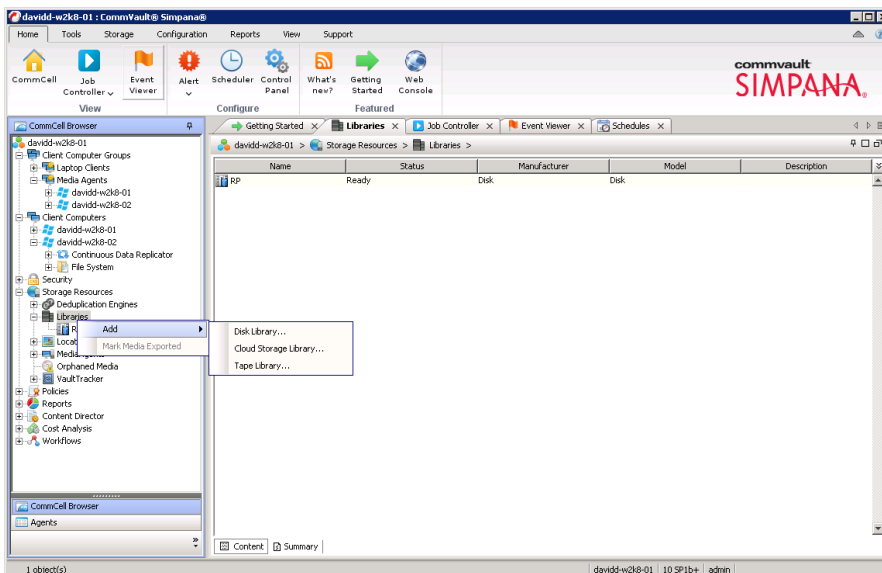
- 6 Confirm the settings and click **Finish**. Confirm that the container is added.



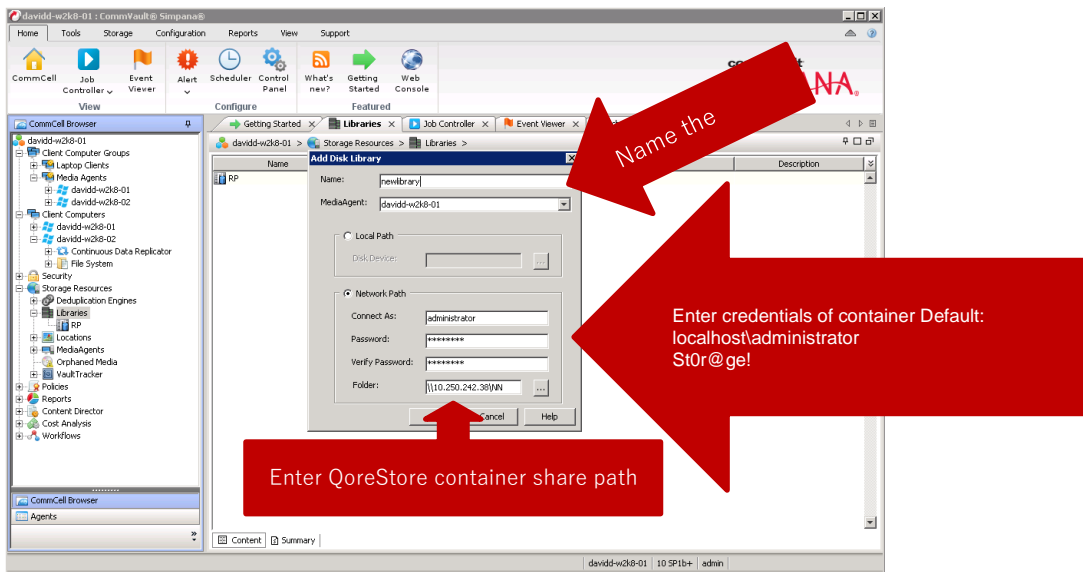
Adding the QoreStor CIFS container as a Magnetic Library in CommVault

Follow these steps to add the container to CommVault.

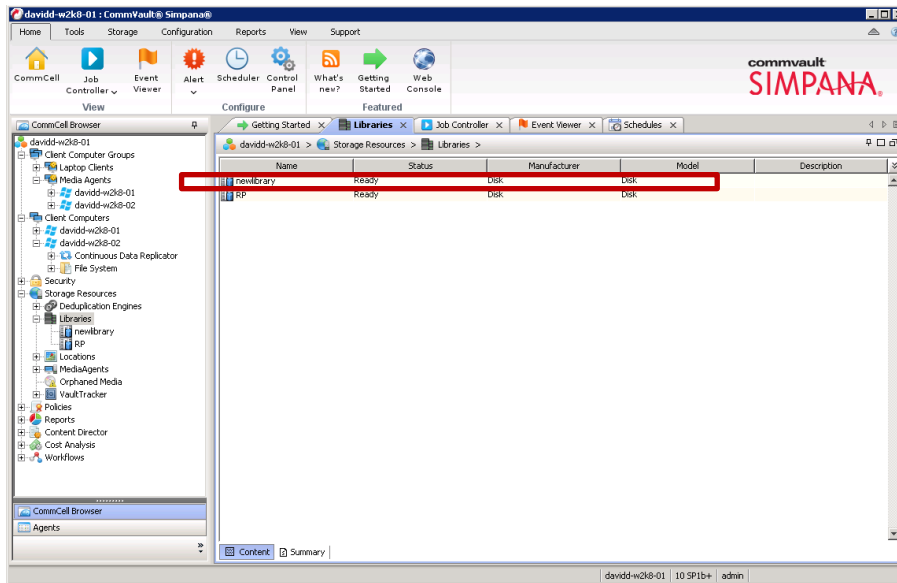
- 1 Open the Commcell Console, expand Storage Resources, right-click Libraries, and select Add → DiskLibrary...



- 2 In the Add Disk Library dialog box, enter a name for the Disk Library and information about the QoreStor container, and click OK.

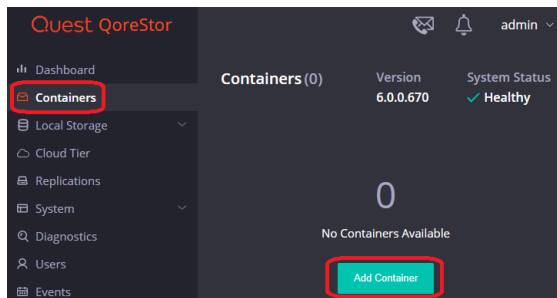


- 3 Confirm that the library is created and that the status is Ready.

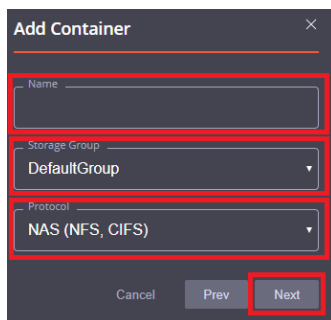


Creating an NFS container for use with CommVault

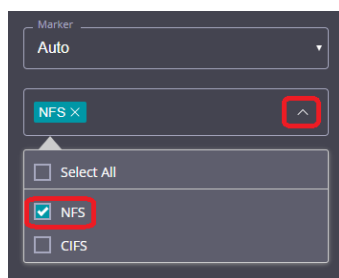
- 1 Select the **Containers** tab, then click **Add container**.



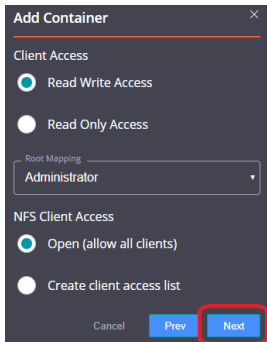
- 2 Enter a container **Name**, select a **Storage Group** or leave the **DefaultGroup** option selected, and select **NAS (NFS, CIFS)** from the **Protocol** dropdown menu. Click **Next**.



- 3 Click the dropdown on the **Access Protocols** field then select the check mark for **NFS**. Leave **Marker Type** on **Auto**, then click **Next**.



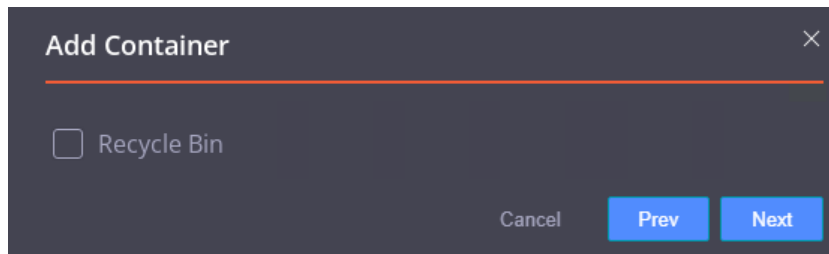
- 4 Fill in the **NFS Client Access** options if need then click **Next**



The screenshot shows the 'Add Container' dialog box. Under 'Client Access', 'Read Write Access' is selected. Under 'NFS Client Access', 'Open (allow all clients)' is selected. The 'Root Mapping' dropdown is set to 'Administrator'. At the bottom, the 'Next' button is highlighted with a red box.

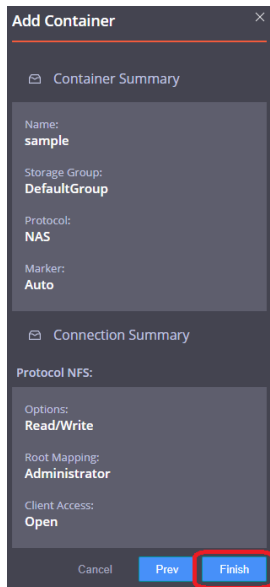
i **NOTE:** For improved security, Quest recommends adding IP addresses for only CommVault Media servers

- 5 On this page, the Recycle Bin feature may be enabled, please check the user guide for more information. Click **Next**.



The screenshot shows the 'Add Container' dialog box with the 'Recycle Bin' checkbox unchecked. The 'Next' button is highlighted with a red box.

- 6 Confirm the settings and click **Finish**. Confirm that the container is added.



The screenshot shows the 'Add Container' dialog box with the 'Container Summary' and 'Connection Summary' sections. The 'Container Summary' shows Name: sample, Storage Group: DefaultGroup, Protocol: NAS, and Marker: Auto. The 'Connection Summary' shows Protocol NFS, Options: Read/Write, Root Mapping: Administrator, and Client Access: Open. At the bottom, the 'Finish' button is highlighted with a red box.

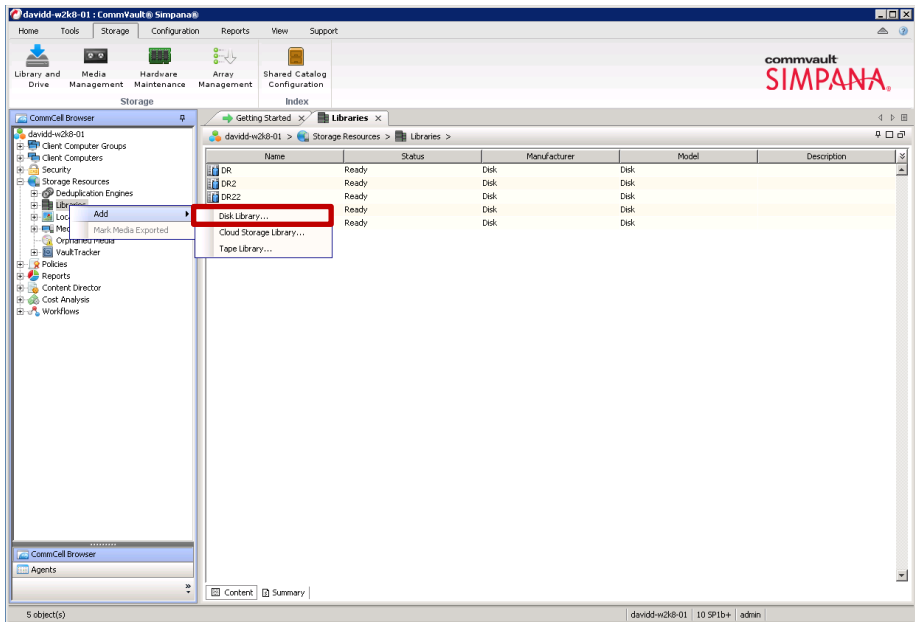
Adding the QoreStor NFS container as a Magnetic Library in Commvault

- 1 Mount the QoreStor container NFS export onto a Unix/Linux Media Agent

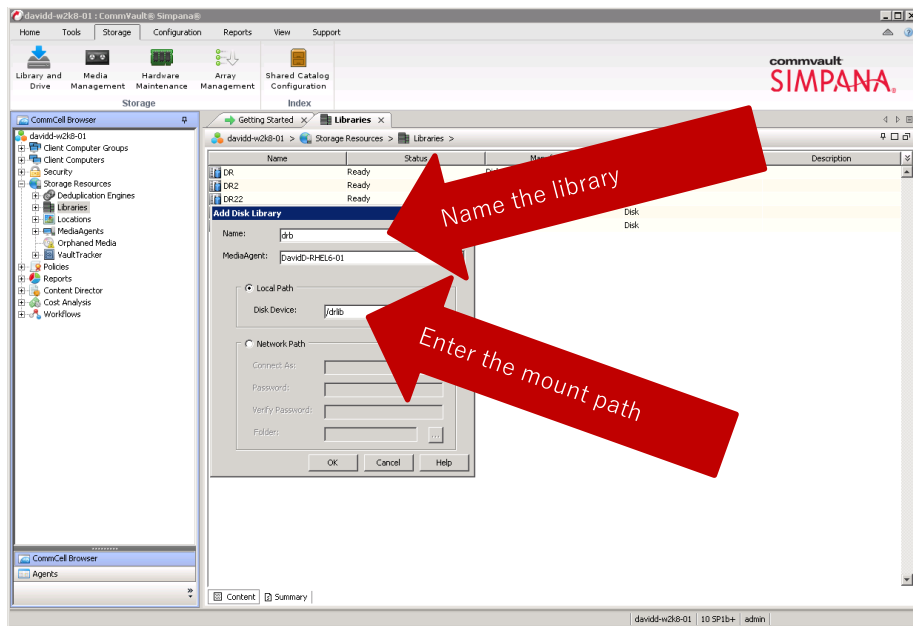
```
[root@r320-sys-41 ~]#  
[root@r320-sys-41 ~]# mkdir /mnt/sample  
[root@r320-sys-41 ~]# mount -t nfs 6300-07:/containers/sample /mnt/sample  
[root@r320-sys-41 ~]#
```



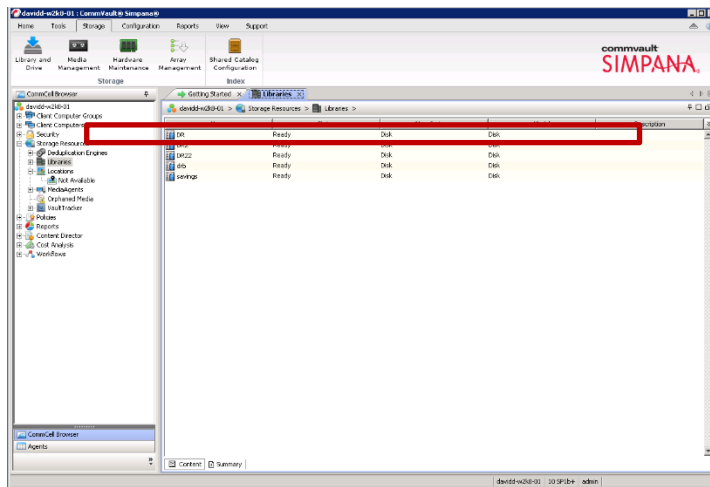
- 2 Open the CommCell Console, expand Storage Resources, right-click Libraries, and select Add -> DiskLibrary...



- 3 In the Add Disk Library window, enter the name for the Disk Library and the mount path of the QoreStor container export, and click OK.



- 4 Confirm that the library is created, and the Status is Ready.



Configuring Rapid CIFS with CommVault

Rapid CIFS is a Quest-developed protocol that accelerates writes to CIFS shares on the QoreStor system. This is done by only sending unique data to the appliance. This usually causes significant network savings and even sometimes performance boosts.

Windows prerequisites

- The Media Agent OS must be the 64-bit version of Windows 2008 R2, Windows 2012/R2, or Windows 2016.

i **NOTE:** For the accelerator to work properly, the backup traffic must go directly to the QoreStor system. For CommVault, you should install RDCIFS on the media agents.

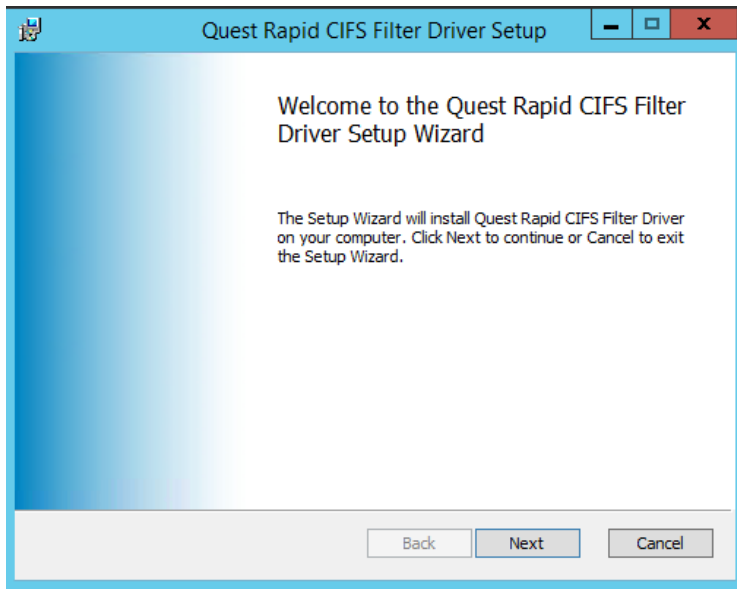
Installing Rapid CIFS on a CommVault Windows media agent

Follow these steps to install Rapid CIFS.

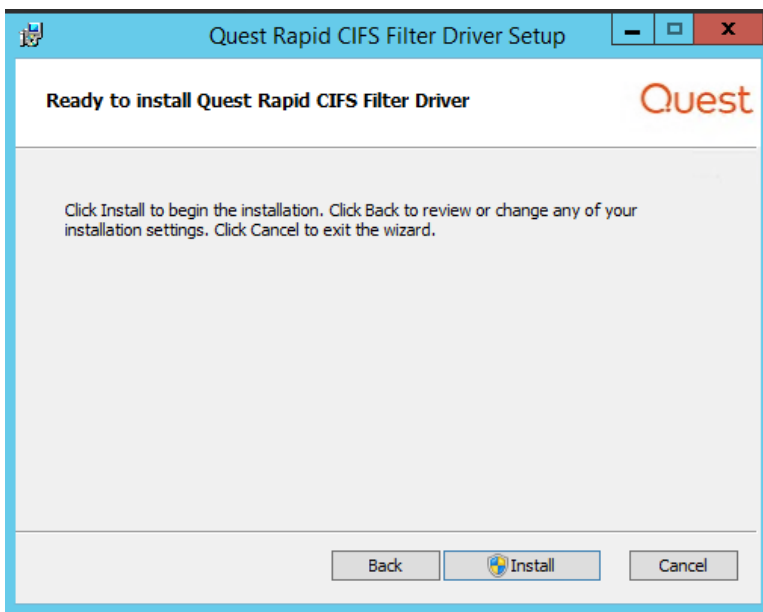
i **NOTE:** Rapid CIFS should only be installed on a CommVault media server.

- 1 Download the MSI to the Server/Proxy by doing the following:
 - a Go to support.quest.com/qorestor/ and select your version.
- 2 On the support page for your product, click Software Downloads.
- 3 For the RDCIFS plugin for your QoreStor version, click the Download icon to download the installer package (.msi file).

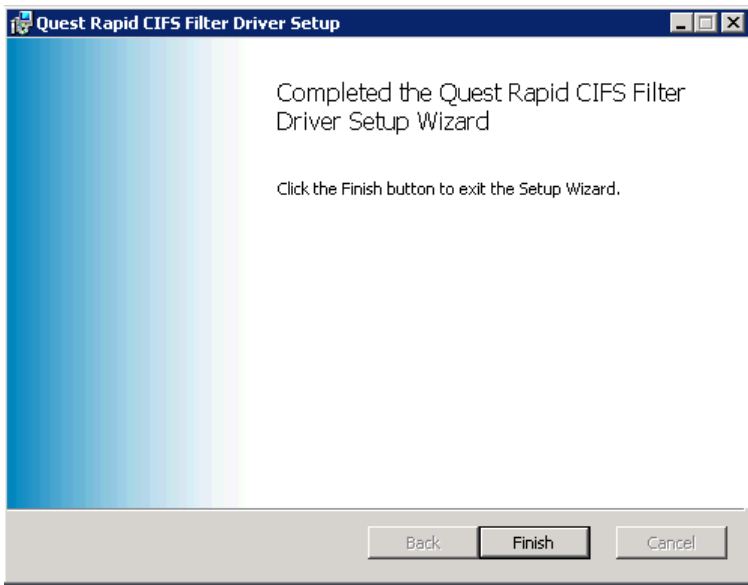
- 4 Run the MSI and follow the instructions in the installation wizard as shown in the screenshots below. Click Next on the first screen.



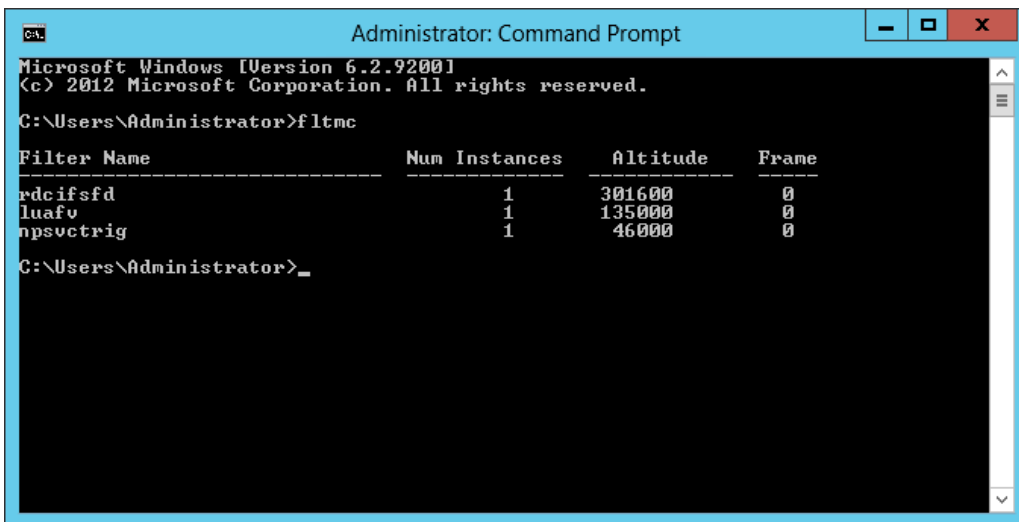
- 5 Click Install.



6 Click Finish.



7 Verify that the "rdcifsfd" driver is loaded automatically; this can be checked by using the command fltmc.



Configuring Rapid NFS with Commvault

Linux prerequisites

- The Media Agent OS must be the 64-bit version of CentOS or SUSE.
- The FUSE module should already be installed, as follows:

On NFS Media Agent, run the command below and verify the command output:

```
# rpm -qa | grep fuse
fuse-2.8.3-4.el6.x86_64
gvfs-fuse-1.4.3-15.el6.x86_64
fuse-libs-2.8.3-4.el6.x86_64
```

- The plug-in must be installed on the designated Linux-based media agent in the following directory, `/usr/opensv/lib/`.

i **NOTE:** For the accelerator to work properly, the backup traffic must go over NFS directly to the QoreStor system and not pass through a media agent. If that is the case, you should install RDNFS on the media agent.

Installing Rapid NFS on a CommVault Linux media agent

Follow these steps to install Rapid NFS.

- 1 Download the installation package to the Media Agent using the following steps:
- 2 Go to support.quest.com/qorestor/ and select your version.
- 3 On the support page for your product, click Software Downloads.
- 4 For the RDNFS plugin for your QoreStor version, click the Download icon to download the installer package (.bin.gz file).
- 5 Use WinSCP or a similar utility to copy the package to the NFS Media Agent. The plug-in must be installed on the NFS Media Agent in the following directory, `/usr/opensv/lib/`.
- 6 On the NFS Media Agent, assuming that the current working directory has the installation package named `QuestRapidNFS-4.0.3036.0-centos5.7-x86_64.bin.gz`, run the following commands in order:


```
gunzip ./ QuestRapidNFS-4.0.3036.0-centos5.7-x86_64.bin.gz
chmod a+x ./QuestRapidNFS-4.0.3036.0-centos5.7-x86_64.bin
```

7 Run the installer:

```
./QuestRapidNFS-4.0.3036.0-centos5.7-x86_64.bin -install
```

```
[root@CVDemoCentOS RapidNFS]# ./QuestRapidNFS-4.0.3036.0-x86_64-RHEL.bin -install
Starting, please wait...
RDNFS file systems are not mounted, proceeding with installation...
2 processors with 4 cores each running at average 2600 MHz ...
Total computing power 20800 MHz ...
Preparing...
QuestRapidNFS
oca-libs
Installation successful!
Log for this operation is /var/log/rdnfs_installer.log
Cleaning up, please wait...
```

8 Create a directory on Media Agent:

```
mkdir /mnt/backup
```

9 Mount the QoreStor NFS container on the Media Agent with the CommVault marker:

```
mount -t rdnfs 4300-26:/containers/backup /mnt/backup -o marker=cv
```

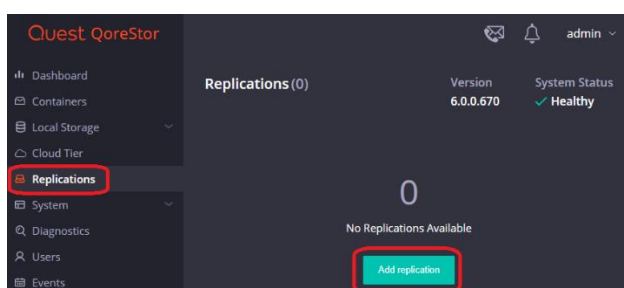
```
[root@CVDemoCentOS RapidNFS]# mount -t rdnfs 4300-26:/containers/backup /mnt/backup -o marker=cv
[root@CVDemoCentOS RapidNFS]# mount |grep backup
4300-26:/containers/backup on /mnt/.backup.2292 type nfs (rw,addr=10.250.235.18)
rdnfs:/mnt/.backup.2292 on /mnt/backup type fuse (rw,nosuid,nodev,allow_other)
```

Setting up QoreStor system replication

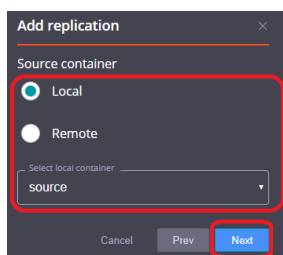
i **NOTE:** For the steps in this procedure, assume QS1 is the replication source QoreStor system, and QS2 is the replication target QoreStor system. 'source' is the replication source container, and 'target' is the replication target container.

Creating a CIFS/NFS replication session

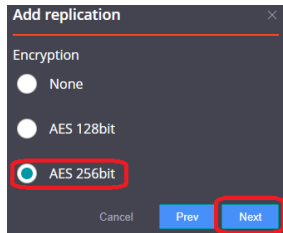
- 1 Create a source container on the source QoreStor system.
- 2 Create a target container on the target QoreStor system.
- 3 On the source QoreStor system, go to the **Replications** Tab. Click the **Add replication** button.



- 4 Select the source Container for Replication and click **Next**.

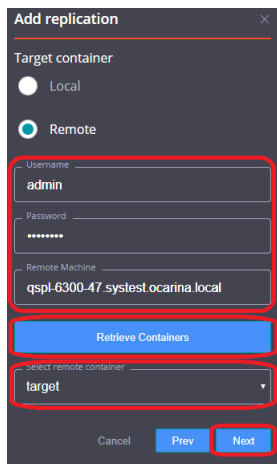


- 5 Select the **Encryption** type for the Source Container and click **Next**.



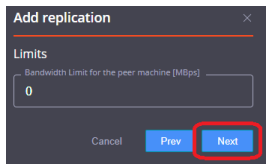
The screenshot shows the 'Add replication' dialog box with the 'Encryption' section. Three radio button options are visible: 'None', 'AES 128bit', and 'AES 256bit'. The 'AES 256bit' option is selected and highlighted with a red circle. Below the options are 'Cancel', 'Prev', and 'Next' buttons. The 'Next' button is highlighted with a red box.

- 6 Enter the target QoreStor systems-related information then click **Retrieve Remote Containers**. Select a target container from the populated list, and click **Next**.



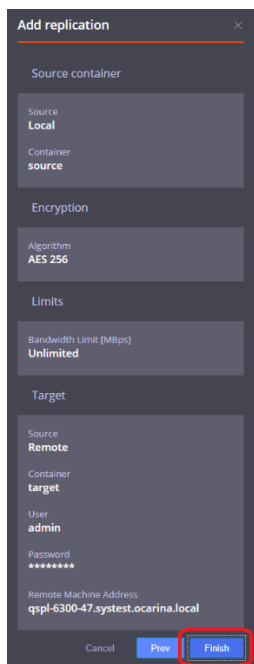
The screenshot shows the 'Add replication' dialog box with the 'Target container' section. Two radio button options are visible: 'Local' and 'Remote'. The 'Remote' option is selected and highlighted with a red circle. Below the options are three text input fields: 'Username' (containing 'admin'), 'Password' (masked with asterisks), and 'Remote Machine' (containing 'qsp1-6300-47.systemt.ocarina.local'). Below these fields is a blue 'Retrieve Containers' button, which is highlighted with a red box. Below the button is a dropdown menu labeled 'select remote container' with 'target' selected. At the bottom are 'Cancel', 'Prev', and 'Next' buttons. The 'Next' button is highlighted with a red box.

- 7 Specify any **Bandwidth Limitations** needed in MBps, and leave 0 for unlimited bandwidth. Click **Next**.



The screenshot shows the 'Add replication' dialog box with the 'Limits' section. A text input field labeled 'Bandwidth Limit for the peer machine [MBps]' contains the value '0'. Below the field are 'Cancel', 'Prev', and 'Next' buttons. The 'Next' button is highlighted with a red box.

- 8 Verify the Summary and click **Finish**.



- 9 Check replication is added successfully and confirm the replication details.

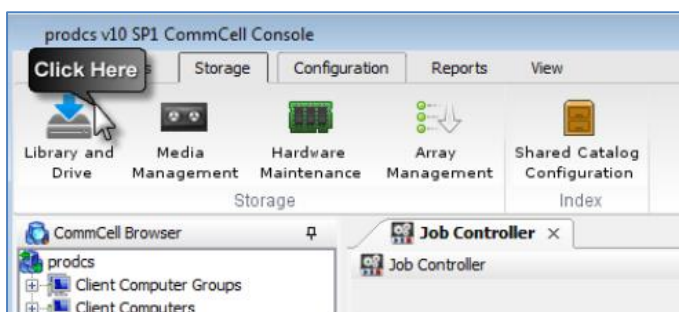
Setting up a CommVault Replica Library

CommVault has a feature called a Replica Library. This feature is useful to prepare CommVault for a Disaster Recovery restore from a QoreStor replication target before the event occurs. With a Replica Library, both the replication source and target containers are added to CommVault. Anything written to the source will be assumed as accessible on the target. Information from CommVault can be found here:

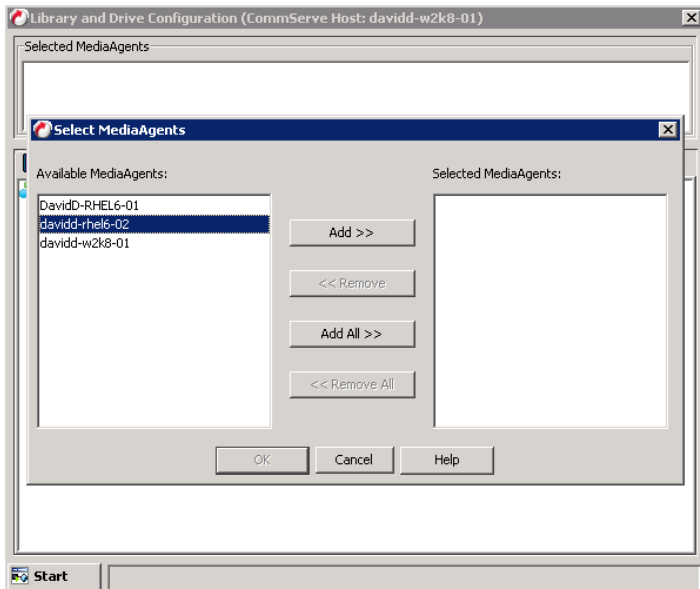
<http://documentation.commvault.com/commvault/v11/article?p=9560.htm>

Follow these steps to set up replication.

- 1 In the CommCell Console, on the Storage tab, click Library and Drive.

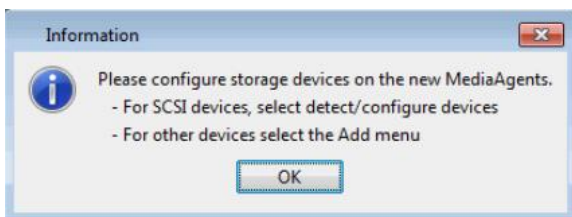


- 2 Select all the Media Agent(s) that will participate in replication, click Add to Selected MediaAgents, and then click OK.

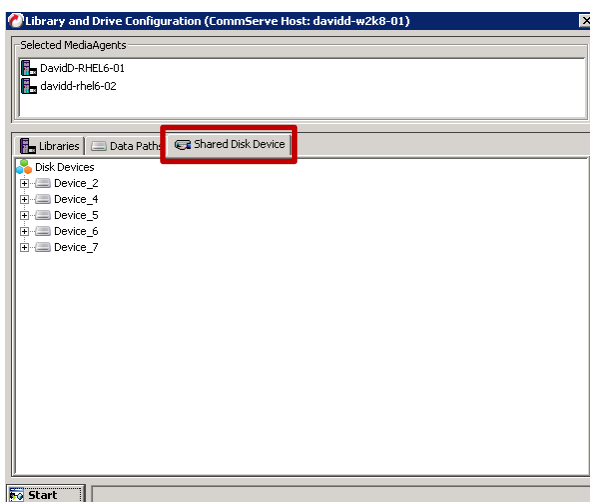


NOTE: To configure a shared library, make sure you select all the MediaAgents that share that library.

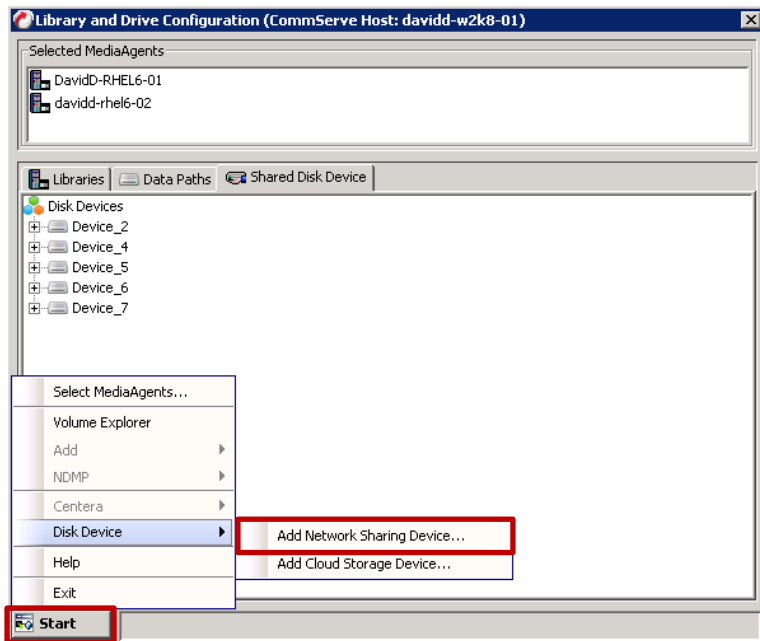
- 3 In the Information dialog box, click OK to continue.



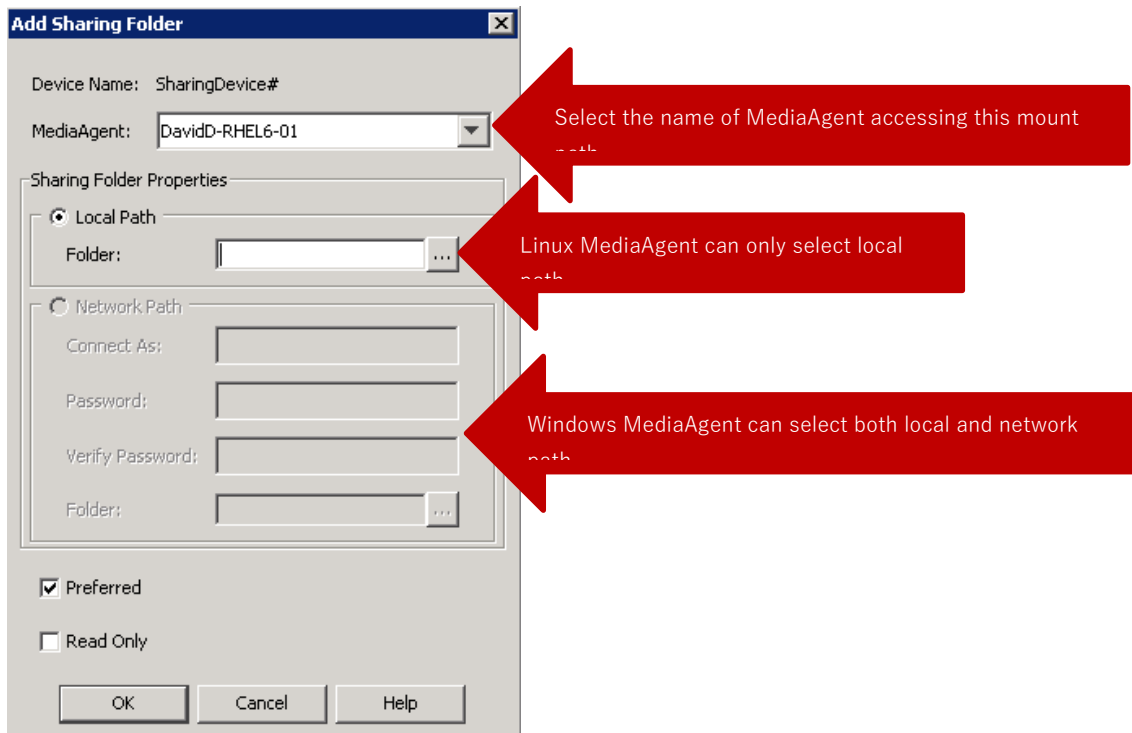
- 4 Click the Shared Disk Device tab.



- 5 Click Start, and select Disk Device > Add Network Sharing Device...

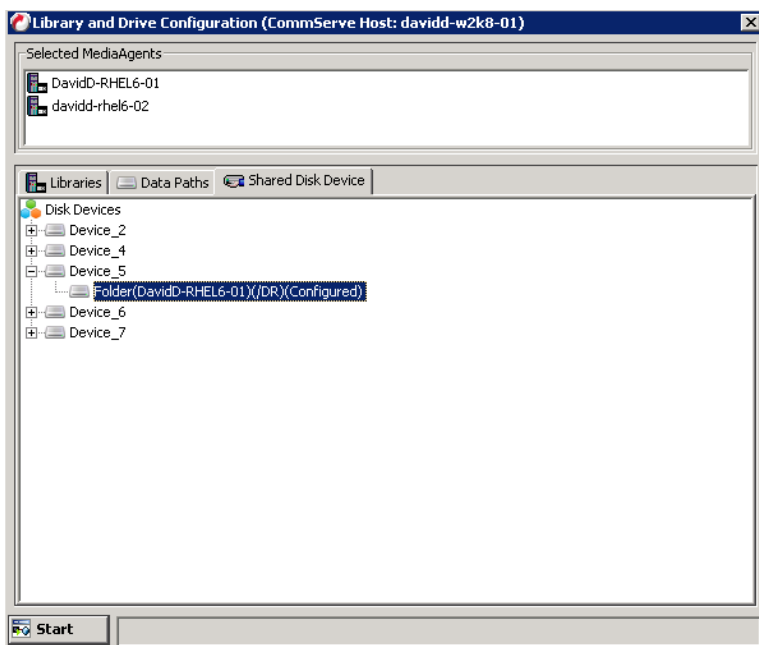


- 6 In the Add Sharing Folder dialog box, enter the source QoreStor container information and then click OK.

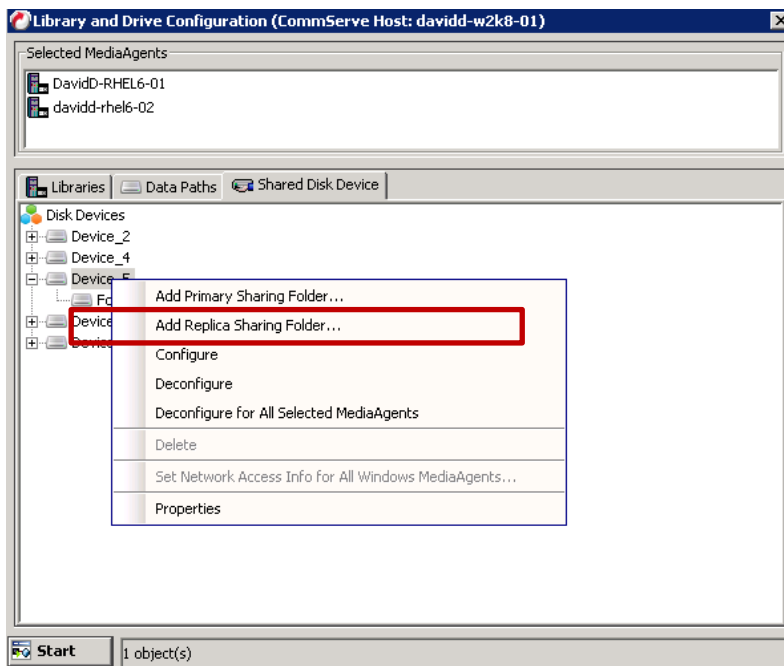


i NOTE: This Device is the replication source. Device information is based on which protocol the container is exposed to the Media Agents.

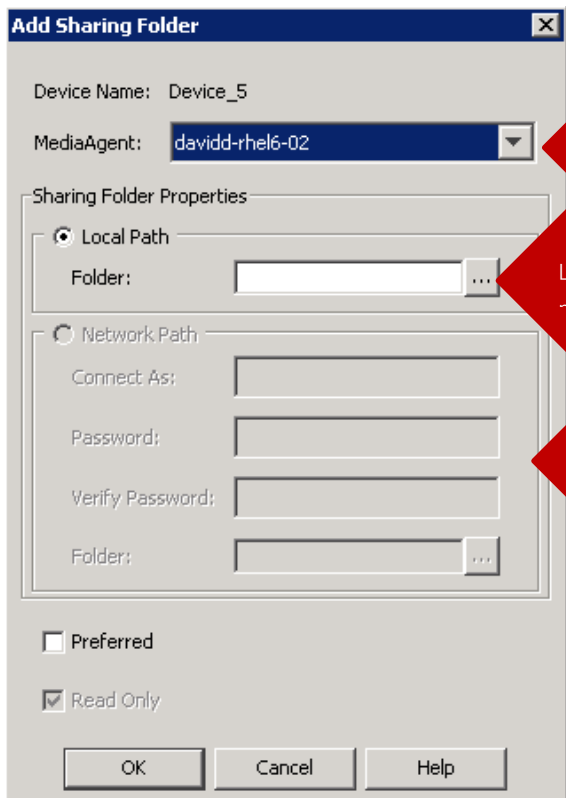
- 7 The system displays the device information with the Media Agent that can access the device in Library and Drive Configuration window.



- 8 Right-click the device and then click Add Replica Sharing Folder.



- 9 In the Add Sharing Folder dialog box, enter the target QoreStor container information and then click OK.



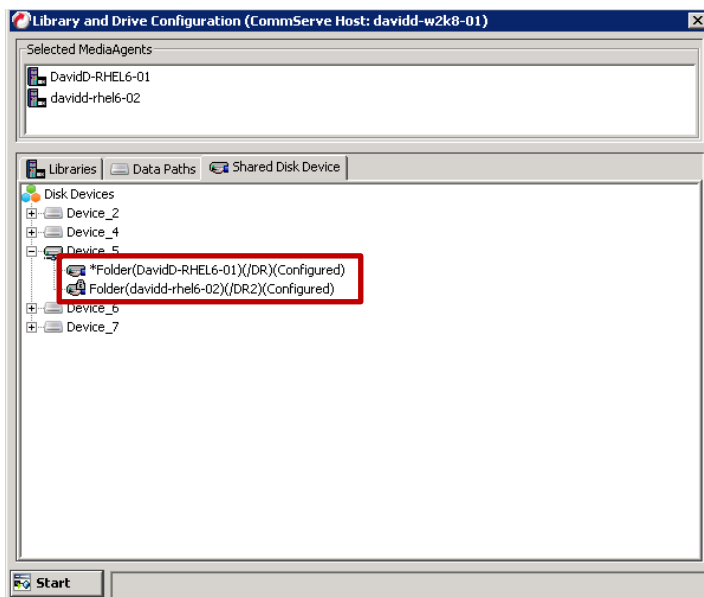
Select the name of MediaAgent accessing this mount path

Linux MediaAgent can only select local path

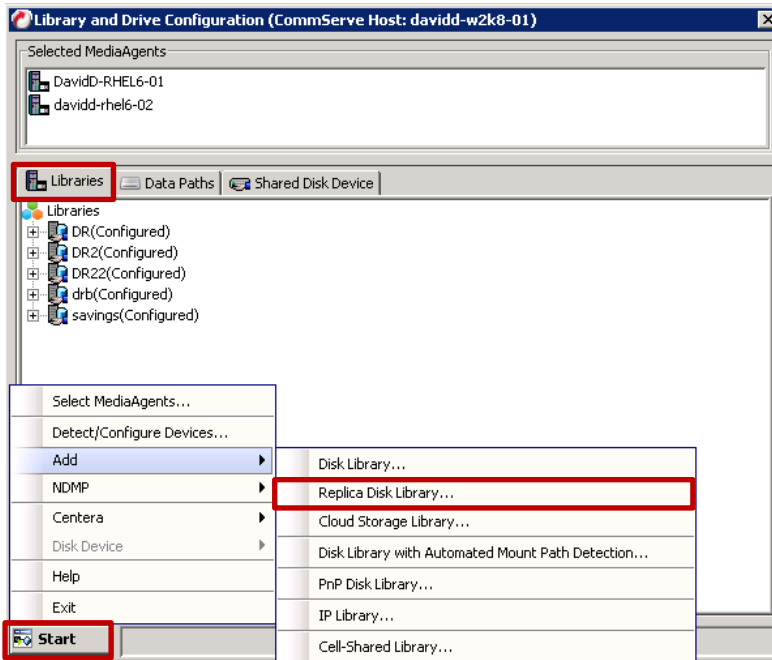
Windows MediaAgent can select both local and network path

i NOTE: This Device is the target destination of the replication. Device information is based on which protocol the container is exposed to the MediaAgents.

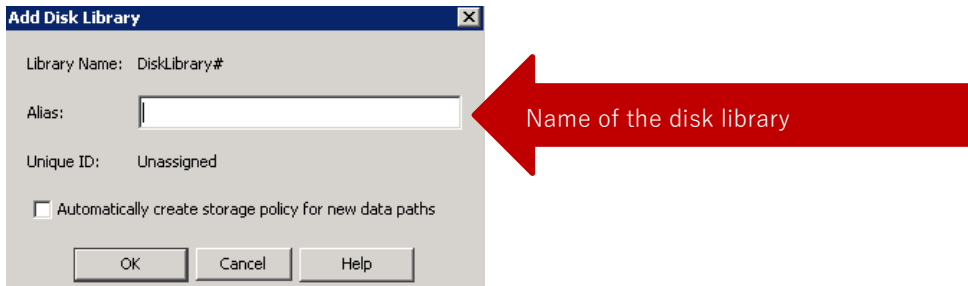
10 The system displays the device information with which the Media Agent can access the device in the Library and Drive Configuration window.



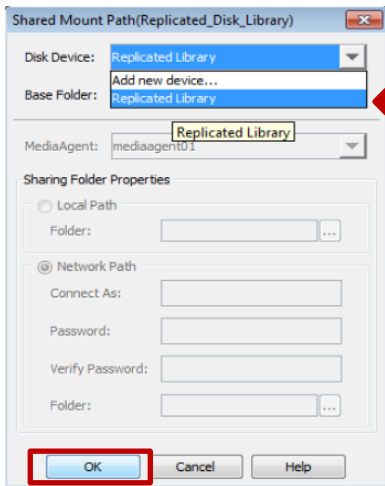
11 On the Libraries tab, click the Start menu, and select Add > Replica Disk Library.



12 In the Add Disk Library dialog box, enter the Alias and clear the Enable replication checkbox.

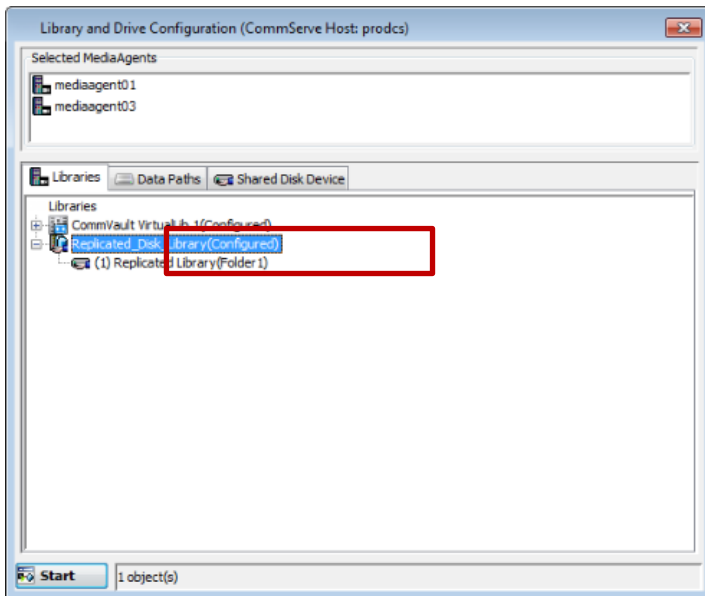


13 In the Share Mount Path dialog box, select the device configured previously, then click OK.



Select the previously configured device

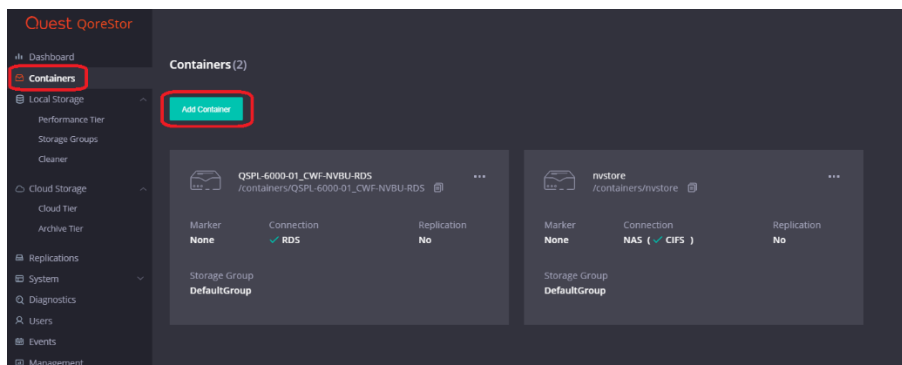
14 Verify the disk library is configured.



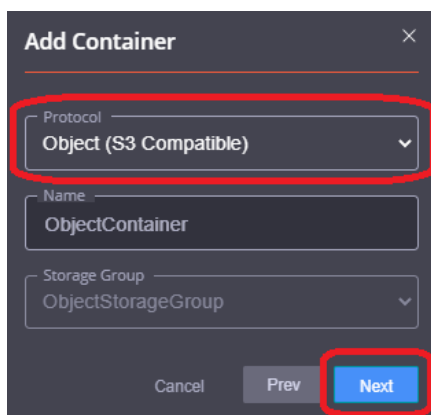
Using QoreStor as a Cloud Storage in CommVault

Creating an Object Container(S3) in QoreStor

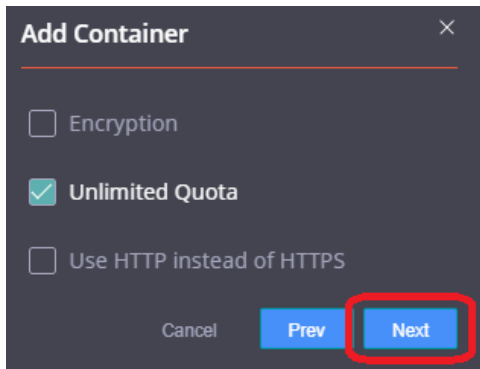
- 1 From the QoreStor UI select **Containers** then click **Add Container**.



- 2 Select the **Protocol** dropdown and set it to **Object (S3 Compatible)**. Click **Next**.



- 3 Click **Next**



Add Container [Close]

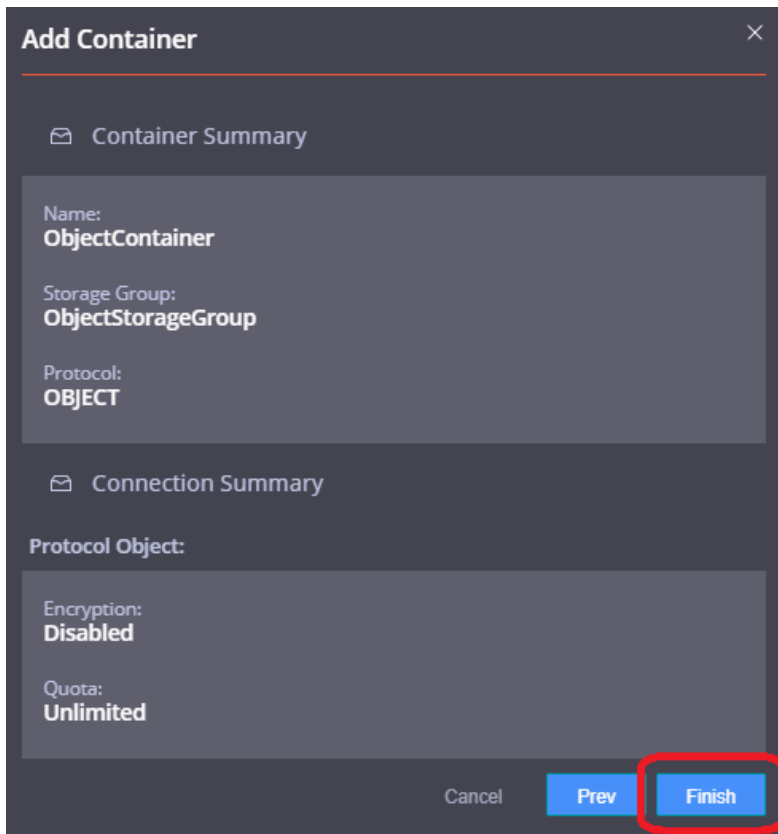
Encryption

Unlimited Quota

Use HTTP instead of HTTPS

Cancel [Prev] **Next**

- 4 Verify the summary is correct and click **Finish**.



Add Container [Close]

Container Summary

Name:
ObjectContainer

Storage Group:
ObjectStorageGroup

Protocol:
OBJECT

Connection Summary

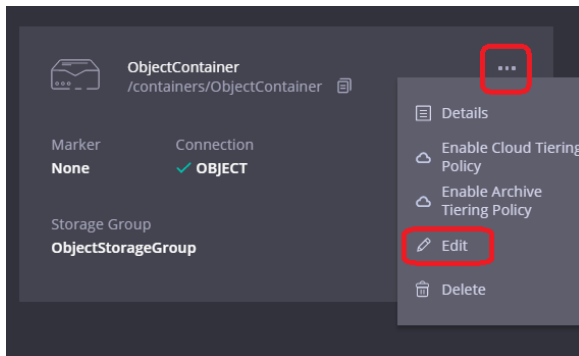
Protocol Object:

Encryption:
Disabled

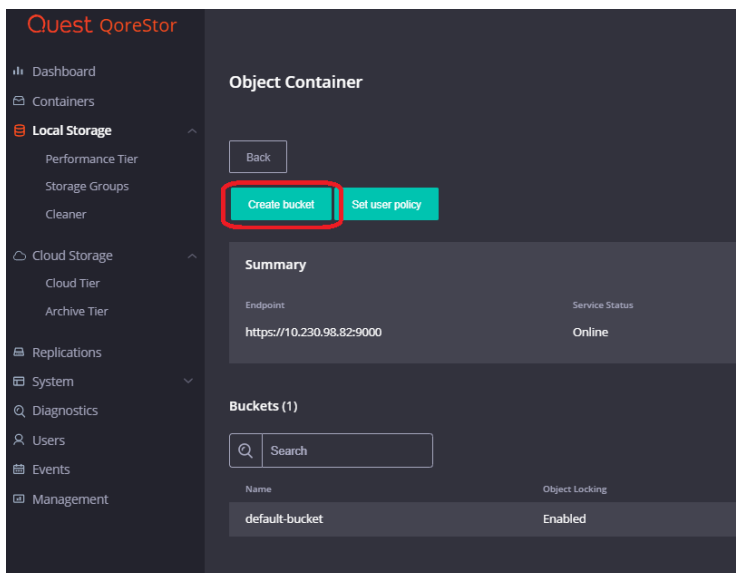
Quota:
Unlimited

Cancel [Prev] **Finish**

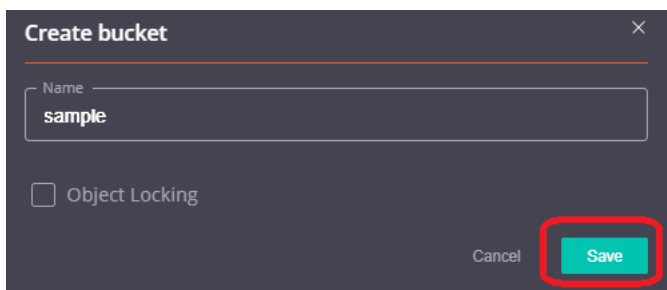
- 5 The Object Container is now created but we need to create a bucket other than the default. Click the **ellipsis** on the container and click **Edit**.



- 6 On the Object Container page click **Create bucket**.

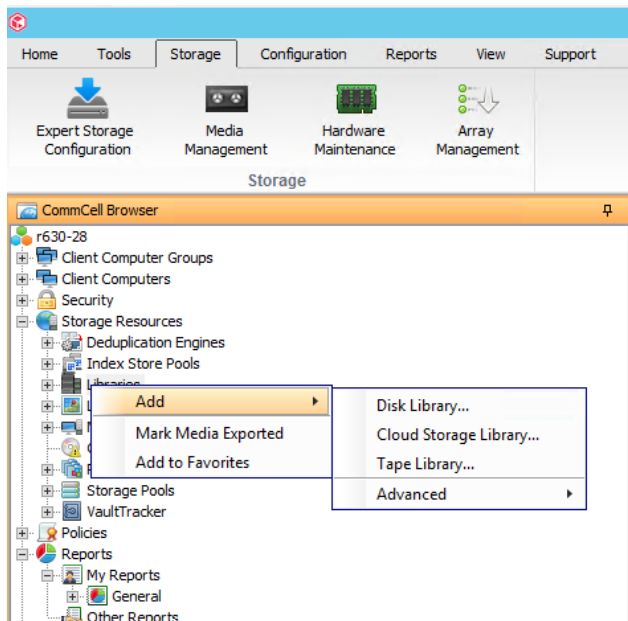


- 7 Name the bucket then click **Save**.

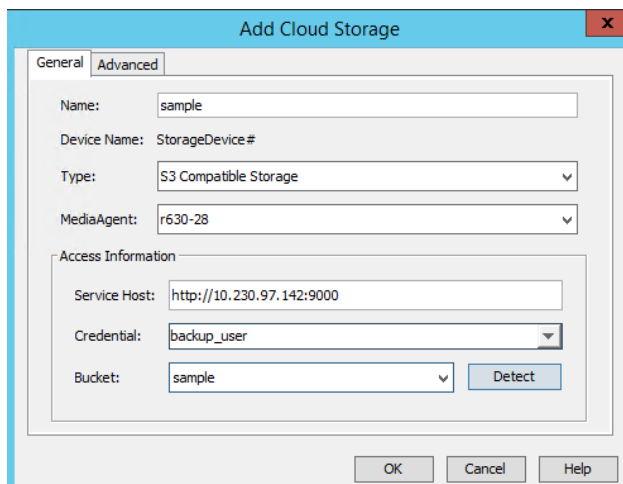


Adding the QoreStor Object Container(S3) to CommVault

- 1) Open the Commcell Console, expand Storage Resources, right-click Libraries, and select Add → Cloud Storage Library...



- 2) In the Name field, enter the user-friendly CommVault library name and select the correct media agent. In the Service host field, you can input the HTTP link to the QoreStor server. With the credentials correctly configured the detect button will automatically find the bucket created in the previous steps. Click OK to add the library.



Performance Tier

A Performance Tier allows you to define a set of faster disks as a Storage Group and created a container within that group. This Performance container will always read/write to these faster disks which will allow operations like restores and standard (non-fast clone) synthetic backups to occur quickly. This tier does not stage data off to the standard disks, this is because a restore of synthetic operation reading from the standard disks would still hamper the operation. All data written to the Performance Tier stays within the performance Tier. Because of this, it is recommended to write only specific jobs, which are required to be highly available and are sized to fit within the performance tier size. Please read the QoreStor User Guide for more details about the Performance Tier.

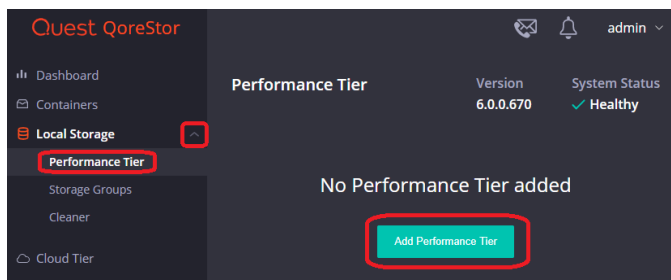


Warning: Please note that once a Performance Tier is added to a system it cannot be easily removed and attempting to do so will most likely result in the destruction of data. Please disable any backup or data copy jobs to the QoreStor system and contact support before attempting removal to find out if this is possible.

Setting up Performance Tier with QoreStor

In this section, we are not going to cover adding a device, creating a partition, creating an XFS filesystem, or defining a mount point in detail. Please reference the QoreStor Installer Guide for this information.

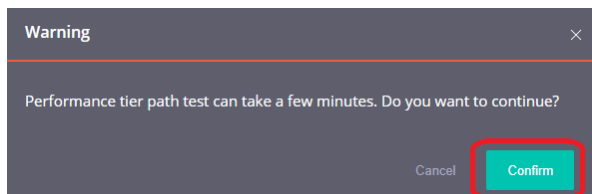
- 1 We first need to cable and add the disks to the OS level. Once seen as a device in the OS an aligned partition will need to be created, an XFS file system created, and a mount point defined in fstab that includes mount option requirements defined in the QoreStor Installer guide.
- 2 Once a file system path to the high-performance storage is added the next step is to add that path as a performance tier in QoreStor. In the QoreStor UI expand **Local Storage** and select the **Performance Tier** tab. Click **Add Performance Tier**.



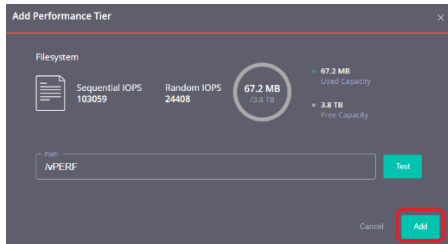
- 3 Enter the performance tier mount path and click the **Test** button.



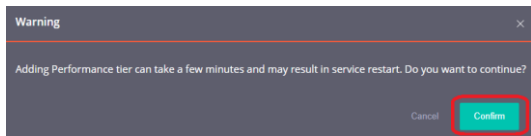
- 4 Click the **Confirm** button



- 5 If the path gets the expected performance click **Add**.

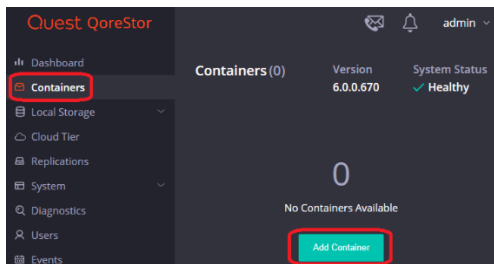


- 6 Click **Confirm** to finish adding the performance Tier, QoreStor services will be restarted

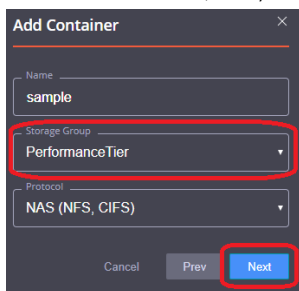


- 7 Once the performance Tier is added you will be logged out. Once logged back in the Performance Tier tab will now list a dashboard for the performance Tier.

- 8 Navigate to the Containers tab and click Add Container



- 9 In the **Storage Group** dropdown, select **Performance Tier**. Input the container **Name** and set the **Protocol** to **NAS (NFS, CIFS)**. Click **Next**.





- 10 Follow the rest of the steps listed in the **Creating a CIFS container for use with CommVault** and **Adding the QoreStor CIFS container as a repository in CommVault** sections of this guild to finish configuring your Performance Tier container.

Cloud/Archive Tier

Cloud Tier

Cloud Tier allows per-container tiering of deduplicated data to low-cost cloud storage. This enables several potential workflows. Namely the ability to keep longer retention while using less physical space on-site or duplicate archival to the cloud. This is done by establishing a Cloud Tier connection and defining per-container policies by which to tier data to the cloud. The policy manager allows for tiering based on time limitations and optionally filtering included and excluded files. It is important to note that individual data blocks will be tiered off not whole backup files. This means if a data block is found frequently over multiple backups it will not necessarily be tiered to the cloud.

 **Warning:** Once a container is configured as Cloud Tier the only way to remove it would be to delete the container or contact Support to fully restore all data blocks from the Cloud. This might involve a read cost from the cloud provider

 **Warning:** It is important to fully consider your CommVault Job configuration and policy configuration when deploying Cloud Tier. Failure to do so could result in unexpected charges from the cloud provider or even failing backup jobs. Please read this section in its entirety as well as check the Cloud Tier section of the QoreStor User Guide.

Important Considerations for Cloud Tier with CommVault

Cloud tiering is achieved by sending deduplicated data blocks to low-cost cloud storage on a cloud provider. These data blocks are identified via a per-container policy manager. The Policy manager options are Idle Time, On-Prem Retention, Include/Exclude Directory paths, and Include/Exclude file types.

- **Idle Time before cloud migration** - Replicates stable data blocks idle for more than the selected number of days/hours to the cloud. After this completes data blocks will be located both On-Premises and on the cloud. All restores will come from the On-Premises data block and not induce any cost. Any attempted modification of files after this idle time will result in access-denied errors. This is why the job type should be considered in CommVault, more on this later in this section.

- **On-Prem Retention Age** - After the selected number of days/hours data blocks that have replicated to the cloud will be removed from On-Premises storage. After this, any data reads, such as restore or synthetic full backups, will be from the Cloud Provider. This can be slower and induce costs from the provider.
- **Folder Paths** - Allows for including or excluding specific paths from cloud tiering replication. Usually, this feature shouldn't be needed with CommVault.
- **File Extensions** - Allows for including or excluding specific file types from cloud tiering replication. Usually, this feature shouldn't be needed with CommVault.

In most cases, with CommVault, Only Idle time and On-Prem Retention need to be considered.

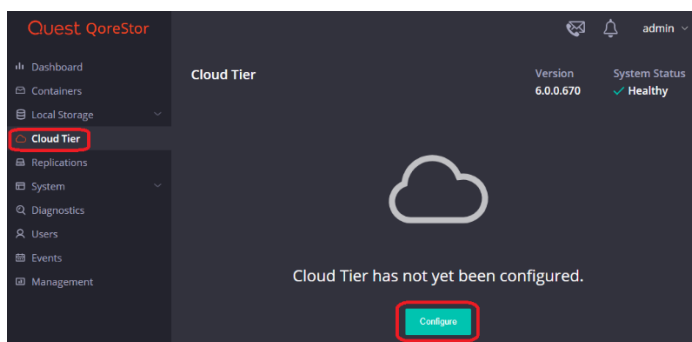


Warning: Idle time is especially important to consider with two workflows. Forever Forward Incremental and forward incremental with Synthetic Full Backups.

Setting up Cloud Tier

Before setting up Cloud Tier it's important to gather some information from your cloud provider. If using Azure, you will need your Connection String, this can be found on your Azure portal under your blob storage account. If using AWS, Wasabi, or an S3 Compatible cloud provider you will need your Access Key, Secret Key, Region, and Endpoint setting (if using a cloud emulator). These can be found on your AWS console or from your cloud provider.

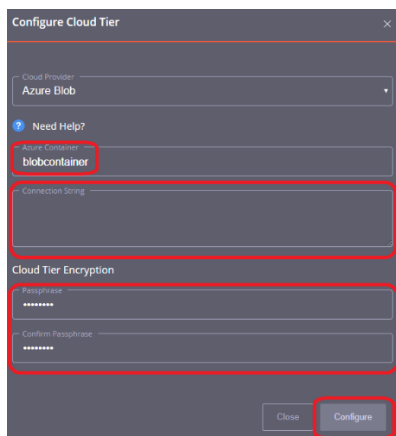
- 1 In the QoreStor UI select the **Cloud Tier** tab then click the **Configure** button.



- 2 For Azure enter your Azure Container name, this will be created automatically in the cloud. Enter your Connection string from the Azure portal and your passphrase. This passphrase is user-defined and used to securely encrypt all files written to the cloud provider. Finally, click Configure.



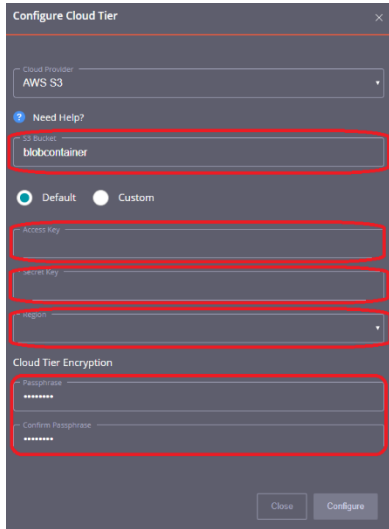
NOTE: Please note the Azure Container name need to be lower case and some symbols are not allowed. This is a limitation of Azure



- 3 For AWS, Wasabi, or S3 compatible enter your S3 bucket name, and this will be created. Enter your Access Key, Secret Key, Region, and passphrase used to encrypt all data written to the cloud provider.



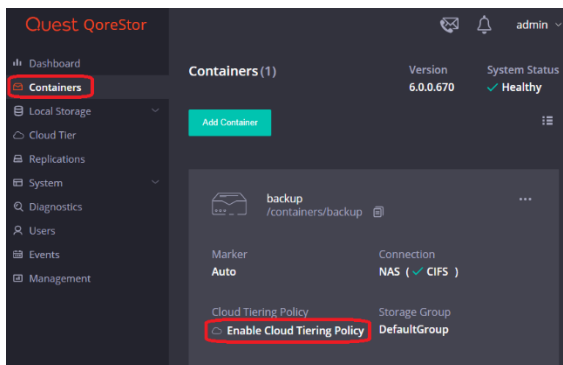
NOTE: Please note the S3 Bucket name need to be lower case and some symbols are not allowed. This is a limitation of S3.



- 4 At this point, Cloud Tier should show as configured and the **Cloud Tier** tab will be populated with statistics. The next step will be to Enable the Cloud Tiering Policy on individual containers.
- 5 Select the **Containers** tab and find or create a container. Click the “Enable Cloud Tiering Policy” hyperlink on this container.



Warning: Once a container is configured as Cloud Tier the only way to remove it would be to delete the container or contact Support to fully restore all data blocks from the Cloud. This might involve a read cost from the cloud provider



- 6 Define the **Idle tie before cloud migration** and **On-Prem Retention Age**, and click **Enable**.



Warning: Please reference the [Important Considerations for Cloud Tier with the CommVault](#) section of this guide before defining idle time and retention age.

Enable Cloud Tiering Policy

Cloud Policy

Idle time before cloud migration format days

On-Prem Retention Age format days

Advanced Options

Cancel **Enable**

- 7 The container will not show as having Cloud Tiering Policy enabled. Idle data will now automatically tier to the cloud provider.

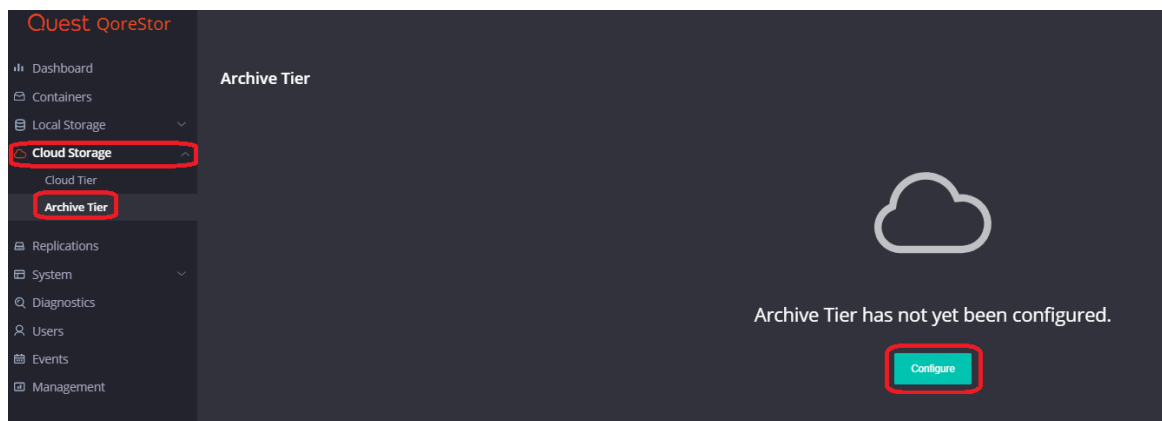
Archive Tier

Important Considerations for Archive Tier with CommVault

Setting Up Archive Tier

Archive Tier is a feature that allows a QoreStor system to tier deduplicated blocks of files to an AWS glacier/deep archive via S3 protocol. Once added one or more containers can be added to a policy. How that policy is configured can determine how long the data is available on-prem in QoreStor, how long it's available both on-prem and in the archive simultaneously, and finally at what point is it only available in the cloud. Archive Tier restores are more difficult, careful consideration should be given to how long the data should be available on-prem before configuring the archive tier.

1. Open the QoreStor UI, expand the **Cloud Storage** section, and select the **Archive Tier** page. Click the **Configure** button.



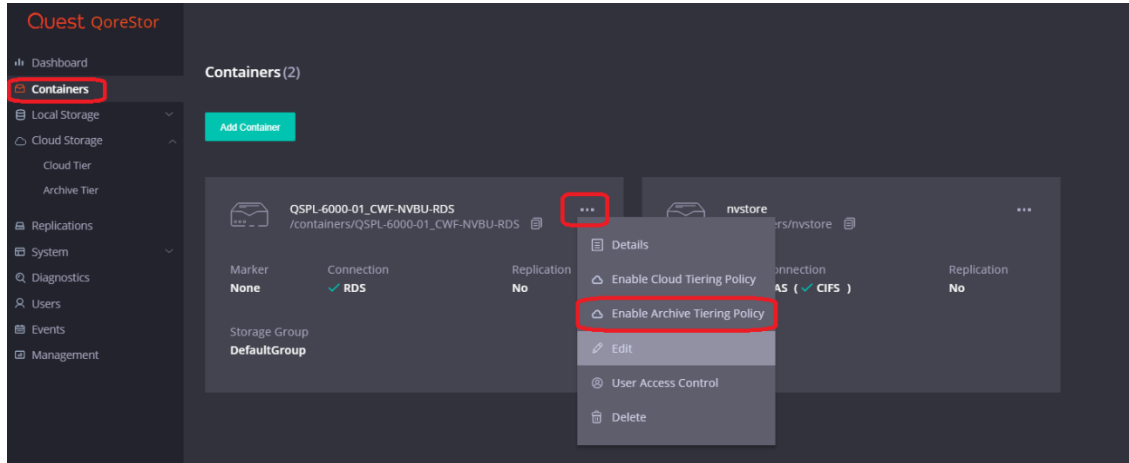
2. You will have to provide several bits of information from your AWS account including the **access key, secret, correct region, ARN role,** and select an **Archive Service Name**. The **S3 bucket name** will be created and is character limited by the provider. Also please make sure to keep your **passphrase**, without this the data is not recoverable in a Disaster Recovery scenario. Finally, click **Configure**.

The screenshot shows a 'Configure Archive Tier' dialog box with the following fields and options:

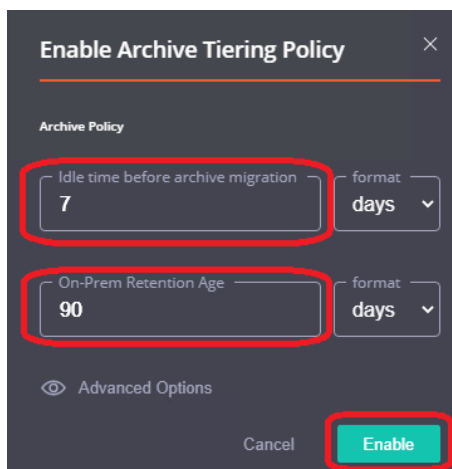
- Archive Provider:** A dropdown menu set to 'AWS S3'.
- Need Help?:** A link with a question mark icon.
- S3 Bucket:** A text input field with a red arrow pointing to it.
- Default/Custom:** Two radio buttons, with 'Default' selected.
- Access Key:** A text input field with a red arrow pointing to it.
- Secret Key:** A text input field with a red arrow pointing to it.
- Region:** A dropdown menu with a red arrow pointing to it.
- Archive Tier Encryption:**
 - Passphrase:** A text input field with a red arrow pointing to it.
 - Confirm Passphrase:** A text input field.
- Archive Tier Options:**
 - Archive Retention in Warm Cloud in days:** A text input field containing '1' with a red arrow pointing to it.
 - Archive Role ARN:** A text input field with a red arrow pointing to it.
 - Archive Service Name:** A dropdown menu with a red arrow pointing to it.

At the bottom right, there are two buttons: 'Close' and 'Configure'. The 'Configure' button is highlighted with a red box.

3. We need to add an Archive tiering policy to a specific container. Do this by navigating to the **Containers** page, selecting the **ellipsis** in the top right corner of the specific container, and clicking **Enabled Cloud Tiering Policy**.



4. In the next window, we need to define the policy. **Idle time before archive migration** specifies the number of hours/days datablocks must be kept idle before being sent to the cloud. The **On-Prem Retention age** specifies the number of hours/days files will be kept locally after they are sent to the archive. Finally, click **Enable**.

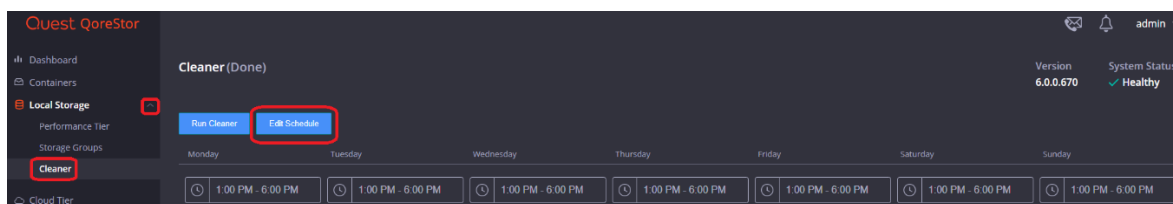


Setting up the QoreStor system cleaner

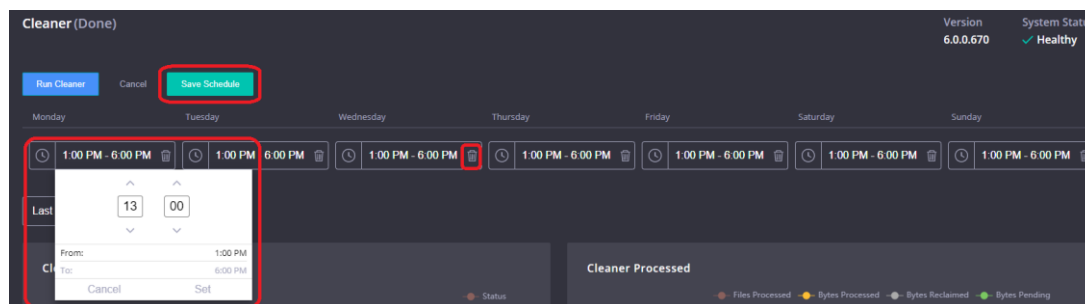
Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from system containers in which files were deleted as a result of deduplication.

The system cleaner runs during idle time. If your workflow does not have a sufficient amount of idle time daily, 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 QoreStor system cleaner can be scheduled. The QoreStor system cleaner should run at least 40 hours per week when backups are not taking place, and generally after a backup job has been completed. Refer to the *QoreStor Series Cleaner Best Practices* white paper for guidance on setting up the cleaner.

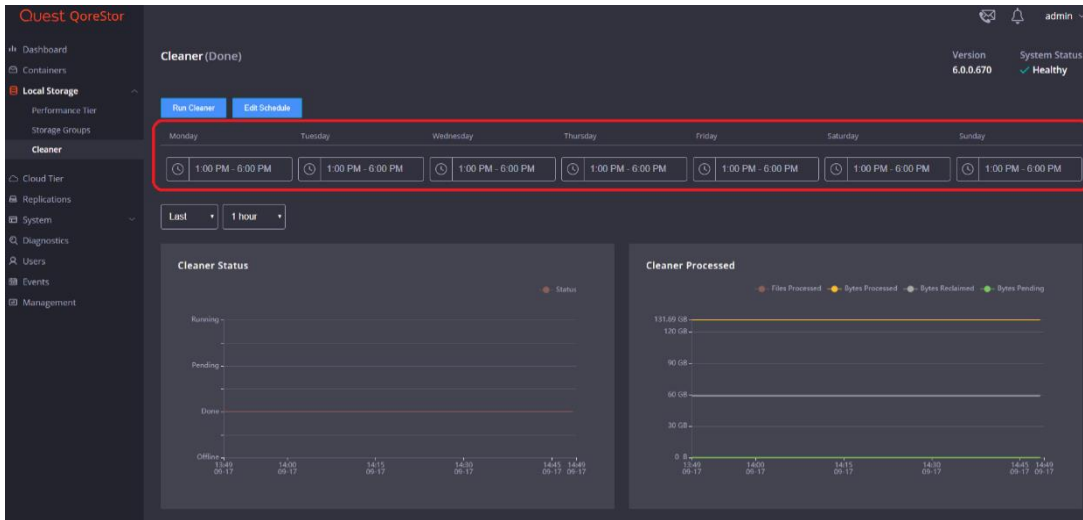
- 1 In the QoreStor system GUI, expand the **Local Storage** tab then click **Cleaner**, and finally **Edit Schedule**.



- 2 Define the schedule and click **Save Schedule**.



3 The new cleaner event is displayed on the **Cleaner** Tab.



Monitoring deduplication, compression, and performance

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

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.

