Setting up Quest® QoreStor™ as an RDA Backup Target for NetVault Backup

Technical White Paper

Quest Engineering

January 2023

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 the 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.**

i **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Setting up Quest® QoreStor™ as an RDA Backup Target for NetVault Backup

Updated – February 21, 2023

Contents

Executive Summary

This white paper provides information about how to set up QoreStor as a backup target for Netvault Backup. This document is a quick reference guide and does not include all QoreStor deployment best practices.

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

http://support.quest.com/qorestor

For more information about NetVault Backup, refer to the NetVault documentation at:

https://support.quest.com/productline/netvault

NOTE: The QoreStor and NetVault Backup screenshots used in this document might vary slightly depending on the QoreStor version and NetVault Backup version you are using.

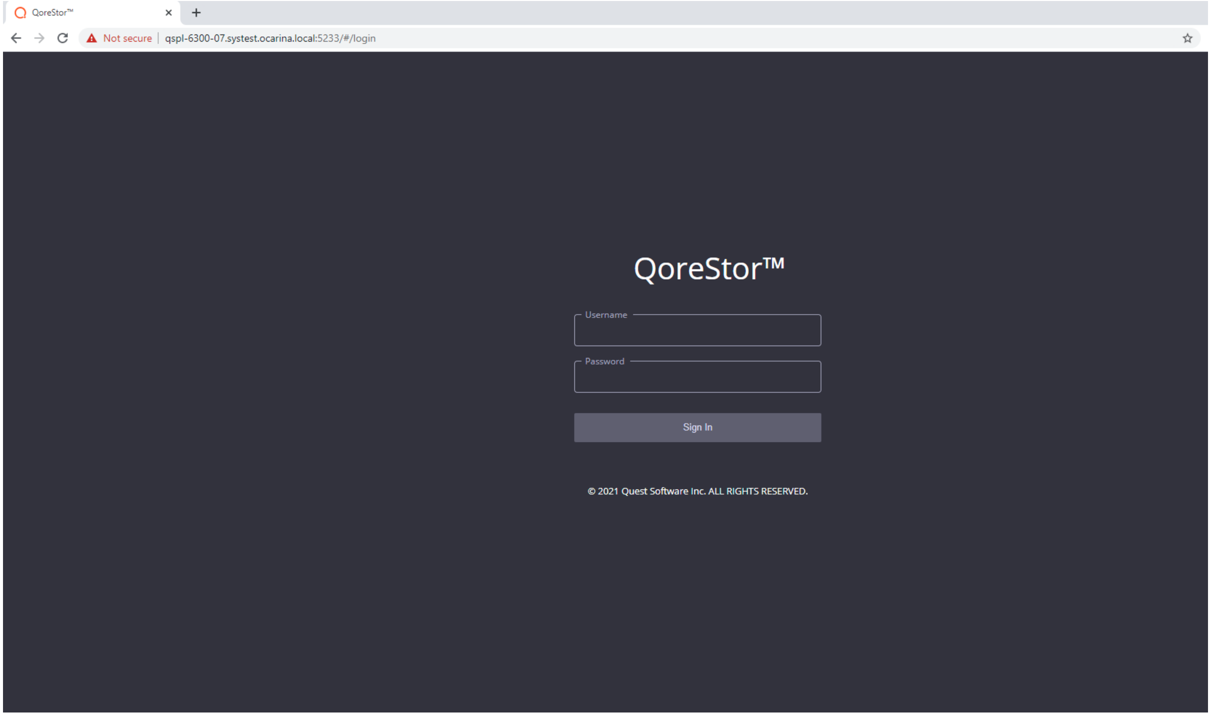
1

Installing and configuring QoreStor

Before installing QoreStor, refer to the *QoreStor Interoperability Guide* to ensure your system(s) meet the installation requirements.

To install QoreStor on your system(s), follow the procedures documented in the *QoreStor Installation Guide*.

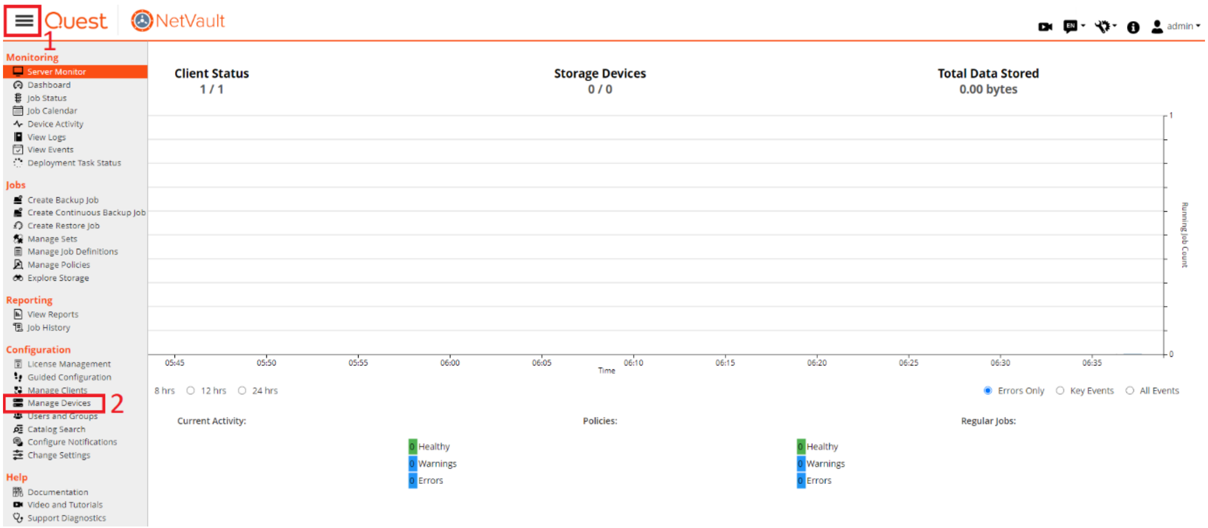
Using a supported web browser (refer to *QoreStor Interoperability Guide* for a list of supported browsers), connect to the QoreStor administrative console via https, using the host IP address/FQDN and port 5233 (https://<hostname:5233>). Log in with the username `admin` and password


QoreStor™
Not secure | qspl-6300-07.systest.ocarina.local:5233/#/login
QoreStor™
Username
Password
Sign In
© 2021 Quest Software Inc. ALL RIGHTS RESERVED.

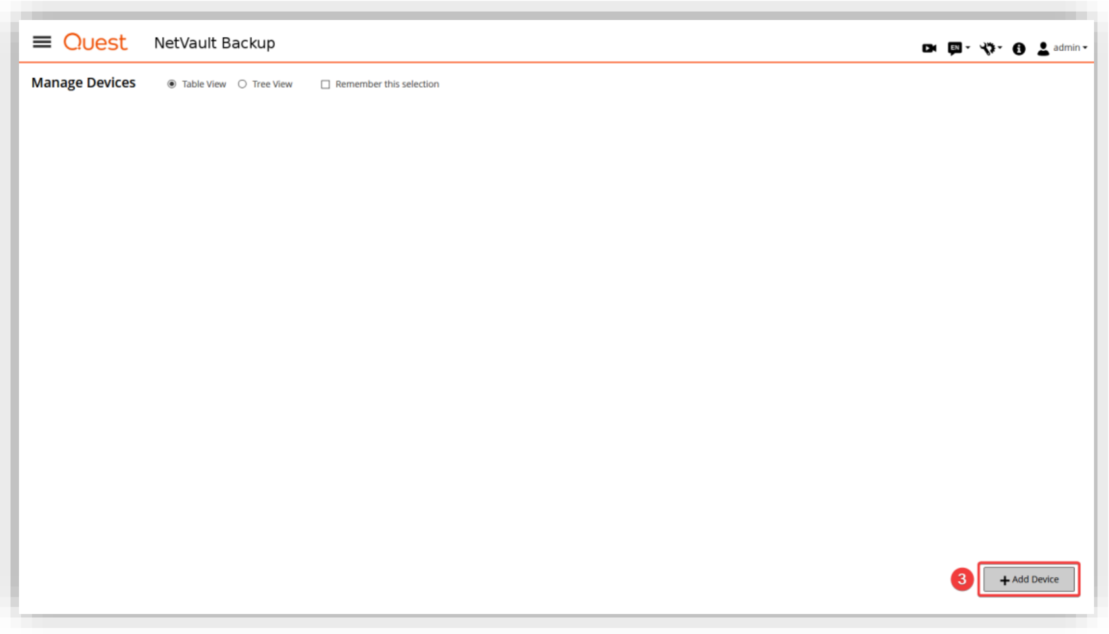
By default, QoreStor has a user with RDA Role named backup_user and password “St0r@ge!”. Refer to the *QoreStor User Guide* for information on changing user accounts.

Adding a QoreStor device to NetVault Backup

1. Open the NetVault Backup UI
2. Open the **menu drawer** ❶, and select **Manage Devices** ❷

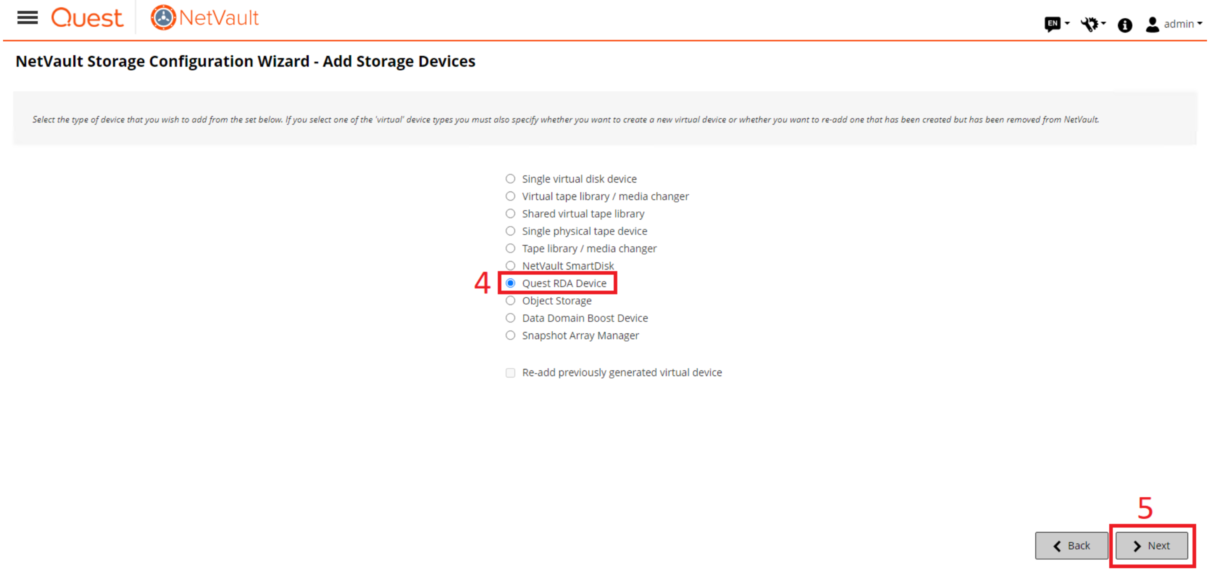


3. Click the **Add Device** button ❸



Manage Devices ● Table View ○ Tree View □ Remember this selection

4. Select **Quest RDA Device** ❹ and click the **Next** button ❺



NetVault Storage Configuration Wizard - Add Storage Devices

Select the type of device that you wish to add from the set below. If you select one of the 'virtual' device types you must also specify whether you want to create a new virtual device or whether you want to re-add one that has been created but has been removed from NetVault.

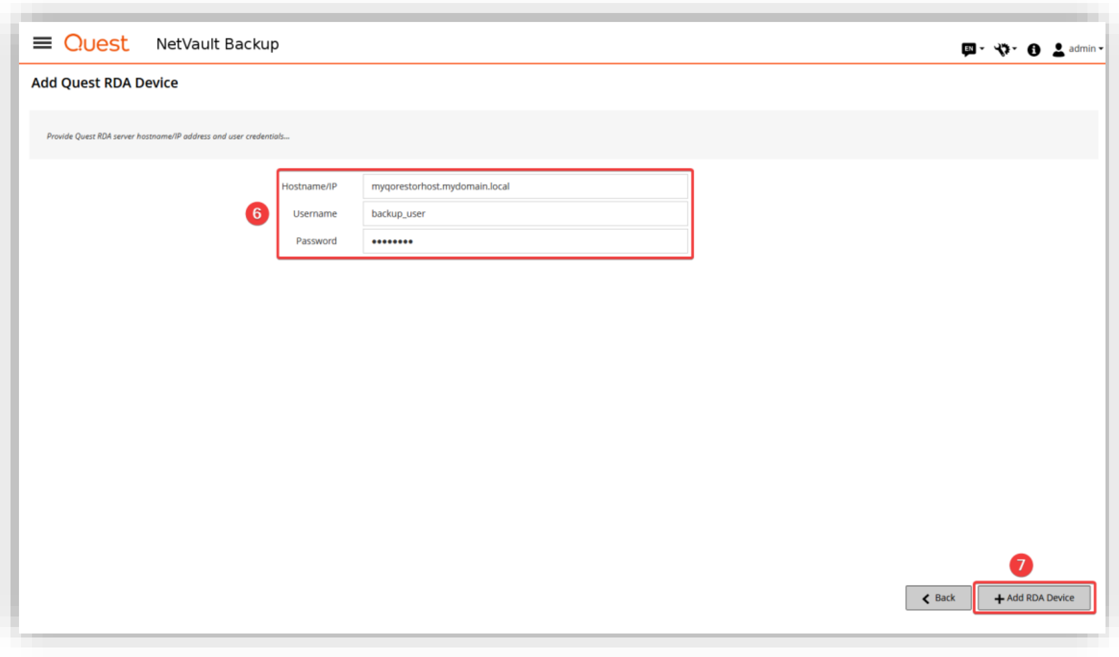
○ Single virtual disk device
○ Virtual tape library / media changer
○ Shared virtual tape library
○ Single physical tape device
○ Tape library / media changer
○ NetVault SmartDisk
● Quest RDA Device
○ Object Storage
○ Data Domain Boost Device
○ Snapshot Array Manager

□ Re-add previously generated virtual device

NOTE: If using NetVault 11.4.5 select **Add Quest DR Device**.

5. Specify the:
   - IP Address or FQDN of the QoreStor host,
   - RDA Username
   - Password ❻

6. Click the **Add RDA Device** button ❼.



Add Quest RDA Device

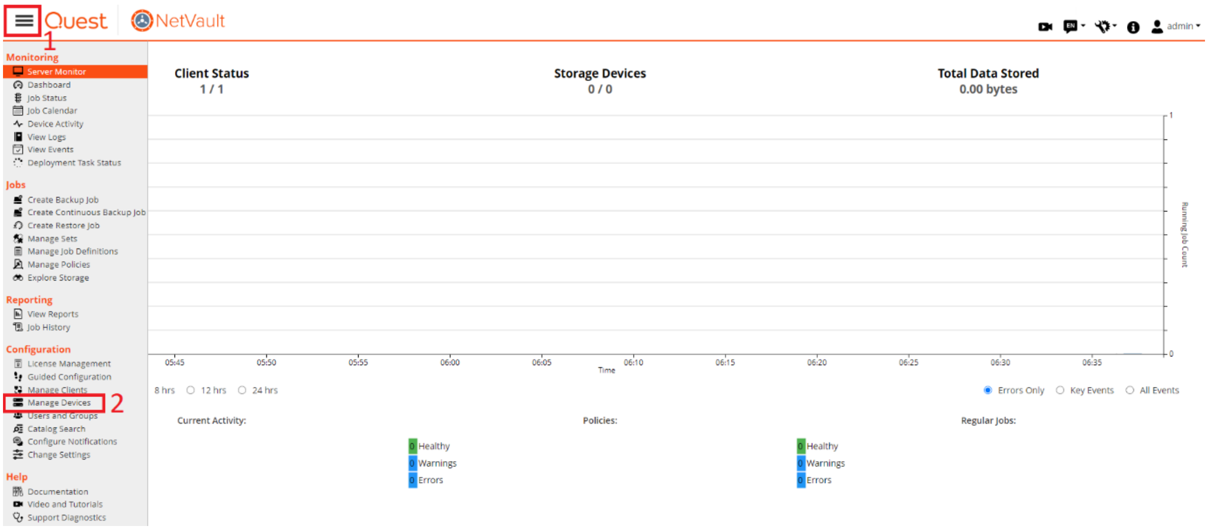
Provide Quest RDA server hostname/IP address and user credentials...

Hostname/IP	myqorestorhost.mydomain.local
Username	backup_user
Password	••••••••

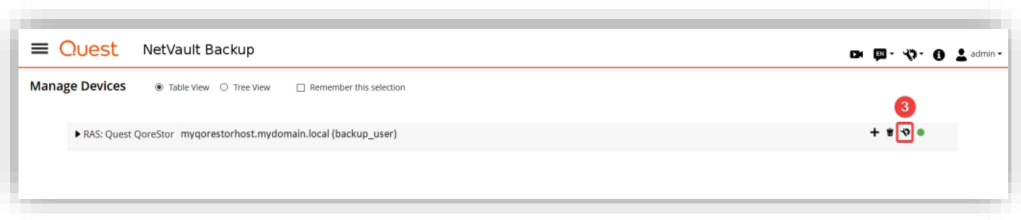
Creating an RDS container for NetVault Backup

This section provides information needed to create an RDS container for NetVault Backup using the NetVault Backup UI. If you wish to use the QoreStor administrative console or CLI, please refer to the *QoreStor User Guide* or the *QoreStor CLI Reference Guide* respectively.

1. Open the NetVault Backup UI
2. Open the **menu drawer** ❶ and select **Manage Devices** ❷

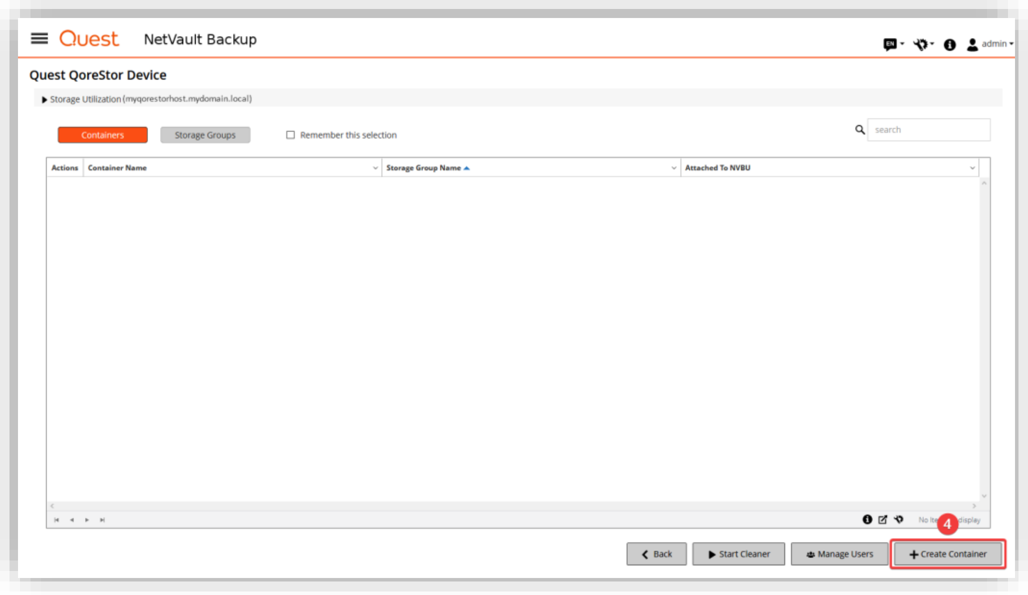


3. Click on the **Manage Device** button ❸



▸ RAS: Quest QoreStor myqorestorhost.mydomain.local (backup_user)

4. Click the **Create Container** button ❹

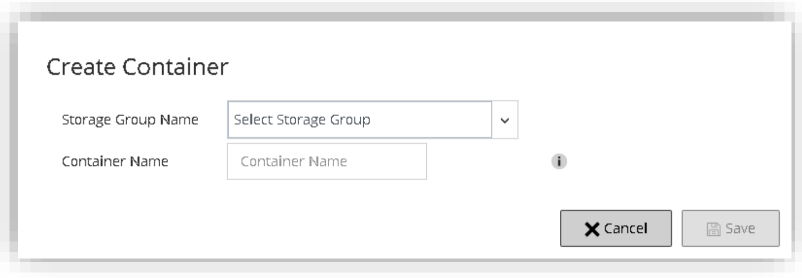


5. On the pop-up dialog:

   a Select the **Storage Group Name*** from the drop-down arrow

   b Enter a Container Name

   c Click the **Save** button.



* By default, the QoreStor host has a storage group created, *DefaultGroup*. If you wish to create a new storage group, please refer to Appendix C in this guide.

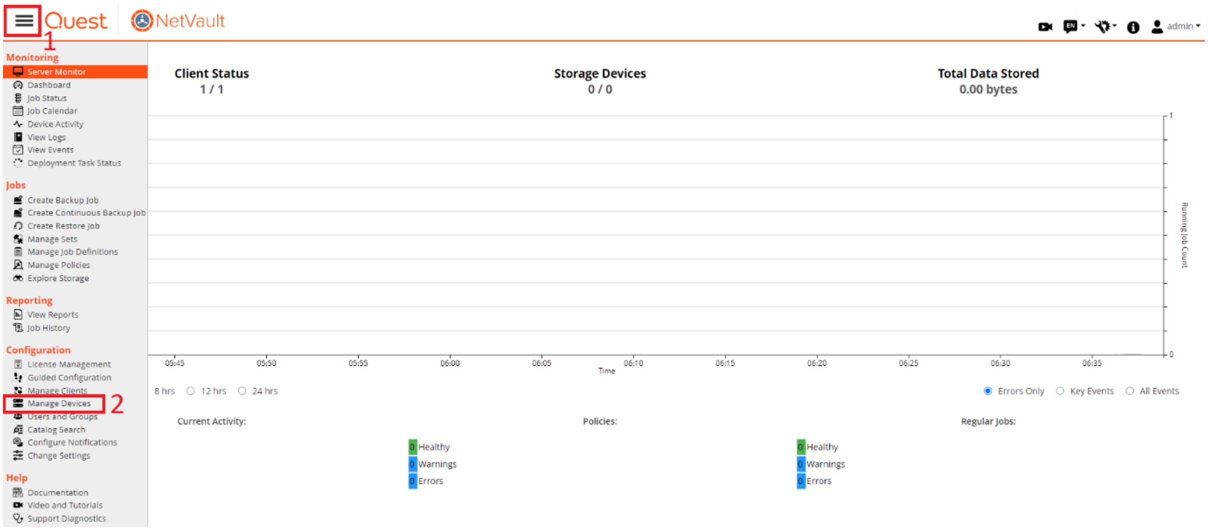
NOTE: If using NetVault 11.4.5, after clicking the **Manage Device** button, open the **menu drawer** under **Actions** and select **Explore** for the chosen Storage Group; then click the **Add LSU** button and enter the name for the Container you wish to create under **Add LSU Name**.

Adding an RDS container to NetVault Backup

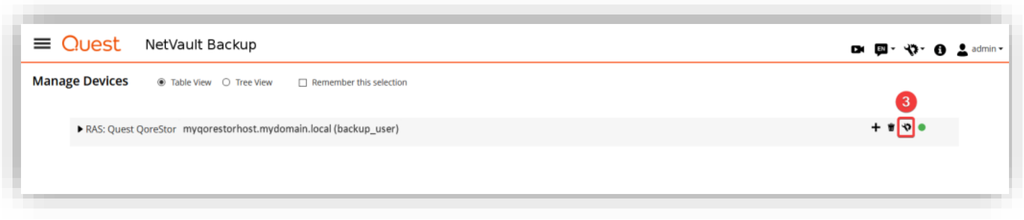
This section provides information needed to add an existing or newly created RDS container to NetVault Backup. The steps below assume that the QoreStor Device has been added to the NetVault Backup configuration. If not, please refer to *Adding a QoreStor Device to NetVault Backup* in this document.

1 Open the NetVault Backup UI

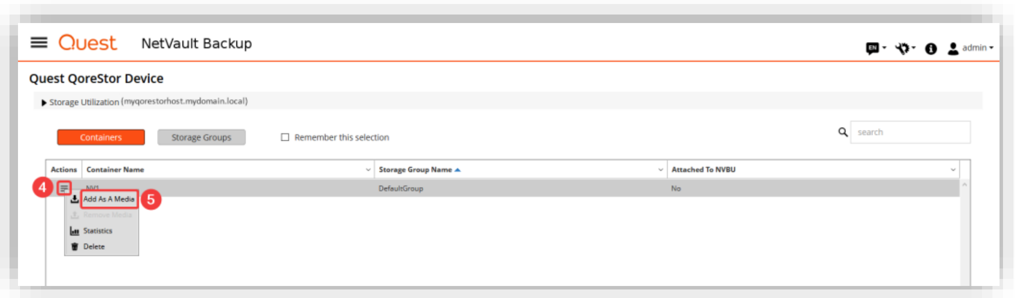
a Open the **menu drawer** ❶ and select **Manage Devices** ❷



b Click on the **Manage Device** button ❸

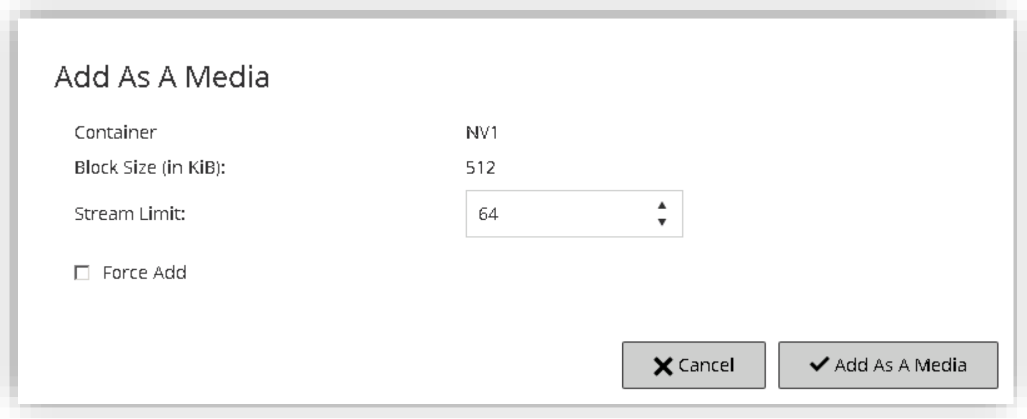

Quest
NetVault Backup
admin
Manage Devices
● Table View ○ Tree View □ Remember this selection
3
▸ RAS: Quest QoreStor myqorestorhost.mydomain.local (backup_user)

c If you wish to add the container, click the **Actions menu drawer** ❹ and select **Add As A Media** ❺



Actions	Container Name	Storage Group Name	Attached To NVBU
	NV1	DefaultGroup	No

d On the pop-up dialog, chose the **Stream Limit** and click on **Add As A Media** button.



Add As A Media

Container NV1

Block Size (in KiB): 512

Stream Limit: 64

☐ Force Add

NOTE: QoreStor supports a maximum of 64 streams per connection with a maximum of 64 connections.

Configuring transport modes for NetVault Backup

There are two transport modes for backing up data over RDA: **Optimized**/**Dedupe** and **Passthrough**. Optimized backup does source-side dedupe on the NVBU clients. The Passthrough mode does target side dedupe on the QoreStor host.

The default mode for each client is decided based on the number of CPU cores in the client machine and whether the architecture is 32-bit or 64-bit. In general, there is no need to change the mode. In the event you want to change the mode, proceed by setting the RDA mode in the QoreStor using the following CLI command:

```
rda --update_client --name <RDA Client Hostname> --mode <auto|passthrough|dedupe>
```

6

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.

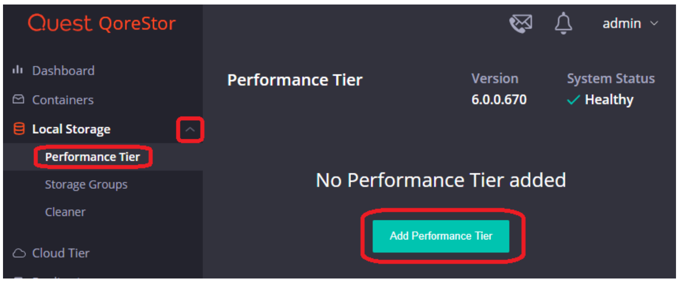
⚠ Warning: **Please note that once a Performance Tier is added to a system it cannot be easily removed and attempting to do so will most likely result in the destruction of data. Please disable any backup or data copy jobs to the QoreStor system and contact support before attempting removal to find out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

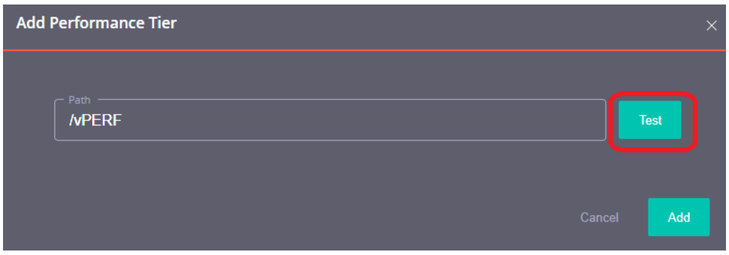
1. We first need to cable and add the disks to the OS level. Once seen as a device in the OS an aligned partition will need to be created, an XFS file system created, and a mount point defined in fstab that includes mount option requirements defined in the QoreStor Installer guide.

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**.



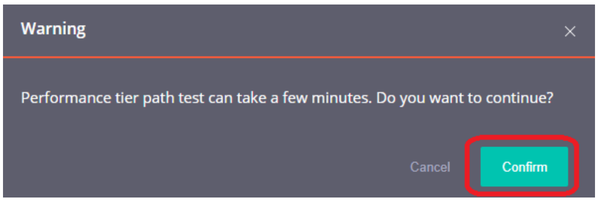
No Performance Tier added

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



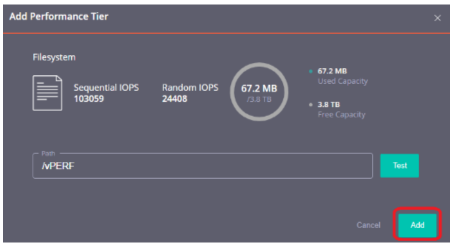
Path: /vPERF

4 Click the **Confirm** button



Performance tier path test can take a few minutes. Do you want to continue?

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



Sequential IOPS 103059

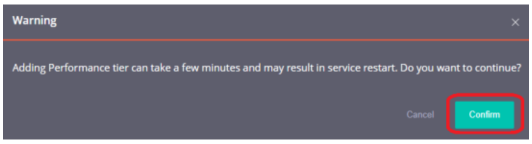
Random IOPS 24408

67.2 MB Used Capacity

3.8 TB Free Capacity

Path: /vPERF

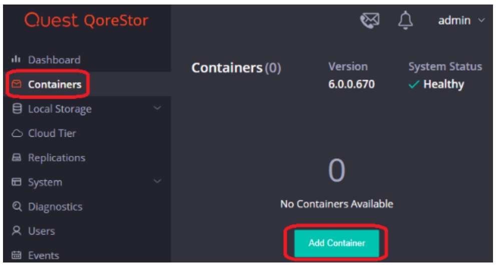
6 Click **Confirm** to finish adding the performance Tier, QoreStor services will be restarted



Adding Performance tier can take a few minutes and may result in service restart. Do you want to continue?

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



Containers (0)

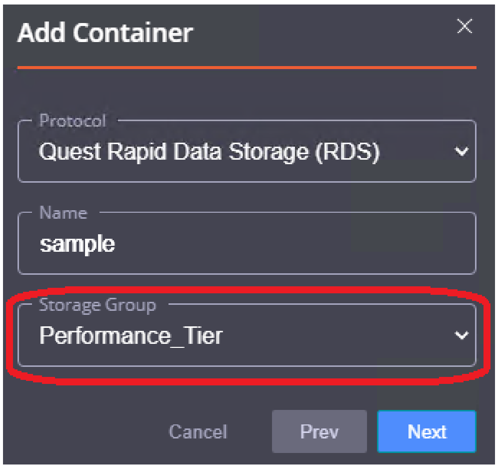
Version 6.0.0.670

System Status ✓ Healthy

0

No Containers Available

9 In the **Storage Group** dropdown, select **PerformanceTier**. Enter the container **Name** and set the **Protocol** to **Quest Rapid Data Storage (RDS)**. Click **Next**.



Add Container

Protocol: Quest Rapid Data Storage (RDS)

Name: sample

Storage Group: Performance_Tier

10 Follow the rest of the steps listed in the **Creating an RDS container for NetVault Backup** and **Adding an RDS container to NetVault Backup** sections of this guild to finish configuring your Performance Tier container.

Cloud/Archive Tier

Cloud Tier

Important Considerations for Cloud Tier with NetVault

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.

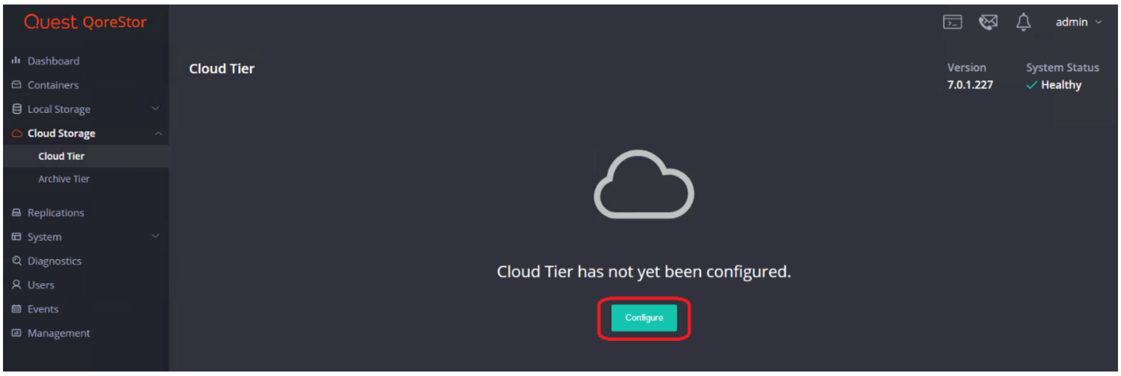
- **Idle Time before cloud migration** - Replicates stable data blocks idle for more than the selected number of days/hours to the cloud. After this completes data blocks with be located both On-Premises and on the cloud. All restores will come from the On-Premises data block and not induce any cost.
- **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. Any attempted modification of files after this retention time will result in access-denied errors.
- **Folder Paths** - Allows for including or excluding specific paths from cloud tiering replication. Usually, this feature shouldn't be needed with NetVault.
- **File Extensions** - Allows for including or excluding specific file types from cloud tiering replication. Usually, this feature shouldn't be needed with NetVault.

⚠ **Warning: Idle time** is especially important to consider with some synthetic or CDP workflows.

Creating a policy-driven Cloud Tier

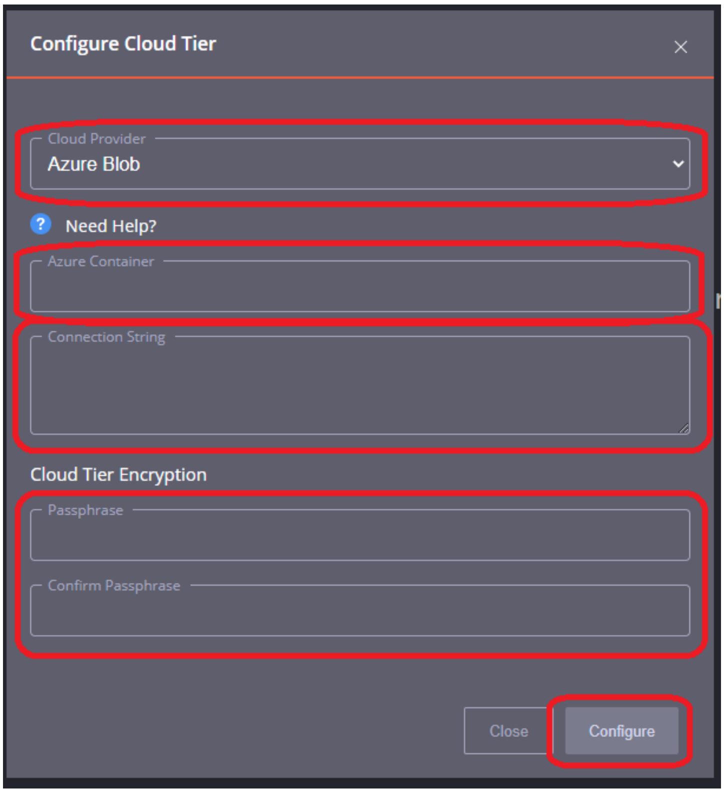
Cloud Tier is a feature that allows a QoreStor system to tier deduplicated blocks of files to a cloud provider via S3 protocol. There are several cloud and on-prem solution providers supported including Azure, AWS, Wasabi, IBM, Google, and many other S3-compatible solutions. Once added one or more containers 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 cloud simultaneously, and finally at what point is it only available in the cloud.

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



Cloud Tier has not yet been configured.

2. Select the **Cloud Provider** dropdown and pick your required provider, depending on the provider the fields below will change. The **Container** field will be a folder/bucket created in the cloud provider, there is no need to create a folder on your own. This folder name is usually limited in accepted characters by the provider. Also please make sure to keep your **passphrase**, without this the data is not recoverable in a Disaster Recovery scenario. Click **Configure**.



Configure Cloud Tier

Cloud Provider: Azure Blob

Azure Container:

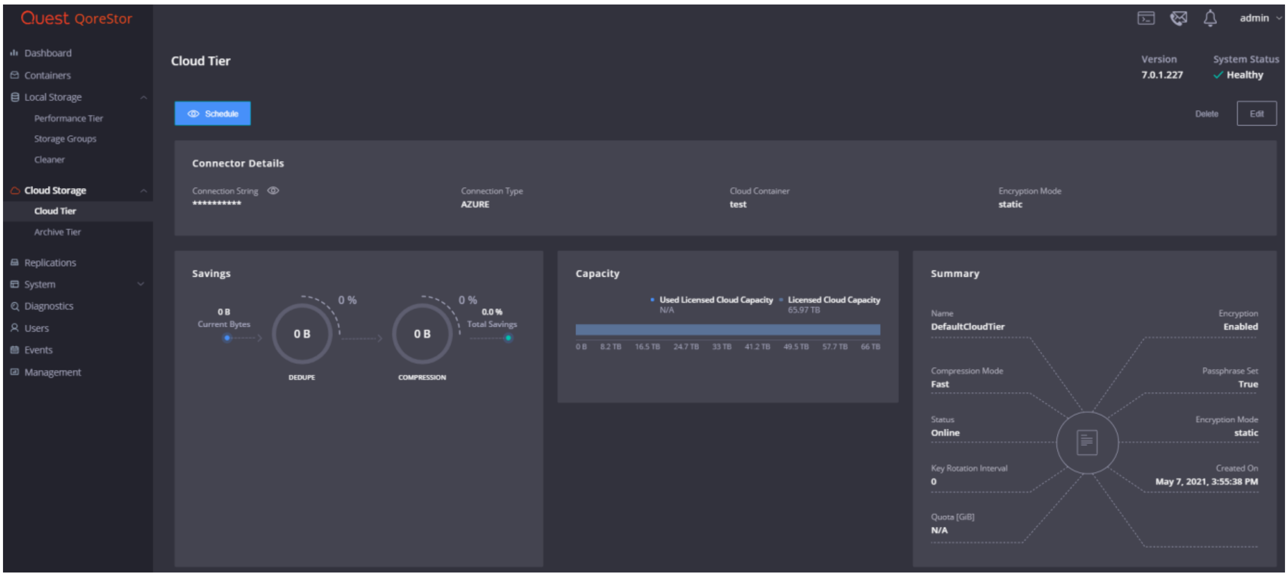
Connection String:

Cloud Tier Encryption

Passphrase:

Confirm Passphrase:

3. Once added, this is how the cloud tier page should appear.



Cloud Tier

Version: 7.0.1.227

System Status: ✓ Healthy

Connector Details

Connection String	Connection Type	Cloud Container	Encryption Mode
**********	AZURE	test	static

Savings

0 B Current Bytes; DEDUPE 0 B, 0 %; COMPRESSION 0 B, 0 %; 0.0 % Total Savings

Capacity

Used Licensed Cloud Capacity: N/A

Licensed Cloud Capacity: 65.97 TB

Summary

Name: DefaultCloudTier

Encryption: Enabled

Compression Mode: Fast

Passphrase Set: True

Status: Online

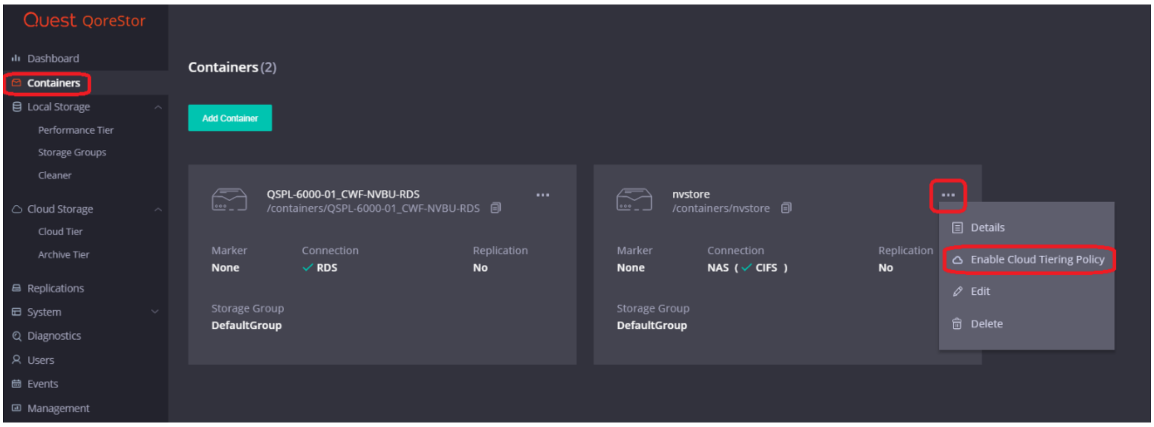
Encryption Mode: static

Key Rotation Interval: 0

Created On: May 7, 2021, 3:55:38 PM

Quota [GiB]: N/A

4. We need to add a cloud 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**.



QSPL-6000-01_CWF-NVBU-RDS
/containers/QSPL-6000-01_CWF-NVBU-RDS

Marker	Connection	Replication
None	✓ RDS	No

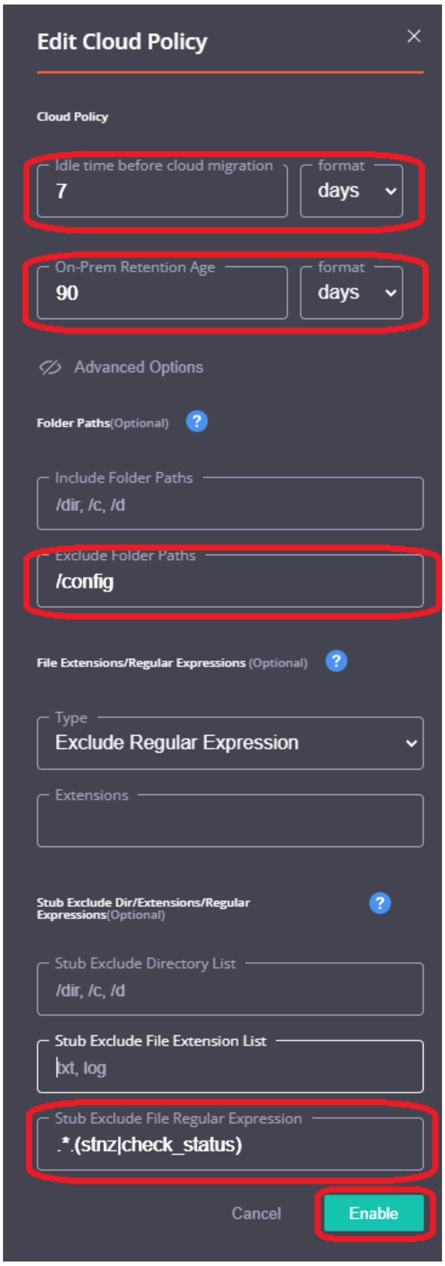
Storage Group
DefaultGroup

nvstore
/containers/nvstore

Marker	Connection	Replication
None	NAS (✓ CIFS)	No

Storage Group
DefaultGroup

5. In the next window, we need to define the policy. **Idle time before cloud migration** specifies the number of hours/days datablocks must be kept idle before being sent to the cloud. **On-Prem Retention age** specifies the number of hours/days files will be kept locally after they are sent to the cloud. We also need to add a few advanced options for NetVault. Click **Advanced Options** and add “/config” into the **Exclude Folder Paths** field as well as ".*.(stnz|check_status)" into the **Stub Exclude File Regular Expression** field. Finally, click **Enable**.



Edit Cloud Policy

Cloud Policy

Idle time before cloud migration: 7
format: days

On-Prem Retention Age: 90
format: days

Advanced Options

Folder Paths(Optional)

Include Folder Paths: /dir, /c, /d

Exclude Folder Paths: /config

File Extensions/Regular Expressions (Optional)

Type: Exclude Regular Expression

Extensions:

Stub Exclude Dir/Extensions/Regular Expressions(Optional)

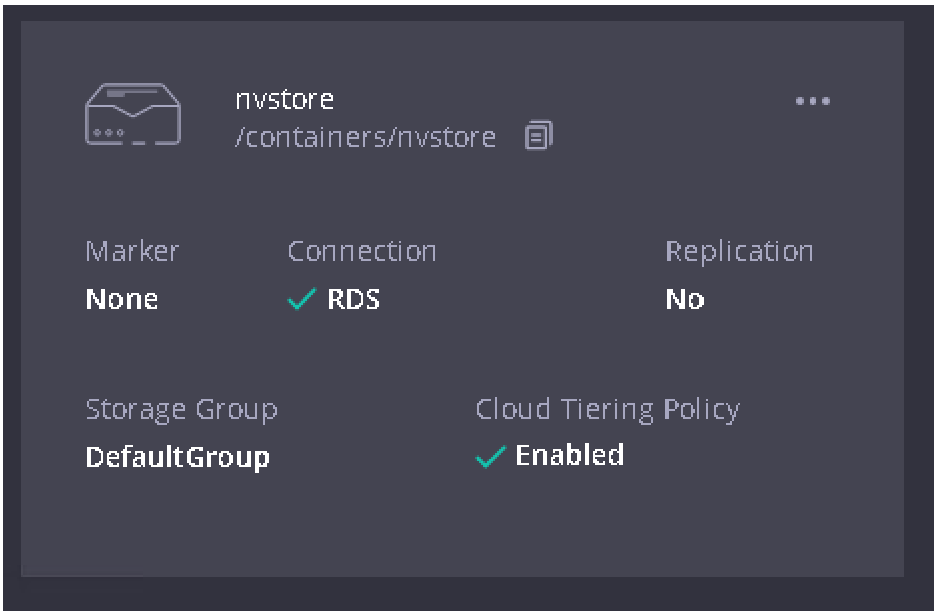
Stub Exclude Directory List: /dir, /c, /d

Stub Exclude File Extension List: txt, log

Stub Exclude File Regular Expression: .*.(stnz|check_status)

CAUTION: Make Please use the Command line command documented in the “Important Considerations” section for Cloud and Archive tier to insure required NetVault files do not get tiered

6. The container should now show with the cloud tiering policy enabled.



nvstore
/containers/nvstore

Marker
None

Connection
✓ RDS

Replication
No

Storage Group
DefaultGroup

Cloud Tiering Policy
✓ Enabled

7

Archive Tier

Important Considerations for Archive Tier with NetVault

QoreStor's archive tier feature enables QoreStor data to be quickly and easily archived to long-term Amazon S3 Glacier or Amazon S3 Glacier Deep Archive storage. Using NetVault and a supported protocol (Object container(S3), files can be written to a QoreStor container and migrated to your archive tier according to easily defined policies. QoreStor provides a policy engine that allows you to set file age and on-premises retention criteria to be used in identifying which files are most suited for replication to the cloud. Policies are defined at the container level and apply to all files within that container. Using the QoreStor Cloud Policy, you can replicate files based on:

- **Idle time** - replicate stable files idle for more than the selected number of hours.
- **File extensions** - replicate files that match or do not match names in a list of extensions.
- **Regular expressions** - include or exclude files based on their match to configured regular expressions.
- **File locations** - replicated files in a list of directories, or all files except those in a list of directories.

Any data that is archived from the QoreStor instance by the archive tier is encrypted with zero knowledge encryption. The encryption keys are solely owned by you. If the encryption keys are placed in the archive tier, a passphrase is used to encrypt those keys and that passphrase is only known to you. For added security, QoreStor obfuscates metadata names such as blockmap and data store objects that are stored in the archive tier.

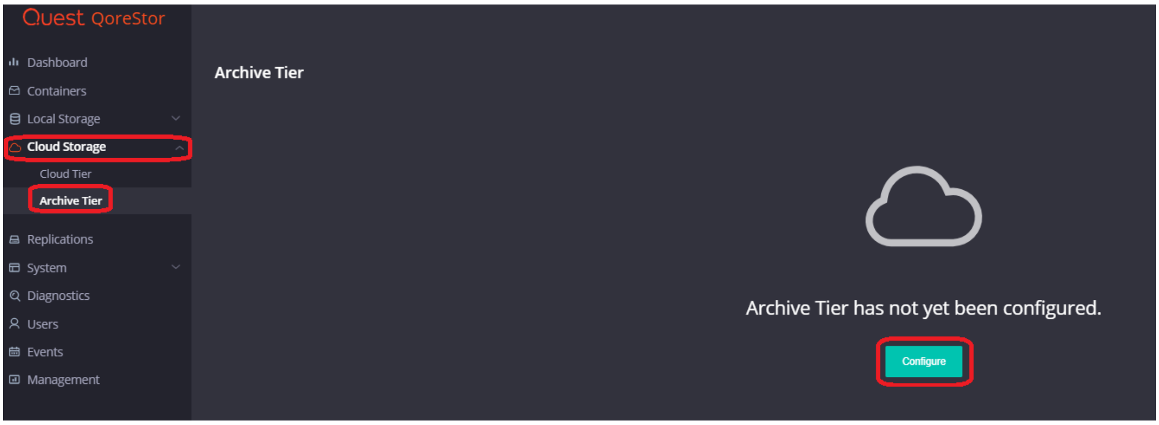
Data stored in the archive tier is not available for immediate recovery. When recovery is initiated, the data stays in the archive tier while a copy is made in S3 standard storage and kept for an amount of time specified by the **archive_retention_in_warm** parameter. Although recovery times may vary, the general expectations for recovery times are:

- Amazon S3 Glacier storage: 3-5 hours
- Amazon S3 Glacier Deep Archive: within 12 hours

Creating a policy-driven Archive Tier

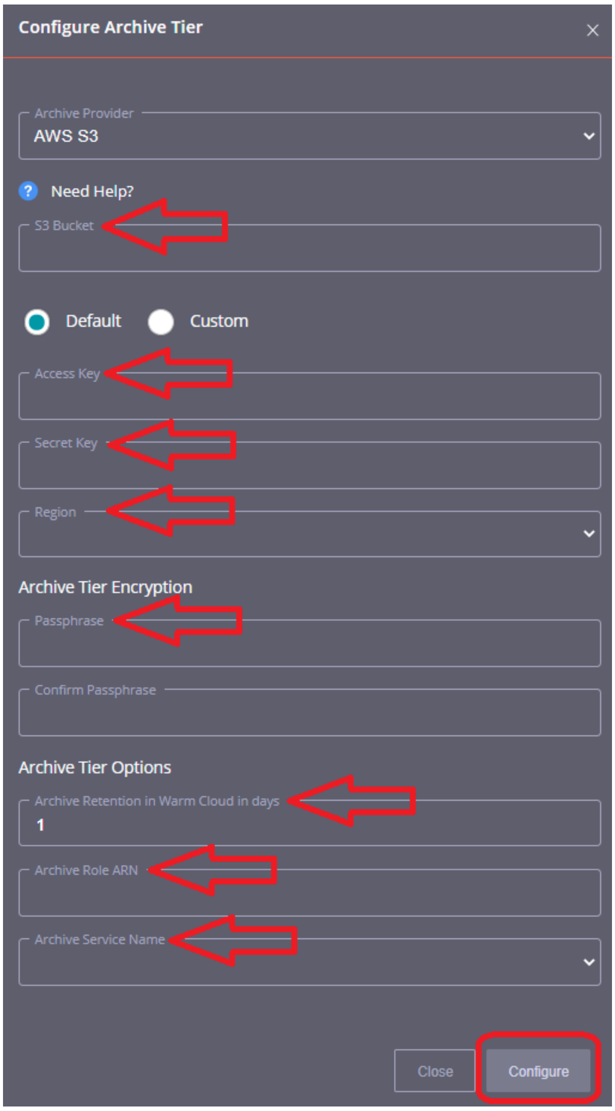
Archive Tier is a feature that allows a QoreStor system to tier deduplicated blocks of files to an AWS glacier/deep archive via S3 protocol. Once added one or more containers can be added to a policy. How that policy is configured can determine how long the data is available on-prem in QoreStor, how 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.



Archive Tier has not yet been configured.

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**.



Configure Archive Tier

Archive Provider: AWS S3

Need Help?

S3 Bucket:

● Default ○ Custom

Access Key:

Secret Key:

Region:

Archive Tier Encryption

Passphrase:

Confirm Passphrase:

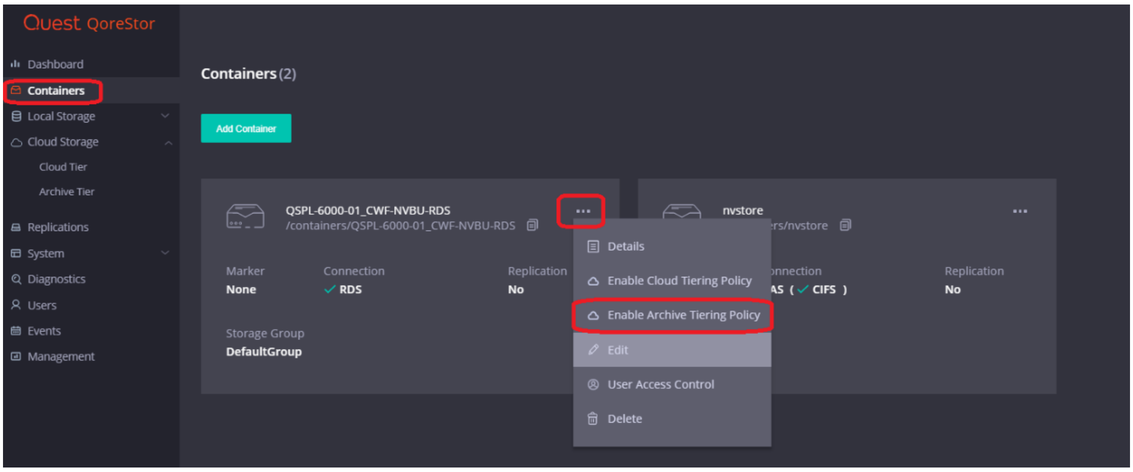
Archive Tier Options

Archive Retention in Warm Cloud in days: 1

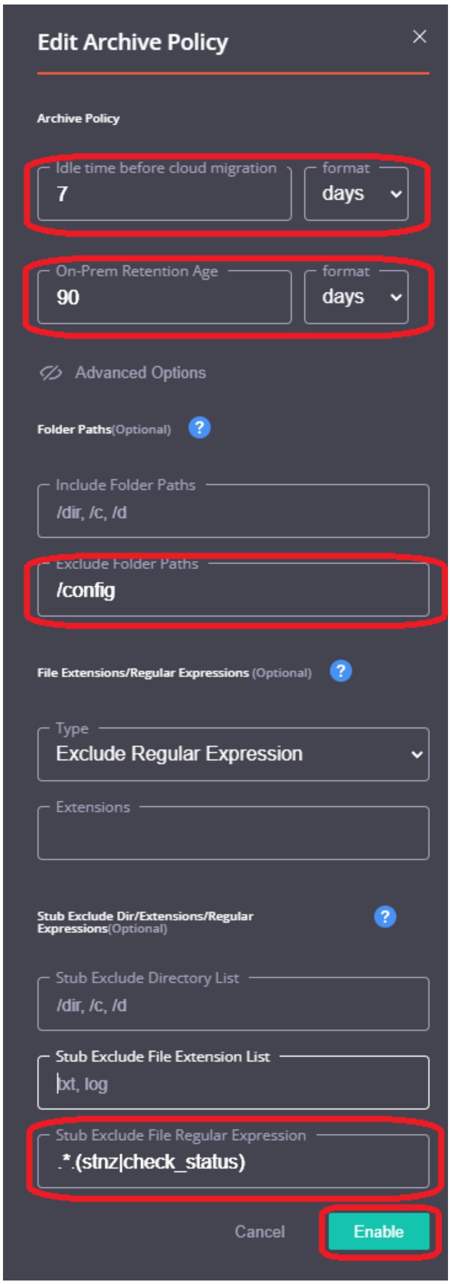
Archive Role ARN:

Archive Service Name:

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 cloud migration** specifies the number of hours/days datablocks must be kept idle before being sent to the cloud. **On-Prem Retention age** specifies the number of hours/days files will be kept locally after they are sent to the cloud. We also need to add a few advanced options for NetVault. Click **Advanced Options** and add “/config” into the **Exclude Folder Paths** field as well as ".*.(stnz|check_status)" into the **Stub Exclude File Regular Expression** field. Finally, click **Enable**.



Edit Archive Policy

Archive Policy

Idle time before cloud migration: 7 — format: days

On-Prem Retention Age: 90 — format: days

Advanced Options

Folder Paths(Optional)

Include Folder Paths: /dir, /c, /d

Exclude Folder Paths: /config

File Extensions/Regular Expressions (Optional)

Type: Exclude Regular Expression

Extensions:

Stub Exclude Dir/Extensions/Regular Expressions(Optional)

Stub Exclude Directory List: /dir, /c, /d

Stub Exclude File Extension List: txt, log

Stub Exclude File Regular Expression: .*.(stnz|check_status)

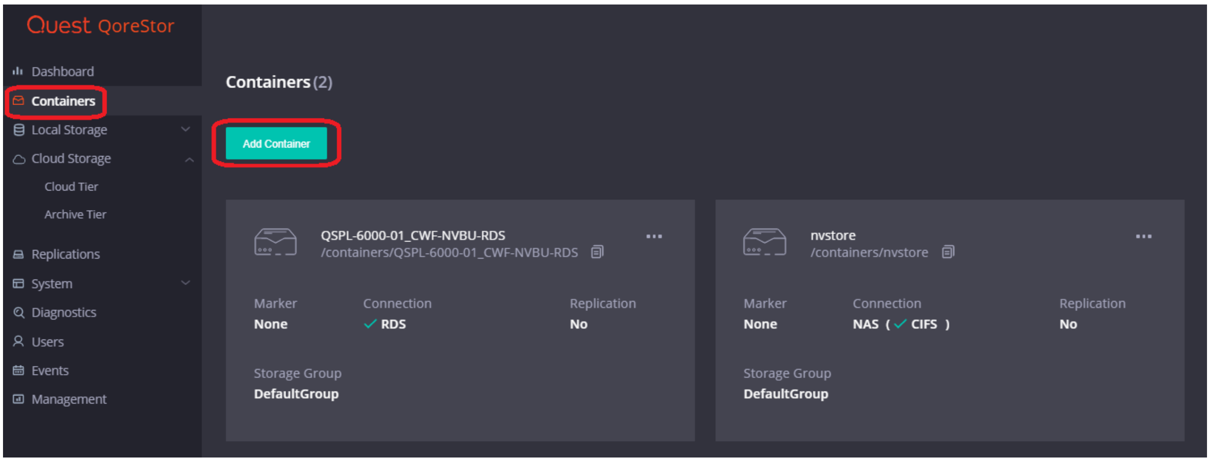
CAUTION: **Make Please use the Command line command documented in the “Important Considerations” section for Cloud and Archive tier to insure required NetVault files do not get tiered**

8

Creating a Cloud or Archive Container

A Cloud or Archive container is a container created directly in the cloud or archive storage group. This container does not have a policy defined, all data written to it goes directly to the cloud or archive. The use case for this is to allow users to configure their data management application with multiple storage devices. Thus, controlling what data is sent to the cloud simply be writing data to one container or the other. Before following these steps please complete the steps documented in the *Creating a policy-driven Cloud Tier* or *Creating a policy-driven Archive Tier* Sections.

1. Open the QoreStor UI and navigate to the **containers** page. Click **Add Container**.



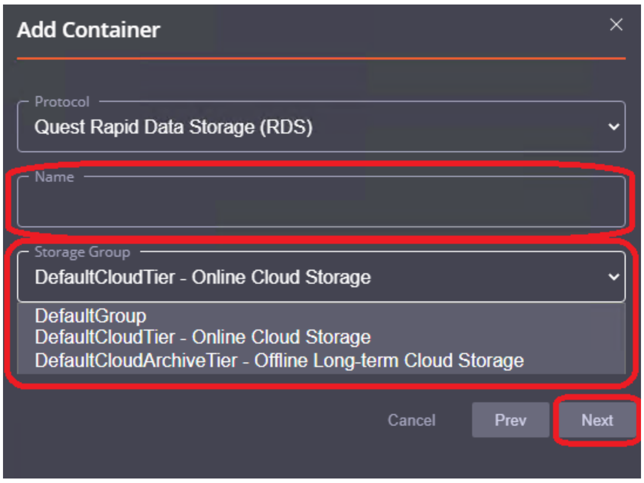
QSPL-6000-01_CWF-NVBU-RDS
/containers/QSPL-6000-01_CWF-NVBU-RDS

Marker: None
Connection: ✓ RDS
Replication: No
Storage Group: DefaultGroup

nvstore
/containers/nvstore

Marker: None
Connection: NAS (✓ CIFS)
Replication: No
Storage Group: DefaultGroup

2. In the **Add Container** wizard enter a **Name** for the container then change the **Storage Group** to either **DefaultCloudTier** or **DefaultCloudArchiveTier** depending on need. These storage groups will not show unless the cloud tier or archive tier is already configured. Click **Next**.



Add Container

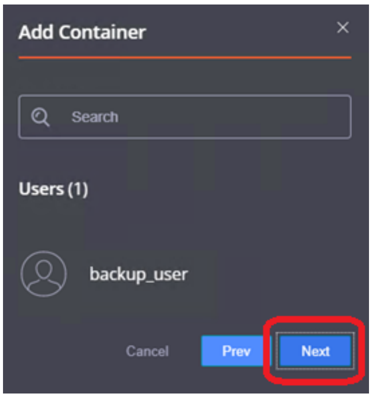
Protocol: Quest Rapid Data Storage (RDS)

Name:

Storage Group: DefaultCloudTier - Online Cloud Storage

DefaultGroup
DefaultCloudTier - Online Cloud Storage
DefaultCloudArchiveTier - Offline Long-term Cloud Storage

3. Click **Next** On the user page.



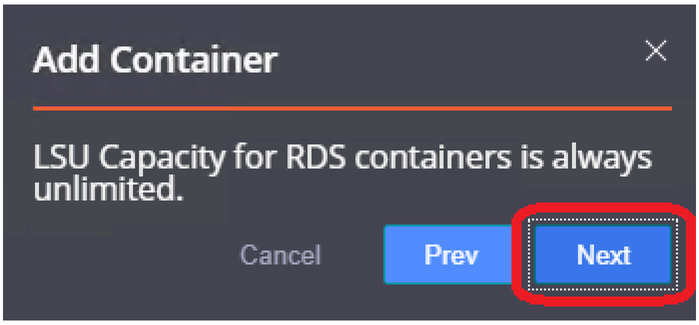
Add Container

Search

Users (1)

backup_user

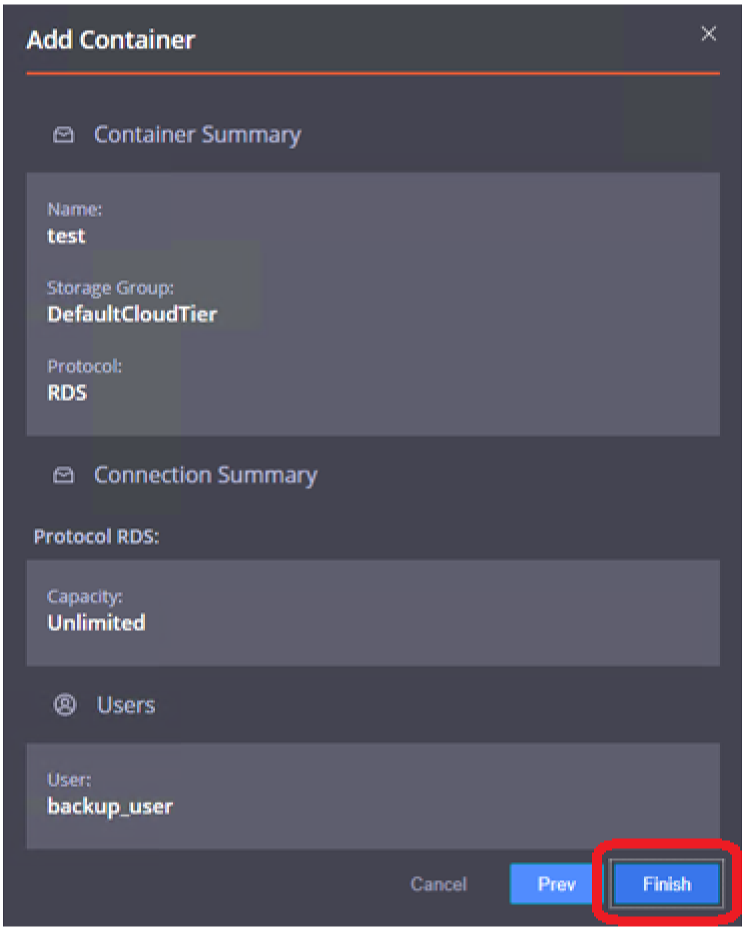
4. Click **Next** on the capacity page.



Add Container

LSU Capacity for RDS containers is always unlimited.

5. Verify configuration and click **Finish**.



Add Container

Container Summary

Name:
test

Storage Group:
DefaultCloudTier

Protocol:
RDS

Connection Summary

Protocol RDS:

Capacity:
Unlimited

Users

User:
backup_user

6. Add this container to the DMA just like previously listed in this guide. All backups to this specific container will go to the cloud/archive without being stored on-prem via policy.

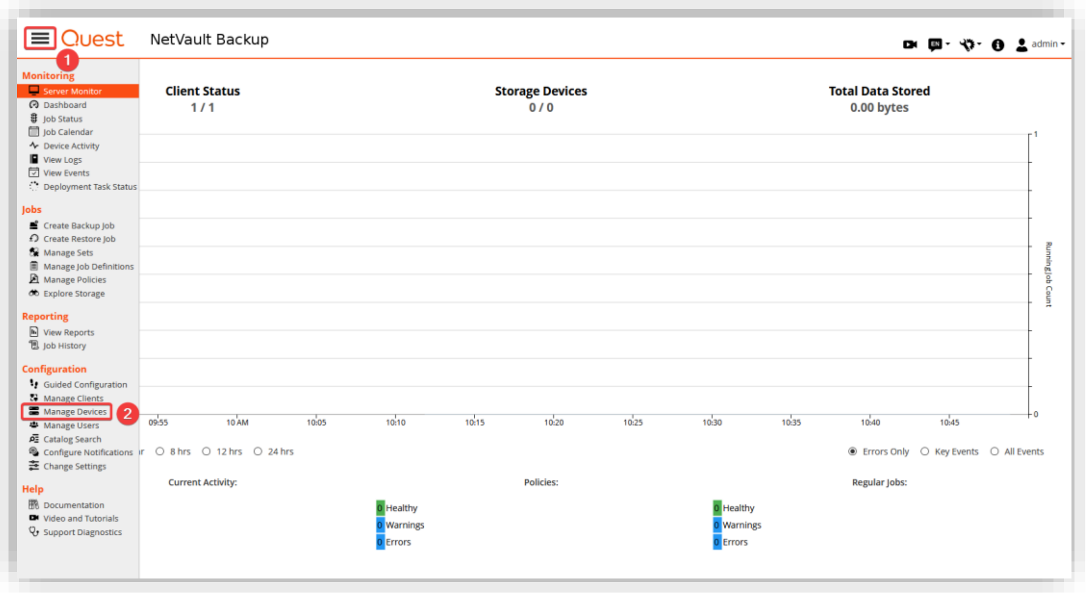
9

Creating a QoreStor storage group

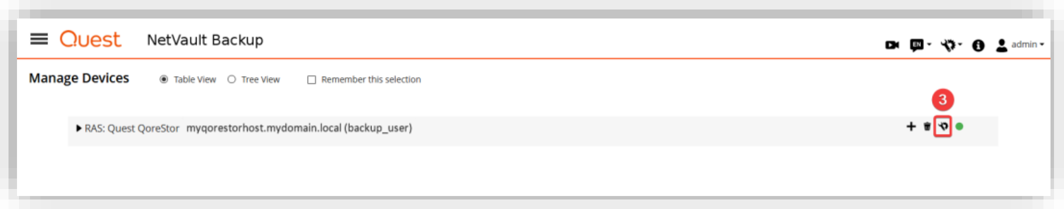
If you wish to create a QoreStor storage group, you can use the QoreStor Administrative Console, QoreStor CLI, or the NetVault Backup UI. In this document, we will show how to do it using the NetVault Backup UI.

1. Open the NetVault Backup UI

Open the **menu drawer ❶** and select **Manage Devices ❷**



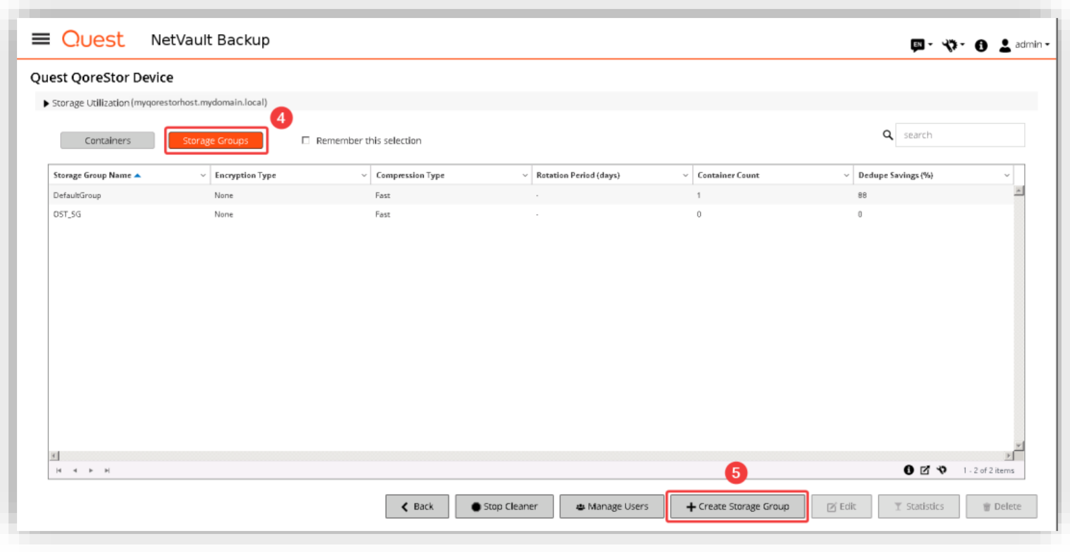
Click on the **Manage Device** button ❸



RAS: Quest QoreStor myqorestorhost.mydomain.local (backup_user)

Click the **Storage Groups** button ❹

Click the Create Storage Group button ❺



Storage Group Name	Encryption Type	Compression Type	Rotation Period (days)	Container Count	Dedupe Savings (%)
DefaultGroup	None	Fast	-	1	88
OST_SG	None	Fast	-	0	0

On the pop-up dialog:

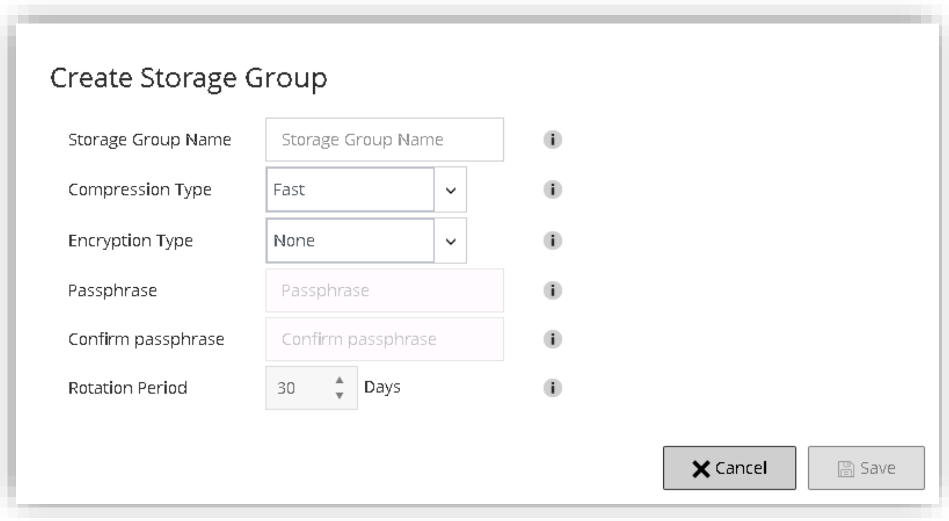
a Enter the Storage Group Name

b Select the desired **Compression Type** using the dropdown arrow

c Select the desired **Encryption Type** using the dropdown arrow if you wish to use encryption

If you select Internal, chose a Passphrase, Confirm passphrase, and Rotation Period

d Click the **Save** button



Create Storage Group

Storage Group Name: Storage Group Name

Compression Type: Fast

Encryption Type: None

Passphrase: Passphrase

Confirm passphrase: Confirm passphrase

Rotation Period: 30 Days

NOTE: If using NetVault 11.4.5, after clicking the **Manage Device** button, open the **menu drawer** under **Actions** and select **Explore** for the chosen Storage Group; then click the **Add LSU** button and enter the name for the Container you wish to create under **Add LSU Name**.

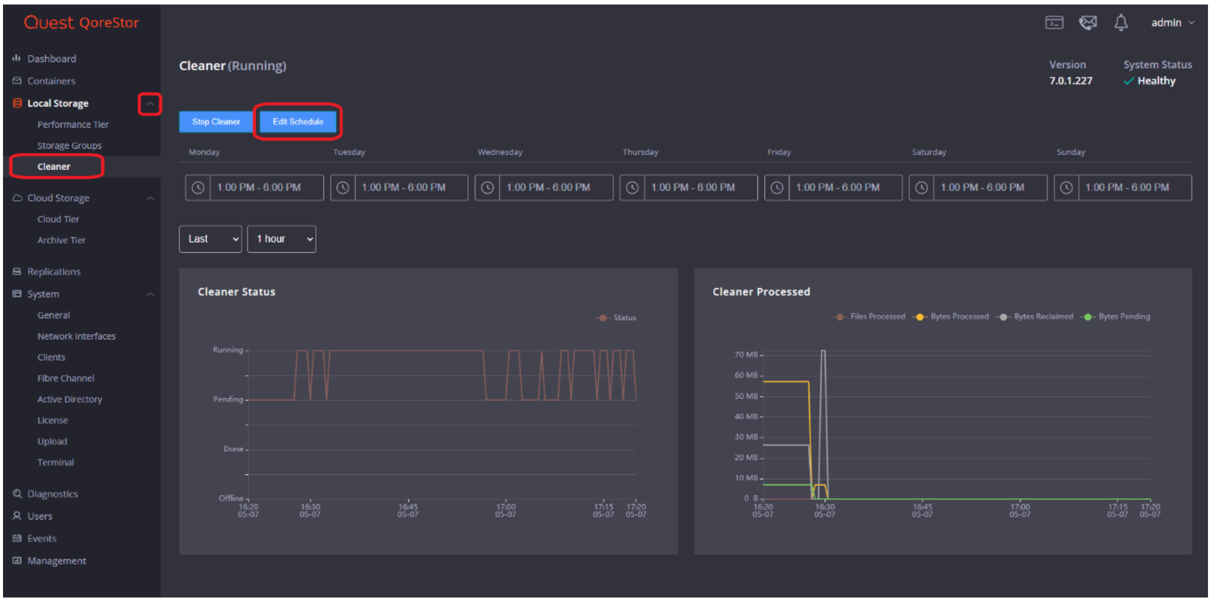
Appendix A

Setting up the QoreStor system cleaner

Performing scheduled disk space reclamation operations are needed as a method for recovering disk space from system containers in which files were deleted as a result of deduplication. Ideally, the QoreStor cleaner should complete a full cycle at least once a week. This will be accomplished in most cases by the predefined QoreStor cleaner schedule. The cleaner also runs during idle time.

To change the predefined cleaner schedule times, perform the following steps:

1. Open the QoreStor administrative console
2. Expand **Local Storage** in the top navigation area
3. Select **Cleaner**
4. Click **Edit Schedule.**



Cleaner (Running)

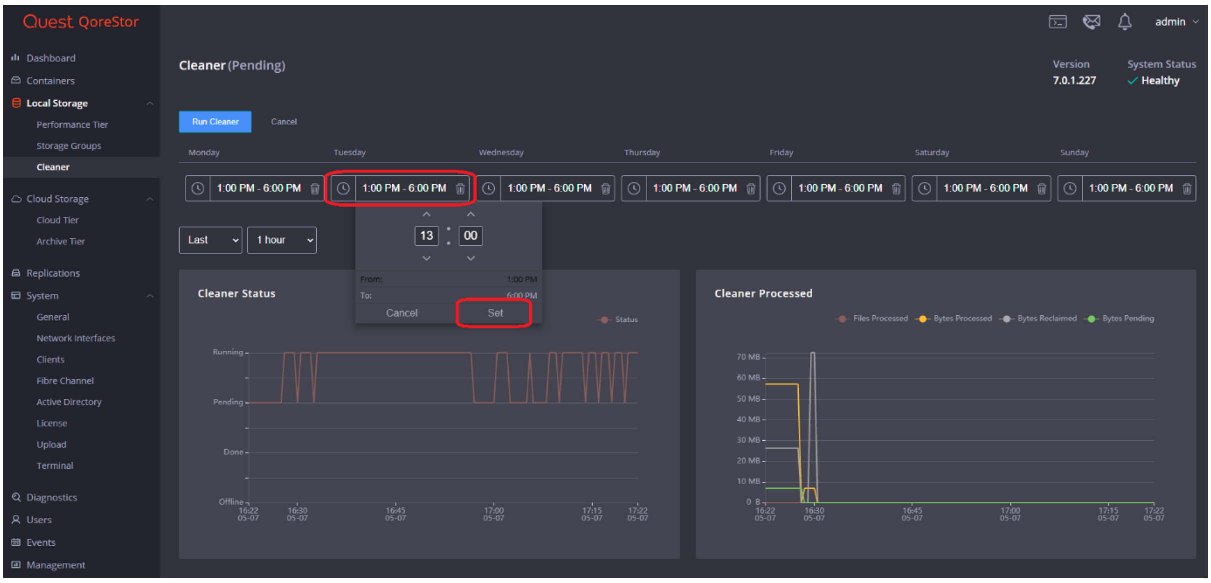
Version 7.0.1.227

System Status ✓ Healthy

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
1:00 PM - 6:00 PM	1:00 PM - 6:00 PM	1:00 PM - 6:00 PM	1:00 PM - 6:00 PM	1:00 PM - 6:00 PM	1:00 PM - 6:00 PM	1:00 PM - 6:00 PM

Last 1 hour

5. Define the schedule and click **Set**.



If necessary, you can also perform a full cleaning cycle manually using either the QoreStor Administrative Console, QoreStor CLI, or the NetVault Backup UI.

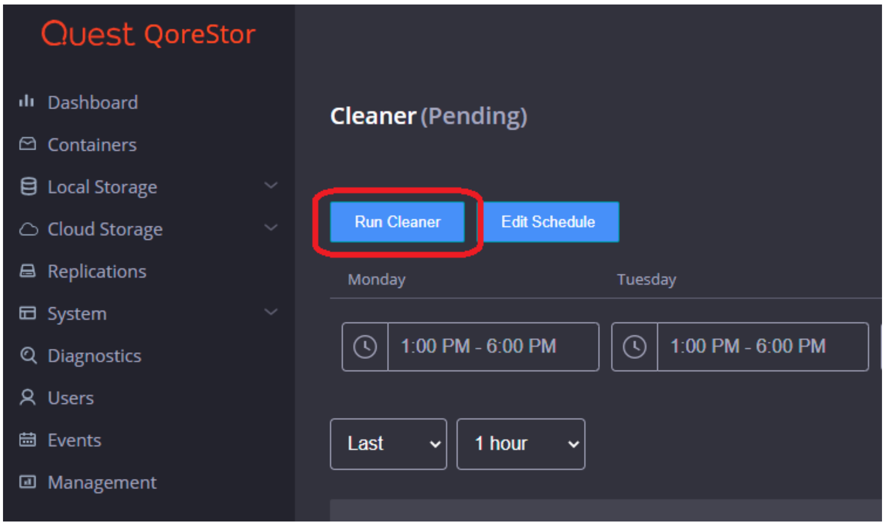
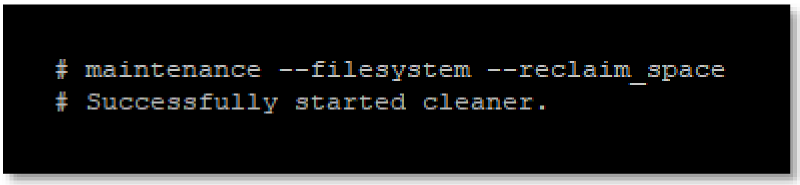
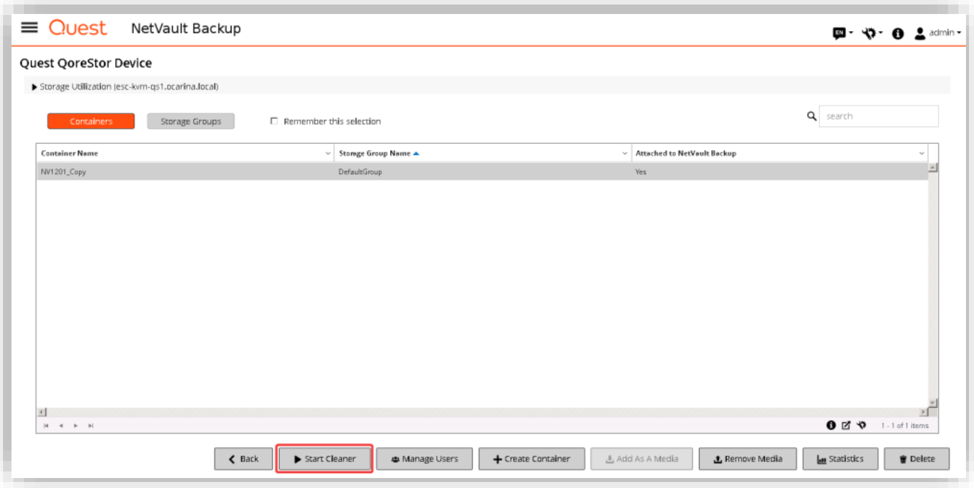


Figure 1: Using the QoreStor Administrative Console



```
# maintenance --filesystem --reclaim_space
# Successfully started cleaner.
```

Figure 2: Using the QoreStor CLI



□ Remember this selection

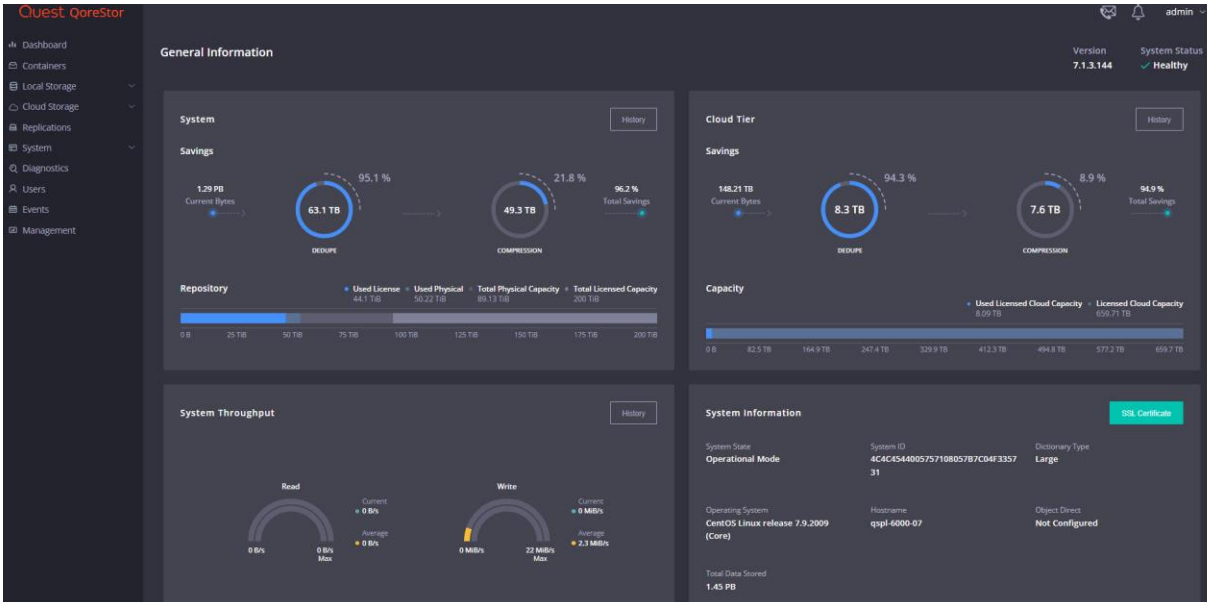
Container Name	Storage Group Name	Attached to NetVault Backup
NV1201_Copy	DefaultGroup	Yes

Figure 3: Using the NetVault Backup UI

Appendix B

Monitoring deduplication, compression, and performance

After backup jobs have run, QoreStor tracks capacity, storage savings, and throughput. The historical representation of these values is shown in the dashboard of the QoreStor administrative console. This information is valuable in understanding the benefits of QoreStor.



Version 7.1.3.144

System Status ✓ Healthy

System State: Operational Mode

System ID: 4C4C4544005757108057B7C04F3357 31

Dictionary Type: Large

Operating System: CentOS Linux release 7.9.2009 (Core)

Hostname: qspl-6000-07

Object Direct: Not Configured

Total Data Stored: 1.45 PB

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.