



Quest® QoreStor™ 7.0

User Guide
Revision 1



© 2023 Quest Software Inc. ALL RIGHTS RESERVED.

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

 **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.

QoreStor User Guide
Updated - September 2020
Version - 7.0

Contents

Introducing Quest® QoreStor™	9
Understanding the QoreStor documentation	10
Other information you may need	10
Information on compatible products	11
Source code availability	12
QoreStor data storage concepts	12
Data deduplication and compression	12
Encryption at rest	12
Streams and connections	13
Quotas	13
Secure connect	13
MultiConnect	14
Replication	14
Reverse replication	15
Reverse replication: alternate method	16
Performance Tier	16
Cloud Tier	16
Archive tier	17
Object interface (S3-compatible)	17
Object Direct Storage	18
Disaster Recovery from the cloud	18
Cloud tier disaster recovery	18
Archive tier disaster recovery	18
Supported file system protocols	18
CIFS	19
CIFS ACL support	19
NFS	20
Rapid NFS and Rapid CIFS benefits	20
Rapid NFS and Rapid CIFS	20
RDA with Quest's Netvault Backup and vRanger	21
RDA with OST for QoreStor	21
Software components and operational guidelines	22
NDMP	23
iSCSI	23
QoreStor processes	24
Accessing QoreStor	26
Networking prerequisites for QoreStor	26
Configurations required when using proxy servers	27

Logging onto the system GUI for the first time	27
Configuring QoreStor with the Configuration Menu	27
Initial login and changing your password	28
Initial network configuration	28
Using the QoreStor Menu	28
QoreStor Administration	31
QoreStor Maintenance	33
QoreStor Statistics	33
Using the QoreStor UI	34
QoreStor UI Overview	34
Using the QoreStor command line	35
Using the QoreStor Web Terminal	36
Using the QoreStor REST API	36
API Overview	37
Authentication	37
API Documentation	37
Configuring QoreStor settings	39
Licensing QoreStor	39
Evaluating QoreStor	39
Viewing your license configuration	40
Installing a license	40
Configuring an SSL certificate for your QoreStor system	41
Installing an SSL certificate	41
Restoring the default certificate	41
Configuring Active Directory settings	41
Adding a login group to an ADS domain	42
Removing a login group	43
Understanding system operation scheduling	43
Configuring cleaner schedules	44
Viewing cleaner status	45
Viewing cleaner statistics	45
Configuring Secure Connect	46
Enabling Secure Connect for OST and RDA plug-ins prior to 4.1.0.265	46
Configuring Secure Connect properties	47
Managing Secure Connect with OST or RDA plug-in 4.1.0.265 or later	48
Checking Secure Connect status	49
Disabling Secure Connect	49
Enabling Secure Connect	50
Adding certificates for Secure Connect	50
Adding a Secure Connect certificate - Windows Client	50
Adding a Secure Connect certificate - Linux Client and QoreStor server	51
Enabling MultiConnect	52

Configuring and using Rapid NFS and Rapid CIFS	53
Rapid NFS and Rapid CIFS benefits	54
Best practices: Rapid NFS	54
Best practices: Rapid CIFS	55
Installing the Rapid NFS plug-in	56
Downloading the Rapid NFS Plug-in	57
Enabling Secure Connect	57
Installing the plug-in	57
Installing the Rapid CIFS plug-in	58
Downloading the Rapid CIFS Plug-in	58
Enabling Secure Connect	58
Installing the plug-in	58
Monitoring performance	59
Uninstalling the Rapid NFS plug-in	60
Uninstalling the Rapid CIFS plug-in	60
Configuring and using VTL	61
Understanding VTL	61
Terminology	61
Supported virtual tape library access protocols	61
NDMP	61
iSCSI	62
VTL and QoreStor specifications	62
Guidelines for configuring VTL	63
Plan your Environment	63
Create Containers of Type VTL	64
Authentication/User Management Considerations	64
Verify the Tape Library Creation	65
Configure the Library in the DMA	65
Configuring and Using Encryption at Rest	66
Understanding Encryption at Rest	66
Encryption at Rest Terminology	66
Encryption at Rest and QoreStor Considerations	67
Understanding the encryption process	68
Configuring email alert settings	68
Managing containers	70
Viewing containers	70
Viewing containers in the GUI	71
Viewing containers via the CLI	71
Viewing container statistics	71
Displaying container statistics by using the CLI	72
Creating a container	73
Creating an OST or RDS connection type container	73
Configuring User Access Controls	74
Creating an NFS or CIFS connection type container	75

Creating an Object container	78
Adding an object container through the command line	79
Creating a VTL type container	80
Viewing VTL tape information	83
Adding a Cloud Tiering policy	84
Using regular expressions	85
Example expressions	85
Limitations	86
Adding an Archive Tiering Policy	86
Deleting a container	87
Deleting a container through the GUI	87
Deleting a container through the command line	87
Managing local storage	89
Viewing storage group information	89
Adding a storage group	91
Adding a storage group through the GUI	91
Adding a storage group through the command line	92
Modifying a storage group	92
Deleting a storage group	94
Deleting a storage group from the GUI	94
Deleting a storage group from the CLI	94
Configuring a Performance Tier	94
Adding a performance tier	95
Adding a performance tier through the command line	95
Editing a performance tier	96
Configuring Object Container	97
Creating an Object container	97
Adding an object container through the command line	99
Creating a bucket	99
Editing bucket settings	100
Changing bucket retention	101
Deleting a bucket	102
Setting user policy	102
Configuring additional storage	102
Guidelines for configuring additional storage	103
Adding additional storage	103
Managing cloud storage	104
Adding a Cloud Tier	104
Adding a cloud tier through the GUI	104
Adding a Microsoft Azure cloud tier	104
Adding an Amazon S3 cloud tier	105
Adding a Wasabi S3 cloud tier	107

Adding a Google S3 cloud tier	108
Adding an S3 Compatible cloud tier	110
Adding a cloud tier through the command line	111
Deleting a cloud tier	111
Deleting a cloud tier from the GUI	111
Deleting a cloud tier from the CLI	112
Configuring an Archive Tier	112
Required permissions to restore from Archive Tier	112
Adding an archive tier	113
Deleting an archive tier	115
Deleting a cloud tier from the GUI	115
Deleting an archive tier from the CLI	116
Restoring from archive tier	116
Manually restoring datastores from Amazon S3 Glacier	116
Performing a recovery from the cloud	118
Next steps	119
Managing replications	121
Guidelines and prerequisites for replication	121
Replication seeding	122
Adding replication relationships	122
Configuring replication schedules	123
Viewing replication information	124
Modifying replication relationships	125
Deleting replication relationships	126
Starting and stopping replication	126
Managing users	127
Managing the default QoreStor user accounts	127
Viewing users	128
Viewing users through the GUI	128
Viewing users through the command line	128
Adding a user	128
Adding a user through the GUI	128
Adding a user through the command line	129
Modifying user roles	129
Modifying a user through the GUI	130
Modifying a user through the command line	130
Changing a user password	130
Deleting a user	131
Deleting a user account through the GUI	131
Deleting a user account through the command line	131

Managing QoreStor Remotely	132
Getting Started With the Global View Cloud Portal	132
Registering QoreStor with the Quest Global View Cloud	132
Enabling Remote Management	133
Viewing and using the GlobalView Cloud Portal	133
Monitoring QoreStor	135
Using the Dashboard page	135
Viewing QoreStor statistics by using the CLI	137
Monitoring system alerts	138
Monitoring clients	138
Monitoring clients through the QoreStor GUI	138
Monitoring clients through the QoreStor CLI	138
Monitoring system events	139
Support, maintenance, and troubleshooting	140
Using QoreStor Diagnostics	140
Viewing system diagnostic log files	140
Understanding diagnostics collection	141
Generating a diagnostics log file	141
Downloading diagnostics log files	142
Deleting a Diagnostics Log File	142
Troubleshooting error conditions	142
About us	144
Contacting Quest	144
Technical support resources	144

Introducing Quest® QoreStor™

Quest® QoreStor™ is a software-defined secondary storage platform based on Quest's proven DR Appliance's resilient deduplication and replication technologies. With QoreStor, you can break free of backup appliances and accelerate backup performance, reduce storage requirements and costs, and replicate safer and faster to the cloud for data archiving, disaster recovery and business continuity.

QoreStor supports all of the major backup software applications in use today and can lower your backup storage costs to as little as \$.16/GB while reducing your total cost of ownership. QoreStor achieves these results using patented Rapid technology as well as built-in, variable block-based deduplication and compression.

Lower costs and maximize the return on your IT investment by leveraging virtually any storage hardware, virtualization platform or cloud provider. QoreStor also supports many backup software solutions — so it's not just for Quest. Simple to deploy and easy to manage, QoreStor enables you to shrink replication time, improve data security and address compliance requirements.

QoreStor helps you to:

- Reduce on-premises and cloud storage costs with industry-leading deduplication and compression.
- Accelerate backup completion with protocol accelerators and dedupe.
- Shrink replication time by transmitting only changed data.
- Improve data security and comply with FIPS 140-2.
- Maximize return on investment for existing data protection technologies.
- Lower total cost of ownership through all-inclusive licensing.

QoreStor includes the following features:

- Hardware and software agnostic platform
- Next-generation storage dedupe engine
- Built-in protocol accelerators
- Support for a wide variety of data backup installations and environments.

Understanding the QoreStor documentation

The topics in this guide introduce and describe how to use the QoreStor web-based graphical user interface (GUI) to manage your system. It describes how to access the comprehensive system GUI and the associated features and capabilities, how to perform a wide variety of data storage and replication operations, how to manage the system, as well as how to manage the related storage and replication containers.

In addition to the QoreStor GUI, you can manage QoreStor by using a command-line interface (CLI). In some instances, the GUI provides additional features and options that are not available in the CLI and vice versa.

This documentation is written for an administrator.

i **NOTE:** For information about the supported web browsers you can use with QoreStor, see the **System Requirements** chapter in the *QoreStor Installation Guide*.

Other information you may need

The following table lists the documentation available for QoreStor. The documents listed in this table are available on the Quest support website by selecting your specific QoreStor version at:

<http://support.quest.com/QoreStor>

Table 1: QoreStor documentation

Document	Description
QoreStor Installation Guide	Provides information on installation and operation requirements, supported platforms as well as procedures for installing QoreStor.
QoreStor User Guide	Provides information on configuring and using QoreStor.
QoreStor Release Notes	Provides the latest information about new features and known issues with a specific product release.
QoreStor Command Line Reference Guide	Provides information about managing QoreStor data backup and replication operations using the QoreStor command line interface (CLI).
QoreStor Interoperability Guide	Provides information on supported infrastructure components.
QoreStor Virtual Machine Deployment Guide	Provides information on deploying the QoreStor virtual machine on VMware ESX or Microsoft Hyper-V.
Additional whitepapers	Instructions and best practices for configuring additional Quest and third-party applications to work with QoreStor.

i **NOTE:** Check for the latest documentation updates and release notes at <http://support.quest.com/qorestor>. Read the release notes first because they contain the most recently documented information about known issues with a specific product release.

Information on compatible products

QoreStor offers direct integration with Quest Software's NetVault® Backup and vRanger®, as well as Veritas NetBackup and Backup Exec. For more information on those products refer to the documents below.

Table 2: Quest NetVault Backup documentation

Document	Description
NetVault Backup Installation Guide	Provides information about installing and upgrading the NetVault Backup server and client software.
NetVault Backup Administration Guide	Describes how to configure and use NetVault Backup to protect your data. This document also provides information on configuring QoreStor repositories and migrating NetVault SmartDisk data to the new QoreStor repository.
NetVault Backup Release Notes	Provides the latest information about new features and known issues with a specific product release.

i | **NOTE:** See the complete NetVault Backup documentation at <https://support.quest.com/netvault-backup>.

Table 3: Quest vRanger documentation

Document	Description
vRanger Installation/Upgrade Guide	This document provides information on supported platforms, system requirements, and instructions on installing and upgrading vRanger.
vRanger User Guide	This document provides information and procedures on configuring and using vRanger to protect virtual and physical environments.
vRanger Release Notes	This document details the issues resolved in this release, the known issues as of this release, and the third party components in vRanger.

i | **NOTE:** See the complete vRanger documentation at <https://support.quest.com/vranger>.

Table 4: Veritas documentation

Document	Description
Veritas NetBackup	For information on Veritas NetBackup, refer to the NetBackup product documentation .
Veritas Backup Exec	For information on Veritas Backup Exec, refer to the Backup Exec product documentation .

Source code availability

A portion of the QoreStor may contain or consist of open source software, which you can use under the terms and conditions of the specific license under which the open source software is distributed.

Under certain open source software licenses, you are also entitled to obtain the corresponding source files. For more information or to find the corresponding source files for respective programs, see the Quest website at opensource.quest.com.

QoreStor data storage concepts

Data deduplication and compression

The QoreStor design uses various data-reduction technologies, including advanced deduplication algorithms, in addition to the generic and custom compression solutions that prove effective across many differing file types. Data deduplication and compression are addressed in the following areas:

- **Deduplication** — This technology eliminates redundant copies of data and in the process it decreases disk capacity requirements and reduces the bandwidth needed for data transfer. Deduplication can be a major asset for companies that are dealing with increasing data volumes and require a means for optimizing their data protection.
- **Compression** — This technology reduces the size of data that is stored, protected, and transmitted. Compression helps companies improve their backup and recovery times while helping reduce infrastructure and network resource constraints.

In general, QoreStor offers advanced deduplication and compression capabilities to reduce the time and cost associated with backing up and restoring data. Based on deduplication and compression technology, QoreStor eliminates the need to maintain multiple copies of the same data. This lets customers keep more data online longer and reduce the need for tape backup dependency.

Using its deduplication and compression technology, QoreStor can help achieve an expected data reduction ratio of 15:1. Achieving this reduction in data means that you need fewer incremental storage operations to run and it provides you with a smaller backup footprint. By removing redundant data, QoreStor deliver fast reliable backup and restore functionality, reduce media usage and power and cooling requirements, and improve your overall data protection and retention costs.

For a complete list of supported management application, refer to the *QoreStor Interoperability Guide*.

Encryption at rest

Data that resides on QoreStor can be encrypted. When encryption is enabled, QoreStor uses the Industry standard FIPS 140-2 compliant 256-bit Advanced Encryption Standard (AES) encryption algorithm for encrypting and decrypting user data. The content encryption key is managed by the key manager, which operates in either a Static mode or an Internal mode. In Static mode, a global, fixed key is used to encrypt all data. In internal mode, key lifecycle management is performed in which the keys are periodically rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7 days. This rotation period is user-configurable and can be specified in days. A user-defined passphrase is used to generate a pass phrase key, which is used to encrypt the content encryption keys. It is mandatory to define a passphrase to enable encryption. The system supports up to a limit of 1023 different content encryption keys.



NOTE: Due to export regulations, the encryption at rest feature is not available in certain markets, and, therefore, may not be available in your locale.

Streams and connections

This topic describes the differences between data streams and application connections.

Streams refer to the number of files written at the same time to QoreStor. QoreStor tracks the number of files being written and assembles the data into 4-MB chunks before processing that section of the data. If the stream count is exceeded, the data is processed out of order and overall deduplication savings can be affected.

Connections are created by applications; and, within a single connection, there can be multiple streams depending on the application and the number backup jobs running in parallel over that single connection.

Quotas

QoreStor provides the option to configure quotas for Storage Groups and Performance Tiers. With quotas, you can define a limit for physical capacity usage. Upon reaching that limit, data ingests to that storage group or performance tier will be disallowed until sufficient space is recovered through cleaner operations.

Before considering implementing quotas, please take into account these limitations and recommendations:

- Quotas are not set by default.
- The minimum quota value is 100 GiB.
- Once set, quotas can be reduced, but cannot be set below the storage group's used capacity.
- For standard storage groups, the maximum quota value is restricted to the current physical capacity of the QoreStor system.
 - For performance tiers, the maximum quota value is restricted to the the size of the performance tier filesystem.

Secure connect

Secure Connect encompasses a set of client and server components that creates a secure channel for QoreStor communication with WAN-connected clients that is also resilient to WAN outages.

Secure Connect uses the TLS 1.2 standard with a 4096-bit RSA key. Certificates are created automatically for both client and server, but you can use you own certificates if you chose. When using Secure Connect (which is enabled by default when using the latest QoreStor and plug-in versions), the client opens a connection to the QoreStor server over port 9443. The client sends the actual QoreStor port number to the server, which then opens a local connection to that port enabling secure communication with the client. Configuration of Secure Connect ports is done through the client and server configuration file. See [Configuring Secure Connect](#) for more information.

Secure Connect also provides a method for resilient WAN connections. Packets processed by Secure Connect clients are assigned a unique identifier and are assigned to a temporary cache before being sent to the QoreStor server. When the packet is successfully delivered to the QoreStor Secure Connect server, the packet identifier is marked as delivered and acknowledged to the Secure Connect client. If the WAN connection is lost, the client and server both continue to cache data packets. When the connection is restored, unacknowledged packets are re-sent and properly processed, avoiding data loss and process interruption.

MultiConnect

QoreStor MultiConnect establishes multiple connections between RDA and OST clients and the QoreStor server. On high-bandwidth networks, these connections can improve backup and replication performance. To obtain the most benefit from MultiConnect, both MultiConnect and SecureConnect should be enabled. Refer to the sections below:

- [Enabling Secure Connect for OST and RDA plug-ins prior to 4.1.0.265](#)
- [Enabling MultiConnect](#)

Replication

Replication is the process by which key data is saved from storage locations, with the goal of maintaining consistency between redundant resources in data storage environments. Data replication improves the level of fault-tolerance, which improves the reliability of maintaining saved data and permits accessibility to the same stored data.

QoreStor uses an active form of replication that lets you configure a primary-backup scheme. During replication, the system processes data storage requests from a specified source to a specified replica target, which acts as a replica of the original source data.

i | **NOTE:** QoreStor includes version checking that limits replication only between other QoreStor instances or DR Series systems that run a compatible software release version. If versions are incompatible, the administrator is notified by an event.

Replicas are read-only and are updated with new or unique data during scheduled or manual replications. QoreStor can be considered to act as a form of a storage replication process in which the backup and deduplication data is replicated in real-time or via a scheduled window in a network environment. In a replication relationship between two or three QoreStor instances or DR Series systems, this means that a relationship exists between a number of systems. One system acts as the source and the other as a replica.

Replication is done at the container level and is one directional from source to replica; however, since replication is done at the container level you can set up various containers to meet your specific replication requirements for your specific workflow. This form of replication is supported for the CIFS, NFS, Rapid CIFS, and Rapid NFS, RDA, and Object protocols and is fully handled by QoreStor.

QoreStor supports replication seeding, which provides the ability to create a local seed and place it in a remote system. The seed backup is a process on the source QoreStor system, which collects all of the unique data chunks from the containers and stores them on the target device. This is helpful if you have a new replication target to set up, the amount of data to be replicated is very large, and the network bandwidth is low.

i | **NOTE:** The storage capacity of the target QoreStor system is directly affected by the number of source systems writing to its containers, and by the amount being written by each of the source systems.

If the source and target systems are in different Active Directory (AD) domains, then the data that resides on the target system may not be accessible. When AD is used to perform authentication for QoreStor systems, the AD information is saved with the file. This can act to restrict user access to the data based on the type of AD permissions that are in place.

i | **NOTE:** This same authentication information is replicated to the target QoreStor system when you have replication configured. To prevent domain access issues, ensure that both the target and source systems reside in the same Active Directory domain.

Reverse replication

The concept of reverse replication is not a supported operation on QoreStor. This is because replica containers are always in a R-O (read-only) mode on QoreStor, thus making write operations a non-supported operation.

Alternate ways to retrieve data

Under very specific conditions, it could be possible for replica containers to support a type of write operation whose sole function is to restore data from an archival target. For example, data could be replicated back to the remote site where a data management application (DMA), or backup software, is connected to allow this data to be restored directly.

This specific type of case applies only to configurations where data is backed up from a remote location to a local container, and then replicated over a WAN to a replica container that is backed up to tape. The data needs to be restored from the tape backup to the original location; first back to QoreStor replica container, and then back to the original source location of the data on the other side of the WAN link.

i **NOTE:** If you choose to use this alternate workaround method, you must set up a new data storage unit in your DMA, and import the images before a restore to the original location can occur.

To leverage this type of deduplication across the WAN, complete the following:

1. Make sure that the replication operation has completed (between source and target).
2. Delete the current replication relationship, and re-create a replication relationship (reversing the source and target roles).
3. Restore data to the original source container (now the target).
4. Make sure that the replication operation has completed.
5. Delete the replication relationship and re-create a replication relationship (restoring original source and target destinations).

Under this scenario, a fraction of the data to be recovered is sent across the WAN link. This could speed up a remote restore significantly. However, there are some downsides to this type of scenario:

- If step 1 is not followed correctly, any changes not fully replicated are lost.
- During steps 2 and 3, any data that is written to the original QoreStor source container may be lost.
- During step 4, if the data is not fully replicated back before the switch is made, it may be lost.

Alternatively, you could still support this type of effort by completing the following:

1. Create a new container on the target QoreStor instance.
2. Set up replication from this container back to the source QoreStor system container.
3. Set up a new disk storage unit in the DMA and make sure that the DMA is aware of any new images.
4. Import the old images back into the DMA from the target QoreStor instance (the original source location).
5. Use a new disk storage unit in the DMA, and then restore the data back to the original client.

Reverse replication: alternate method

For an alternate method of reverse replication, complete the following steps:

1. Create a new container on the target QoreStor instance.
2. Set up replication from this container back to the source QoreStor container.
3. Set up a new disk storage unit in your Data Management Application (DMA) and make sure that the DMA is aware of any new images.
4. Import the old images back into the DMA from the target QoreStor instance (the original source location).
5. Use a new disk storage unit in the DMA, and then restore the data back to the original client.

Performance Tier

In situations where certain workloads have requirements for faster recovery, QoreStor allows you to write these workloads to a performance tier to enable faster read back unaffected by activity in other QoreStor Storage Groups. By utilizing a performance tier, you are able to maximize the value of higher-performing storage by ensuring that only the most critical workloads are written to it.

To create a QoreStor performance tier, you must create a physical volume comprised of high-performing storage (such as SSD) and then create a QoreStor storage group mapped to that volume. Containers created on that storage group will write and read from high-performance storage exclusively and will be isolated from read activity on other volumes.

Cloud Tier

QoreStor's cloud tier feature enables QoreStor data to be quickly and easily accelerated to the cloud tier. Using your existing data management applications (DMAs) and any supported protocol, files can be written to a QoreStor container and replicated to your cloud tier according to easily defined policies.

QoreStor provides a policy engine that allows you to set idle time 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.

In addition, there is an **On-Prem Retention Age** policy that allows you to specify how long a copy of a file is kept after it has been replicated to the cloud tier. Once a file has been replicated, the file on the QoreStor server becomes a stub, meaning it exists in the namespace but the data exists only in the cloud tier. Once a file has been stubbed and moved to the cloud tier, that file can no longer be edited.

With these policy options, you are able to configure cloud tier replication to meet one of three use cases:

- **Data replication** - this creates a direct copy of the backup data stored in QoreStor on the cloud tier.
- **Extended hold** - this offloads older and less frequently accessed data to the cloud tier for long-term

archiving.

- **Replicate and extend** - this provides both a direct replica and a long-term archive.

Any data that is transferred from the QoreStor instance by the cloud tier is encrypted with zero knowledge encryption. The encryption keys are solely owned by you. If the encryption keys are placed in the cloud 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 cloud tier.

Archive tier

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 your existing data management applications (DMAs) and a supported protocol (Object(S3), VTL or RDS), 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 a 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_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

Object interface (S3-compatible)

QoreStor's Object container provides an object storage interface which enables customers to write Object data(S3 format) directly to Qore. This allows solutions that leverage an S3-based connection to send data directly to a QoreStor instance instead of Amazon S3 with the added benefits of deduplication, encryption, replication and network optimized data transfer.

With object storage enabled, QoreStor creates a **ObjectStorageGroup** storage group and **ObjectContainer** container. This container can be configured with a cloud tiering policy to seamlessly move data to long-term storage. QoreStor allows you to configure multiple buckets within your object container namespace, each with different locking and retention settings.

Object Direct Storage

Object storage organizes files and their associated metadata into objects, which are then stored in a flat address space. Object storage provides greater insight to data usage, improved scalability, and lower storage costs when compared to traditional file or block storage. QoreStor can be installed in object-direct mode, which utilizes object storage for the main data repository, while metadata is written to higher performing storage. For more information, refer to the topics **QoreStor Installation Modes** and **Installing QoreStor with Object Direct Storage** in the *QoreStor Installation Guide*.

i | **NOTE:** When QoreStor is installed in an Object Direct configuration, if the backend object storage is not accessible QoreStor will go into Manual Intervention mode.

Disaster Recovery from the cloud

When configured with a Cloud Tier or Archive Tier, QoreStor provides the ability to capture QoreStor configuration information as well as storage group and container data. With this information, it is possible to re-create a lost or failed QoreStor server using the data in the cloud. Please note that the data which is not cloud replicated and is still present in the local disk is not recoverable in case of a failure with the primary QoreStor.

Cloud tier disaster recovery

In the event of QoreStor server failure, a recovery can be initiated on a new, licensed QoreStor server to restore from the previous configuration stored in the cloud. At a high-level, a recovery will go through the following steps:

- Connect to your cloud provider with configured credentials and passphrase.

i | **IMPORTANT:** The required passphrase is the passphrase used when creating the Cloud Tier. Without the Cloud Tier passphrase recovery cannot proceed.

- The new QoreStor will read the stored configuration once it is connected to the cloud .
- Rebuilds the cloud-replicated containers as well as other storage groups and containers.
- Runs the filesystem check and brings the QoreStor to a consistent state.

For more information refer to [Performing a disaster recovery from the cloud](#).

Archive tier disaster recovery

When performing data recovery from an Archive Tier, you must first restore all datastores to standard AWS S3 storage using the AWS Management Console. For more information refer to [Manual Restore from Glacier](#) and [Restoring from archive tier](#).

Supported file system protocols

QoreStor supports the following file system protocols. The Rapid Data Access (RDA) protocols below provide a logical disk interface that can be used with network storage devices to store data and support data storage operation.

- Network File System (NFS)
- Common Internet File System (CIFS)
- Rapid Data Access (RDA)
 - Rapid NFS
 - Rapid CIFS
 - RDA with OpenStorage Technology (OST)
 - RDA with NetVault Backup
 - RDA with vRanger
- The virtual tape library (VTL) tape access protocols:
 - Network Data Management Protocol (NDMP)
 - Internet Small Computer System Interface (iSCSI)
- Other supported access protocols
 - Object (S3)

CIFS

The Common Internet File System (CIFS) remote file access protocol is supported by QoreStor, and is also known as a Server Message Block (SMB). SMB occurs more commonly than the Network File System (NFS) protocol on systems that run the Microsoft Windows operating system. CIFS allows programs to request files or services on remote computers.

CIFS also uses the client-server programming model, whereby the client requests access to a file or passes a message to a program running on the server. Servers review all requested actions and return a response. CIFS is a public (or open) variation of the SMB that was originally developed and used by Microsoft.

i | **NOTE:** QoreStor currently supports version 2.0 and 3.0 of the Server Message Block (SMB).

i | **NOTE:** For complete details on CIFS feature restrictions, see the *QoreStor Interoperability Guide*, at support.quest.com/qorestor.

CIFS ACL support

QoreStor supports the use of access control lists (ACLs) for CIFS and share-level permissions. By definition, an ACL is simply a list of permissions that can be associated with any network resource.

Each ACL can contain access control entries (ACEs) that define or describe the permissions for an individual user or a group of users. An ACL can consist of zero (meaning that all users have access) or a number of ACEs that define specific permissions on a per-user or per-group basis.

i | **NOTE:** If an ACE list is empty (meaning that it contains zero entries), this means that all access requests will be granted.

An ACL describes the entities that are allowed to access a specific resource. ACLs are a built-in access control mechanism in the Windows operating systems.

i | **NOTE:** QoreStor supports setting up share-level permissions for a CIFS share using a Microsoft Windows administrative tool. Share-level permissions let you control access to shares. For more information, see [Configuring Share-Level Security](#).

NFS

The Network File System (NFS) is a file system protocol that is designated to be a file server standard, and its protocol uses the Remote Procedure Call (RPC) method of communication between computers. Clients can access files via the network similar to the way that local storage is accessed.

NFS is a client-server application in which a client can view, store, and update files on a remote system just like they are working on a local system. System or Network Administrators can mount all or a portion of a file system, and the file system (or portion) that is mounted can be accessed using the privileges assigned to each file.

i | **NOTE:** If you want to do a mount on AIX, you must set the `nfs_use_reserved_ports` and `portcheck` parameters first. The parameters cannot be set to 0. For example: `root@aixhost1 / # nfsso -po portcheck=1 root@aixhost1 / # nfsso -po nfs_use_reserved_ports=1`

Rapid NFS and Rapid CIFS benefits

When Rapid NFS and Rapid CIFS are used with QoreStor they offer the following benefits:

- Reduce network utilization and DMA backup time
 - Chunk data and perform hash computation on the client; transfer chunked hash files on the back-end
 - Reduce the amount of data that must be written across the wire
- Improve performance
- Support DMAs such as CommVault, EMC Networker, and Tivoli Storage Manager. For the current list of supported DMAs, see the *QoreStor Interoperability Guide*.
- Compatible with existing NFS and CIFS clients — just need to install a plug-in (driver) on the client
 - Can use Rapid NFS and Rapid CIFS to accelerate I/O operations on any client — including a client that uses home-grown backup scripts
 - Can service multiple and concurrent media server backups

Rapid NFS and Rapid CIFS

Rapid NFS and Rapid CIFS enable write operation acceleration on clients that use QoreStor replication and NFS or CIFS file system protocols. Similar to OST and RDS, these accelerators allow for better coordination and integration between QoreStor backup, restore, and optimized deduplication operations with Data Management Applications (DMAs) such as CommVault, EMC Networker, and Tivoli Storage Manager. For the current list of qualified DMAs, see the *QoreStor Interoperability Guide*.

Rapid NFS is a new client file system type that ensures that only unique data is written to QoreStor. It uses user space components and file system in user space (FUSE) to accomplish this. Metadata operations such as file creates and permission changes go through the standard NFS protocol, whereas write operations go through RDNFS.

Rapid CIFS is a Windows-certified filter driver that also ensures that only unique data is written to QoreStor.

All chunking and hash computations are done at the media or client server level.

Rapid NFS and Rapid CIFS require you to install a plug-in on the client or media server, depending on your DMA and configuration. For details, see "Configuring and Using Rapid NFS and Rapid CIFS".

RDA with Quest's Netvault Backup and vRanger

Rapid Data Access (RDA) with NetVault Backup and with vRanger provides the logical disk interface that can be used with network storage devices. QoreStor requires the NetVault Backup Plug-in *for Rapid Data Access* to integrate its data storage operations with NetVault Backup and vRanger. The plug-in is installed by default on the NetVault Backup and vRanger servers and QoreStor when the latest software updates are installed. Using the Plug-in *for Rapid Data Access*, NetVault Backup can take full advantage of key QoreStor and DR Series system features like data deduplication and managed replication.

When the Plug-in *for Rapid Data Access* is used with QoreStor, it offers the following benefits:

- RDA with NetVault Backup and RDA with vRanger protocols provides faster and improved data transfers:
 - Focus is on backups with minimal overhead
 - Accommodates larger data transfer sizes
 - Provides throughput that is better than CIFS or NFS
- RDA and data management application (DMA) integration:
 - NetVault Backup-to-media server software communication
 - QoreStor storage capabilities can be used without extensive changes to NetVault Backup or vRanger.
 - Backup and replication operations are simplified by using built-in DMA policies
- QoreStor RDA ports and write operations:
 - Control channel uses TCP port 10011
 - Data channel uses TCP port 11000
 - Optimized write operations enable client-side deduplication
- Replication operations between QoreStor systems:
 - No configuration is required on the source or target QoreStor systems
 - Replication is file-based, not container-based
 - Replication is triggered and managed by the backup application
 - QoreStor transfers the data file (not the media server)
 - After duplication completes, QoreStor notifies the DMA to update its catalog (acknowledging the second backup). This makes the DMA aware of the replication location. Restores from either the source or replication target can be used directly from the DMA.
 - Supports different retention policies between source and replica
 - Replication is set up in the DMA itself, not QoreStor

RDA with OST for QoreStor

OpenStorage Technology (OST), by Veritas, provides a logical disk interface for use with network storage devices. QoreStor can use OST via QoreStor plug-in software to integrate its data storage operations with NetBackup and Backup Exec.

RDA with OST allows for better coordination and tighter integration between QoreStor system backup, restore, and optimized duplication operations and data management applications (DMAs). For a list of the supported applications, see the *QoreStor Interoperability Guide*.

Integration is done via a RDA with OST plug-in developed for QoreStor, through which data management applications can control when the backup images are created, duplicated, and deleted. The major benefit of RDA with OST is that it allows the deduplication operations to happen on the client side so that network traffic can be reduced.

The RDA with OST plug-in allows data management applications to take full advantage of such QoreStor features as data deduplication, replication, and energy efficiency. QoreStor systems can access the OpenStorage API code through the plug-in, which can be installed on the media server platform choice you make (Windows or Linux). The OST protocol allows the supported backup applications to communicate directly with QoreStor and determine whether a specific chunk of data already exists on the system. This process means that if the data already exists, only the pointers need to be updated on QoreStor, and the duplicate chunk of data does not need to be transferred to the system. This process provides two benefits: it improves the overall backup speed, and also reduces the network load.

When RDA with OST is used with QoreStor, it offers the following benefits:

- OST protocol provides faster and improved data transfers:
 - Focused on backups with minimal overhead
 - Accommodates larger data transfer sizes
 - Provides throughput that is significantly better than CIFS or NFS
- RDA with OST and DMA integration:
 - OpenStorage API enables the DMA-to-media server software communications
 - QoreStor storage capabilities can be used without extensive changes to DMAs
 - Backup and replication operations are simplified by using built-in DMA policies
- QoreStor and RDA with OST:
 - Control channel uses TCP port 10011
 - Data channel uses TCP port 11000
 - Optimized write operations enable client-side deduplication

Software components and operational guidelines

To better coordinate and integrate OpenStorage Technology (OST) with QoreStor data storage operations, the following guidelines list the required components and supported operations. For details on the supported operating systems and data management application (DMA) versions, see the *QoreStor Interoperability Guide*.

QoreStor licensing is all-inclusive, so that no additional licensing is required to use OST or the optimized duplication capability. The OST plug-in that gets installed on a supported Linux or Windows media server platform is a free download. However, Veritas NetBackup requires that you purchase an OpenStorage Disk Option license. Similarly, Veritas Backup Exec requires that you purchase the Deduplication Option to enable the OST feature.

- OST Media Server Component:
 - An OST server component resides on the QoreStor server.
 - For Linux media server installations, use the Linux OST plug-in and the Red Hat Package Manager (RPM) installer
 - For Windows media server installations, use the Windows OST plug-in and the Microsoft (MSI) installer
- Windows-based OST plug-in
- Linux-based 64-bit OST plug-in
- Supported OpenStorage (OST) protocol:
 - Version 9
 - Version 10
- Supported Veritas DMAs
 - NetBackup
 - Backup Exec
- Supported OST operations
 - Backup (Passthrough writes and Optimized writes)
 - Restore
 - Replication
 - Auto Image Replication (AIR)

NDMP

The Network Data Management protocol (NDMP) is used to control data backup and recovery between primary and secondary storage in a network environment. For example, a NAS server (Filer) can talk to a tape drive for the purposes of a backup.

You can use the protocol with a centralized data management application (DMA) to back up data on file servers running on different platforms to tape drives or tape libraries located elsewhere within the network. The protocol separates the data path from the control path and minimizes demands on network resources. With NDMP, a network file server can communicate directly to a network-attached tape drive or virtual tape library (VTL) for backup or recovery.

The QoreStor VTL container type is designed to work seamlessly with the NDMP protocol.

iSCSI

iSCSI or **Internet Small Computer System Interface** is an Internet Protocol (IP)-based storage networking standard for storage subsystems. It is a carrier protocol for SCSI. SCSI commands are sent over IP networks by using iSCSI. It also facilitates data transfers over intranets and to manage storage over long distances. iSCSI can be used to transmit data over LANs or WANs.

In iSCSI, clients are called *initiators* and SCSI storage devices are *targets*. The protocol allows an *initiator* to send SCSI commands (*CDBs*) to the *targets* on remote servers. It is a storage area network (SAN) protocol, allowing organizations to consolidate storage into data center storage arrays while providing hosts (such as database and

web servers) with the illusion of locally attached disks. Unlike traditional Fibre Channel, which requires different cabling, iSCSI can be run over long distances using existing network infrastructure.

iSCSI is a low-cost alternative to Fibre Channel, which requires dedicated infrastructure except in FCoE (Fibre Channel over Ethernet). Note that the performance of an iSCSI SAN deployment can be degraded if not operated on a dedicated network or subnet

The VTL container type is designed to work seamlessly with the iSCSI protocol. For details, see [Creating a VTL type container](#).

QoreStor processes

The table below describes the processes that QoreStor installs and runs on the QoreStor server.

Table 5: QoreStor processes

Process	Description
nhm	Node Health Monitoring service - maintains a database for alerts and events.
object_server	Used for object container support
oca_idm_eda	An event and data aggregator service for events and alerts.
ocaagent_charts	Periodically (every hour) sends QoreStor chart related data to the Global View Cloud.
ocaagent_diagnostics	Periodically queries database for keep-alive commands. Responsible only for handling diagnostic upload command.
ocaagent_keeplive	Queries the Global View Cloud for keep-alive commands (diagnostic upload and portal unregistration) and executes them. This query occurs once a minute.
ocaagent_managebutton	Allows for remote control of QoreStor through Global View Cloud. When enabled, waits for remote management RPC commands from Global View Cloud, invokes them via API on QoreStor, and sends results back to the Global View Cloud.
ocaagent_registration	Handles Global View Cloud registration, operates on a DB table responsible for holding registration status, and performs registration/unregistration requests.
ocaagent_stats	Periodically(every 30 minutes, or when significant changes occur) sends statistic data (storage groups, containers, analytics, system information etc.) to the Global View Cloud.
ocaconfigsvc	QoreStor configuration service to manage the storage groups, containers, and replication links and handle requests from the QoreStor CLI and UI.
ocafsd	QoreStor file system service to export containers, process data and manage the data on the disk.
ocahttp	QoreStor HTTP server to service requests for QoreStor web UI and REST API methods. Uses ocafsd, ocaconfigsvc and r3 database (graphs).
ocamonitor	QoreStor process for periodically collecting stats from ocafsd, ocaconfigsvc and Linux system monitoring tools and populating an internal (r3) database.

ocardslogwriter	Process captures logging from all the processes, writes the data to the corresponding logs, and rotates the logs.
sc_server	A Secure Connect server that handles secure connects from OST and RDA plug-ins
watcher	Watcher process monitors other QoreStor processes. The watcher process will respawn other processes as necessary to keep the service online.
watcher_spawn	This process monitors watcher process and spawns if necessary.

Accessing QoreStor

You can interact with QoreStor using one of the methods below:

- The QoreStor GUI, accessible in a web browser using the URL `https://<YourQoreStorServerName>:5233`.
- The QoreStor command line interface (CLI). Refer to the *QoreStor Command Line Reference Guide* for more information.
- The QoreStor configuration menu, which can be accessed via a terminal emulation program using the `qsservice` credentials. Refer to [Configuring QoreStor with the Configuration Menu](#) for more information.

In the system GUI, you can configure your system as well as create and manage containers, which store your backup and deduplicated data. A data container is a shared file system that is imported using a client, and is accessible via file system or tape access protocols. For details, see [Supported File System Protocols](#). The system GUI also provides real-time summary information for monitoring the status of the data capacity, storage savings, and the throughput of your data containers.

Networking prerequisites for QoreStor

Before you can start using QoreStor, ensure that you have satisfied the following networking prerequisites:

- **Network:** An active network is available using Ethernet cables and connections.
- **Replication ports:** the replication service in QoreStor requires that enabled fixed ports be configured to support replication operations that are to be performed across firewalls (TCP ports 9904, 9911, 9915, and 9916).
 - **NOTE:** For more information about replication ports, see [Managing Replication Operations](#), and for more information about system ports, see the *QoreStor Installation Guide*.
- **Proxy servers:** when using a proxy server, some additional configurations are required. Refer to [Configurations required when using proxy servers](#).

Configurations required when using proxy servers

If you have configured your QoreStor instance to use one or both of the Linux exports below, the QoreStor Watcher service will not be able to function properly as watcher communications will be sent to the proxy.

```
export http_proxy=http://<hostname>:<port>
export https_proxy=http://<hostname>:<port>
```

To ensure proper operation, you must also include the **no_proxy** export.

```
export no_proxy="localhost, 127.0.0.1"
```

i **NOTE:** In order for these configurations to persist after a system reboot, they must be entered into `/etc/environment`.

Logging onto the system GUI for the first time

To log on to the QoreStor GUI for the first time, complete the following steps:

1. In a supported web browser, enter:

- `https://<YourQoreStorServerName>:5233`

i **NOTE:** The QoreStor Login page may display a warning message if the web browser you are using does not properly support QoreStor. If you are running a Microsoft Internet Explorer (IE) web browser, make sure that you disable the Compatibility View. For more information about disabling the Compatibility View settings, see the topic, [Disabling the Compatibility View Settings](#). For more information about supported web browsers, see the **System Requirements** chapter of the *QoreStor Installation Guide*.

2. In the **Username** field, type **admin**, and in the Password field, type **St0r@ge!** and then click Log in or press **<Enter>**.

Your logon username is displayed at the top of the page in the right corner.

Configuring QoreStor with the Configuration Menu

The sections below contain the steps and information required to configure the QoreStor server for the first time.

- [Initial login and changing your password](#)
- [Initial network configuration](#)

- [Using the QoreStor Menu](#)
 - [QoreStor Administration](#)
 - [QoreStor Maintenance](#)
 - [QoreStor Statistics](#)


Initial login and changing your password

After the QoreStor is complete, you will be prompted to log in. When logging in for the first time with the default credentials, you are required to change the password.

1. on to the QoreStor using the default credentials:
username: **qsservice**
password: **changeme**
2. You will be prompted to enter the current password. Enter **changeme**.
3. You will be prompted to enter your new password, and then to confirm it.
4. Continue to [Initial network configuration](#).

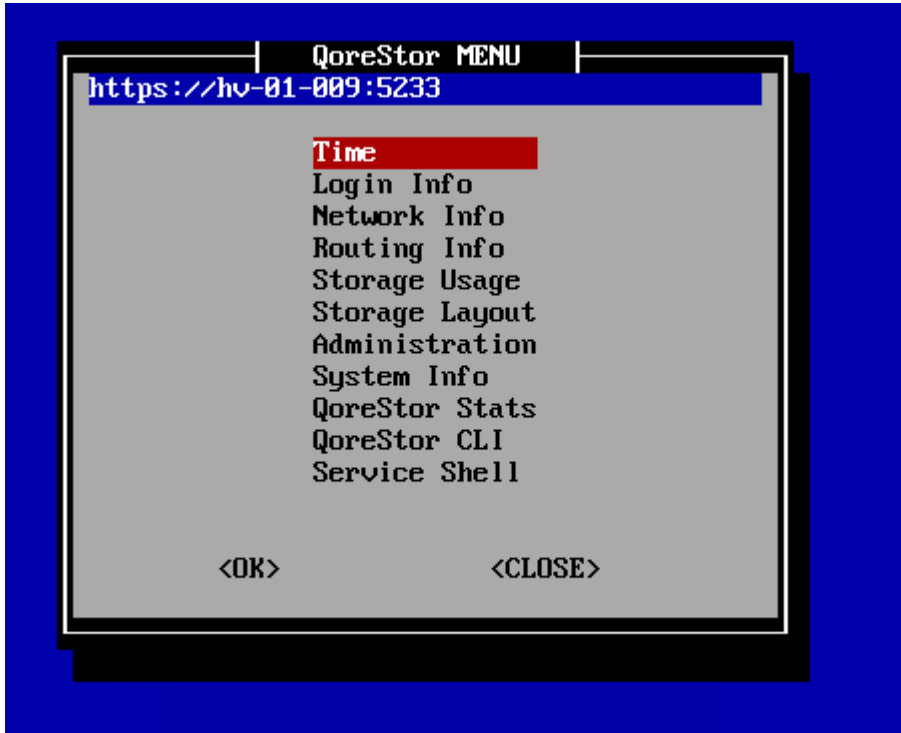
Initial network configuration

After changing the default password, you will be prompted to provide the initial networking information for your environment.

1. At the **Change Hostname** page, enter a valid hostname or fully qualified domain name (FQDN).
 **NOTE:** Hostnames must comply with the standards RFC 1123 and RFC 952. Hostnames may only contain the letters a-z, the numbers 0-9, the "-" (hyphen), and the "." period (or dot).
2. At the **Edit Network Connections** page, you will be prompted to edit the network connections. If you are using DHCP, select **No**. If you are using Static IP, select **Yes**.
3. Follow the screen prompts to configure the required network entries and confirm the configuration settings.
4. After the required network settings are configured, QoreStor will run the initial configuration, which may take up to 3-4 minutes to complete.
5. Continue to [Using the QoreStor Menu](#).

Using the QoreStor Menu

After the initial configuration, the QoreStor menu will be displayed.



The table below details the configurations available for each menu item. The **Administration**, **QoreStor Maintenance**, and **QoreStor Stats** menu items provide access to additional sub-menus, and are documented separately in the topics linked to below.

NOTE: To navigate the menu, use the arrow keys to select an entry, then press **[Enter]**. To return to the menu, use the **[Tab]** key to select **Ok** or **Back**, then press **[Enter]**.

Table 6:
QoreStor Menu options

Menu item	Available configurations
Time	<ul style="list-style-type: none"> • Show time and date configuration • Configure system clock • Sync time to pool.ntp.org • Show hardware clock • Set hardware clock to system time • Change time zone
Login Info	Displays information about which accounts are currently logged into the QoreStor server, and the processes those accounts are using.
Network Info	Displays the current network configuration.
Routing Info	Displays the current routing table.

Storage Usage	<p>Displays the current storage configuration for each filesystem, including:</p> <ul style="list-style-type: none"> • size • used space • available space • used percentage • mount path
Storage Layout	<p>Displays the layout per storage device, including:</p> <ul style="list-style-type: none"> • Device name • Filesystem type • Mountpoint • UUID • Schedule • Model
Administration	<p>Provides options to configure networking, storage, application and operating system configurations. Refer to the section QoreStor Administration</p>
System Info	<p>Displays information about the QoreStor system, including:</p> <ul style="list-style-type: none"> • output of the QoreStor system <code>--show</code> command • Management user interface information and credentials • license information
QoreStor Stats	<p>Provides access to QoreStor system statistics. Refer to QoreStor Statistics for more information.</p>
QoreStor CLI	<p>Allows access to the QoreStor CLI commands using the qsadmin account. Refer to the <i>QoreStor Command Line Reference Guide</i> for more information. To return to the QoreStor Menu from the CLI, type exit at the prompt.</p> <p>i IMPORTANT: You must be logged in as the qsadmin account when executing QoreStor commands.</p>
Service Shell	<p>Allows access to the Service Shell using the qsservice account. The Service Shell is intended for OS and storage maintenance, and as such, the qsservice account has sufficient privileges for those tasks. To return to the QoreStor Menu from the shell, type exit at the prompt.</p> <p>i NOTE: The qsservice account is not intended for executing QoreStor commands. To execute QoreStor commands you must use the qsadmin account. From the Service Shell, you must either change user accounts to the qsadmin account using</p> <pre>#sudo su - qsadmin</pre> <p>or exit to the QoreStor menu and select QoreStor CLI.</p>

QoreStor Administration

The Administration Menu includes the options described in the table below. In addition, the Administration menu includes a status banner that indicates the status of the QoreStor service:

- Blue: Operational Mode
- Red: Manual Intervention
- Yellow: Maintenance Mode

Table 7: Operation menu options

Menu item	Available configurations
Network Config	Allows you to edit the network configuration.
Set Hostname	Allows you to change the hostname configuration.
QoreStor services	Provides options to check, stop, start, and restart QoreStor services.
QoreStor Update	Provides options to check for available QoreStor updates, download the Qorestor update package, and update QoreStor if the package is valid.
QoreStor Maintenance	Provides access to QoreStor filesystem maintenance utilities and diagnostic management. Refer to QoreStor Maintenance for more information.
QoreStor Advanced Features	Provides options to tune system performance: <ul style="list-style-type: none">• Replication Tuning - allows you to configure the number of concurrent replication streams. Default value is 1.• Buffers TCP Tuning - allows you to change the system buffer configuration up to 1.5 GB.• ActiveDS tuning - allows you to enable or disable ActiveDS on the metadata location.• O3E IO Thread tuning - Enables IO thread tuning. This requires a restart of the QoreStor services.• SMB Offload Copy - Enables SMB Server Offload Copy support, used for Rapid CIFS-based Veeam Fast Clone backups. Enabling this option requires a restart of QoreStor services.
Troubleshooting tools	Provides tools to troubleshoot your QoreStor machine. Consult the documentation for each utility for more information. <ul style="list-style-type: none">• EPEL Repository - Enables or disables the Oracle EPEL repository.• top - allows you to monitor processes and system resource usage.

- **atop** - allows you to monitor processes and system resource usage. You will be prompted to install atop on first use.
- **htop** - - allows you to monitor processes and system resource usage. You will be prompted to install htop on first use.
- **iostat** - allows you to view I/O usage.
- **iftop** - allows you to view bandwidth usage. You will be prompted to install iftop on first use.
- **nmon** - allows you to monitor processes and system resource usage. You will be prompted to install nmon on first use.
- **glances** - - allows you to monitor processes and system resource usage. You will be prompted to install glances on first use.
- **tree** - provides a recursive directory listing with a depth-indented listing of files. You will be prompted to install tree on first use.

i | **NOTE:** To return to the Troubleshooting tools menu from the selected monitoring tool, press **q** to quit.

Operating System	Provides options to update , restart , and shutdown the operating system. Additionally, this menu provides options for removing and/or adding the built-in QoreStor accounts (root , qsservice , and qsadmin).
Terminal	Provides options to select from a list of terminal emulators. Options are: <ul style="list-style-type: none"> • XTERM • XTERM-256 • ANSI • VT220 • VT110
Color theme	Provides options to change the color theme settings.
Locale	Provides the option to select the locale for QoreStor. Currently, the only option is US English.
Proxy Settings	Provides the option to enable proxy settings. <p>i NOTE: Editing or disabling proxy settings requires QoreStor services to be restarted.</p>

QoreStor Maintenance

The QoreStor System Maintenance menu provides access to both diagnostic and maintenance utilities for QoreStor. The QoreStor System Maintenance menu includes the utilities listed in the table below.

Table 8: QoreStor Maintenance menu options

Menu item	Available configurations
QoreStor Diagnostics	<ul style="list-style-type: none">• Diagnostics Show• Diagnostics Collect• Diagnostics Delete• Diagnostics Delete All
Maintenance Filesystem	<ul style="list-style-type: none">• Filesystem Scan Status• Filesystem Scan Report• Filesystem Scan Start• Filesystem Scan Restart• Filesystem Scan Stop• Filesystem Repair Start• Filesystem Repair Progress• Filesystem Repair History• Filesystem Clear Quarantine• Filesystem Start Cleaner• Filesystem Stop Cleaner

QoreStor Statistics

The QoreStor Stats menu provides access to QoreStor system statistics. The QoreStor Stats menu includes the statistics listed below:

- System
- CPU
- Memory
- Container
- Storage Group
- Replication
- Cleaner
- Clients
- Servers
- Seed

- Performance tier
- Archive Tier
- Object container

Using the QoreStor UI

QoreStor offers a web-based user interface that you can use to configure, manage, and monitor your QoreStor system. You can use the QoreStor UI to perform tasks such as:

- Configure containers, storage groups, and cloud storage groups
- Add and manage replications
- View system information and monitor performance
- Manage user accounts
- Generate and download diagnostic bundles

You can access the QoreStor UI from any supported browser. Refer to [Logging onto the system GUI for the first time](#) for more information.

QoreStor UI Overview

The QoreStor UI consists of the Header pane, the Navigation pane, a Status pane, and the Operations pane.



The panes provide the functions and options described below:

Pane	Description
Header pane	Provides the following items:

- Terminal icon - Provides a quick link to the QoreStor web terminal. Refer to [Using the QoreStor Web Terminal](#).
- Contact Us icon - information for contacting Quest sales and Support.
- QoreStor Alerts - lists any Alerts on the QoreStor system.
- Current user - displays the current user account, provides the option to log out, and provides the option to switch the UI to the Light theme.

Status pane	Provides the following items: <ul style="list-style-type: none"> • Version - displays the version of QoreStor • System Status - displays the status of the QoreStor.
Navigation pane	Provides navigation options to: <ul style="list-style-type: none"> • Dashboard • Containers • Local Storage • Cloud Storage • Replications • System • Diagnostics • Users • Events • Management
Operations pane	Displays the data and dialogs appropriate for the chosen navigation option.

Using the QoreStor command line

QoreStor includes a custom shell implementation that simplifies and secures command line access. During installation, QoreStor creates the **qsadmin** user account with the permissions and configurations necessary to run QoreStor commands. You can access the QoreStor command line through a remote access program (such as PuTTY) or through the QoreStor UI Web Terminal.

To access the command line interface for QoreStor:

1. Using a remote access program, connect to your QoreStor server.

i | **NOTE:** You may also access the QoreStor command line through the QoreStor Web Terminal. Refer to [Using the QoreStor Web Terminal](#) for more information.

2. Log in using the credentials:

user: qsadmin

password: St0r@ge!

3. Enter the desired command at the prompt. To view the available QoreStor CLI commands, type **help**.

i | **NOTE:** Refer to the *QoreStor Command Line Reference Guide* for more information on the QoreStor CLI.

Using the QoreStor Web Terminal

The QoreStor UI offers direct access to the QoreStor terminal for execution of CLI commands through the browser.

To access the Web Terminal

1. On the QoreStor UI, select **System** to expand the menu. Click **Terminal**

2. In the **Username** field, enter the desired user name. You will be prompted for the password.

i | **NOTE:** QoreStor includes a custom shell implementation that simplifies and secures command line access. During installation, QoreStor creates the **qsadmin** user account with the permissions and configurations necessary to run QoreStor commands. Unless absolutely necessary, Quest recommends using the **qsadmin** account for CLI access. The default credentials are:

user: qsadmin

password: St0r@ge!

3. Click **Connect to** authenticate and access the terminal.

4. To view the list of available QoreStor commands, enter **help** at the prompt.

i | **NOTE:** Refer to the *QoreStor Command Line Reference Guide* for more detailed information on QoreStor CLI commands.

5. To log out of the terminal, enter **exit** at the prompt.

i | **NOTE:** When using Internet Explorer 11 to access the QoreStor UI, the Terminal page is displayed directly after logging in to QoreStor. The QoreStor navigation menu is not displayed and use of other UI functions is not supported.

Using the QoreStor REST API

QoreStor provides a REST API in order to provide an efficient method for application management or integration. For more information on using the REST API, see the sections below.

API Overview

All API requests should be sent to **https://<QoreStor host>:5233/api**. With the exception of the Authentication request, all requests should carry the HTTP header `Authorization: Bearer <token>`.

API calls will generate one of the response types below. Refer to the API documentation for the specific request for more information on expected responses.

- 200 - OK
- 400 - Bad request
- 401 - Unauthorized
- 404 - Not found
- 500 - Internal server error

Authentication

Authentication to the API is accomplished using the username and password for an existing QoreStor account. Once logged in, a token will be generated that can be used to authenticate API commands.

To use API authentication:

1. Execute the **login** request using the username and password for the desired QoreStor account as well as the IP or domain name of your QoreStor server.

```
curl -X POST "https://QoreStor.host.com:5233/api/auth/login" -H "accept: application/json" -H "Content-Type: application/json" -d "{ \"name\": \"TestUser\", \"password\": \"TestUserPassword\"}"
```

2. In the request response, find and record the value for **JWT_Token**.
3. For subsequent API requests, ensure that the header contains the value **Authorization: Bearer <token>**. You may also use this token to authorize API requests via the documentation page. To do so,
 - At the top of the API documentation page, click **Authorize**.
 - In the **Value** field, enter the token.
 - Click **Authorize**.

API Documentation

The detailed documentation for the QoreStor API is hosted on your QoreStor server. To view the documentation, enter the URL below into a browser.

https://<QoreStor Server>:5233//api/docs/index.html

i | **NOTE:** In the example above, replace <QoreStor Server> with the FQDN or IP address of your QoreStor server.

The API documentation contains the following:

- An **Authorize** button to enable authentication.
- A list of available API resource categories. Each list is expandable to reveal the resources in each category.

- Each resource listing can be expanded to view the resource description, parameters and responses, and a **Try it Out** button that can be used to execute the API call with entered parameters.

To view and test an API

i | **NOTE:** The example below uses the **GET containers** request. The steps are similar for other requests.

1. Before testing the API, authenticate as described in [Authentication](#).
2. In the resource list, expand **Containers**.
3. Find the Get Containers request (GET/v1/Containers) and click to expand.
4. Click **Try it Out**. Note that the parameters fields are now enabled.

i | **NOTE:** Parameters for Get Containers are optional. Some requests have required parameters.

5. Optionally, enter the parameters as described below:
 - **Storage Group** - The name of the storage group to which the containers belong
 - **Type** - required container type (cloud, link, or tier)
6. Click **Execute**.

Configuring QoreStor settings

In the QoreStor GUI, you can easily view and configure system settings such as, active directory, system date and time, expansion shelf enclosures, licenses, networking, schedules for system operations, SSL certificates, storage groups, and users.

Licensing QoreStor

QoreStor offers a backend capacity licensing model to allow for simple integration with other Quest Data Protection products.

- **Standalone license** - QoreStor is licensed by the amount of backend capacity required. Standalone licenses are available as either **perpetual** licenses (with no expiration), or **term** licenses, which expire after a specified period of time.
- **i** **NOTE:** Term licenses are intended for specific customer use cases, i.e., licensing according to yearly billing cycles. A perpetual license is appropriate for most customers.

QoreStor licenses are additive, meaning that if you purchase a 5TB license now, and a 10TB license in the future, you will have 15TB total capacity.

- **i** **NOTE:** Licenses for QoreStor are specific to the QoreStor server. When installing a license, the System ID for your QoreStor server is required. You can obtain the System ID with the command **system --show | grep "System ID"**

Evaluating QoreStor

QoreStor offers two methods for evaluation:

- **Default installation** - If no license is installed, QoreStor defaults to a no-cost, 1TB capacity installation supported by the QoreStor Community. This option requires no license and does not expire.
 - If a license is applied to a server running in this mode, the free 1TB is **not** added to the purchased license capacity.
 - When installed in Demo mode, the capacity is limited to 100GB.
- **Full capacity trial** - available on the Quest Software Trial site, which provides a 30-day evaluation license for up to 360TB and access to Quest Support. After the evaluation period has expired, the QoreStor server will operate in Manual Intervention mode until a license is applied. To use QoreStor beyond that time frame, you will need to purchase a perpetual standalone license.
 - If installed in Demo mode, the capacity is limited to 100GB
 - If a longer trial period is required, please contact Quest Sales.

If you have purchased a standalone license, you can install it using the **system --license** command, as described in the *QoreStor Command Line Reference Guide*.

i | **NOTE:** When ordering a license, the System ID for your QoreStor server is required. You can obtain the System ID with the command **system --show | grep "System ID"**

Viewing your license configuration

You can view QoreStor license configuration information through the QoreStor GUI or the command line interface.

To view the current license configuration in the GUI

1. In the navigation menu, click **System** to expand the menu, then click **License**.
2. Information about the configured license is displayed.

To view the current license configuration via the command line, use the command

```
system --show [--license] [--verbose]
```

Installing a license

You can add a license to QoreStor through either the QoreStor GUI or the command line interface.

To install a license:

1. In the navigation menu, click **System** to expand the menu, then click **License**.
2. Click **Upload License**.
3. Click **Upload License** and select the license file.
4. Click **Apply**.

i | **NOTE:** You may also install a QoreStor license from the command line interface using the command:

```
system --license [--show] [--verbose] [--validate] [--file <path>] [--add] [--file <path>]
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

Configuring an SSL certificate for your QoreStor system

For additional security, you can replace the self-signed, factory-installed certificate with another SSL certificate, for example, with one that is signed by a third-party CA. Once you have obtained your signed certificate and private key, you can install them by using the QoreStor UI or CLI. Only one certificate can be installed on a QoreStor system at any given point in time. The same certificate will be used for HTTPS access to object containers.

Installing an SSL certificate

To install an SSL certificate, complete the following steps:

1. In the navigation menu, click **Dashboard**.
2. In the System Information pane at the bottom, click **SSL Certificate**.
3. Click **Upload Certificate**.
4. Select the SSL certificate on your system that you want to install.
5. Click **Upload Key** and select your private key.
6. Click **Upload**.

Restoring the default certificate

To restore your certificate to the default, complete the following steps:

1. In the navigation menu, click **System Configuration**. Click **Restore Default**.
2. Click **Apply**.

Configuring Active Directory settings

You can easily join the QoreStor to your Microsoft Active Directory Services (ADS) domain. This topic describes how to configure Active Directory (AD) settings for the QoreStor system, which requires that you direct your QoreStor system to join or leave a domain that contains a Microsoft Active Directory Service (ADS). Instructions are provided below to join an ADS domain or to leave an ADS domain. When you join QoreStor to an ADS domain, this disables the Network Time Protocol (NTP) service and instead uses the domain-based time service.

To configure QoreStor for a domain using ADS, complete the following steps:

1. In the left navigation menu, click **System > Active Directory**.
2. Click **Join Domain**.

3. Enter the following AD logon information:
 - **Domain**—Enter a fully qualified domain name for the ADS; for example, AD12.acme.com. *(This is a required field.)*
 - i** **NOTE:** Supported domain names are limited to 64 characters in length and can only consist of a combination of A-Z, a-z, 0-9, and three special characters: a dash (-), a period (.), and an underscore (_).
 - **Organization**—Enter a valid organizational name that meets the organization name guidelines for the ADS. *(This is an optional field.)*
 - **Username**—Enter a valid user name that meets the user name guidelines for the ADS. *(This is a required field.)*
 - i** **NOTE:** Supported user names are limited to 64 characters in length and can only consist of a combination of A-Z, a-z, 0-9, and three special characters: a dash (-), a period (.), and an underscore (_).
 - **Password**—Enter a valid password that meets the password guidelines for the ADS. *(This is a required field.)*
4. Click **Join**.
5. To leave a domain, find the domain on the Active Directory page and click **Leave Domain**.
 - a. In the Leave Active Directory pane, enter the username and password for the ADS domain.
 - b. Click **Leave**.

Adding a login group to an ADS domain

i **NOTE:** This is an optional configuration, and only necessary if Domain users in a login group are expected to authenticate to the QoreStor UI.

After you configure your QoreStor within the same ADS domain, you must ensure that a login group exists and add it to the domain. Adding a login group is only possible when the QoreStor system is joined to a domain. Also, you must be logged in as a domain user that is part of an enabled login group.

To add a login group in an ADS domain, complete the following steps:

1. On the left navigation menu, click **System > Active Directory**.
2. On the **Active Directory** page, find the domain pane and click **Add Login Group**.
3. In the **Add Login Group** pane, type the name of the login group including the domain name; for example, *Domain\Domain Admins*. If your login group name contains spaces, you must not enclose it in quotation marks. (This differs from the equivalent CLI command.)
4. Click **Add Login Group** to add the login group.
 - i** **NOTE:** Changes made to the login group take effect on the next log in attempt (unlike Windows ADS, no active checking is done on the group).

Removing a login group

To remove a configured ADS login group from the QoreStor system, complete the following steps.

1. On the left navigation menu, click **System > Active Directory**.
2. On the **Active Directory** page, find the domain pane and click **Remove Login Group**.
3. When prompted to confirm, click **OK**.

i | **NOTE:** Changes made to the login group take effect on the next log in attempt (unlike Windows ADS, no active checking is done on the group).

Understanding system operation scheduling

By scheduling system operations, you can optimize your system resources and achieve the best possible QoreStor performance. The most important thing to remember when scheduling critical QoreStor operations is that you want to ensure that you perform each of these operations at a time when it will not overlap or interfere with the running of any of the other key system operations.

You should carefully plan and schedule time periods in which to perform the following critical system operations:

- Data ingests (which are dependent upon your usage of your DMA(s))
- Replication
- System cleaner (space reclamation)

i | **NOTE:** 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.

In QoreStor, the main goal in planning and scheduling operations should be to run the Cleaner and Replication operations at times when they do not overlap or interfere with other important system operations. You want to make sure that by properly scheduling and planning, your system can perform each of these key operations independent of the other.

The best practice is to run these two operations during non-standard business hours, so that they do not conflict with any of your other backup or ingest operations.

i | **NOTE:** By default, QoreStor is configured to run Cleaner operations daily between 1:00 P.M and 6:00 P.M.

The **Cleaner** schedule can be viewed and edited on the **Cleaner** page of the QoreStor GUI (**Local Storage > Cleaner**), or via the QoreStor command line interface, using the **schedule** command:

```
schedule --show --cleaner
```

The **Replication** schedule can be viewed and edited via the **Replications** page of the QoreStor GUI, or via the QoreStor command line interface using the **schedule** command:

```
schedule --show --replication [--name] <name>
```



NOTE: For more information on the **schedule** command, refer to the *QoreStor Command Line Reference Guide*.

Configuring cleaner schedules

Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from the system. The recommended method is to schedule a time when you can run the Cleaner on your QoreStor system with no other planned processes running.

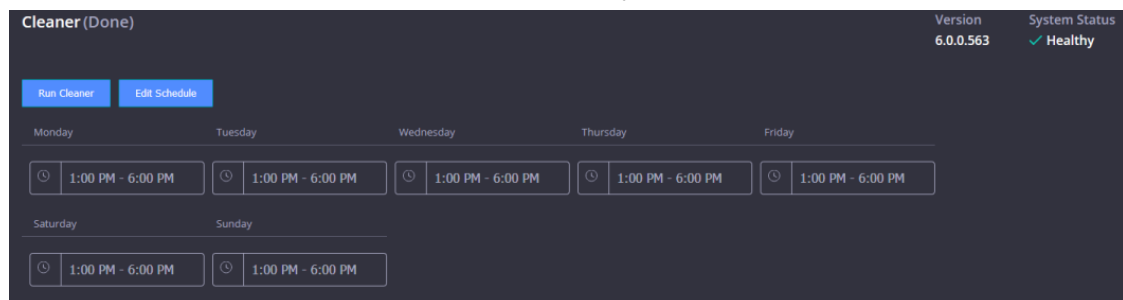
Even if no Cleaner schedule is set, but the system detects that there is disk space that can be reclaimed, the Cleaner process runs. However, the Cleaner will not start until the following conditions are met:

- it detects that there are no active data ingests,
- that two minutes of system idle time have elapsed since the last data file ingest was completed,
- and that the Replication process is not running (the Cleaner process runs as a lower system priority operation than the Replication process).

To schedule cleaner operations on your system using the GUI:

1. On the navigation menu, click **Local Storage** to expand the menu, then click **Cleaner**.
2. On the Cleaner page, click **Edit Schedule**.

The schedule lists a **Start Time** and **End Time** for each day of the week.



3. For each day of the week, click the time selector field. Select the **From** and **To** times to configure a window during which replication can run. Click **Set**.
4. Click **Save Schedule**.
5. Click **Submit**



NOTE: Even if no Cleaner schedule is set, but the system detects that there is disk space that can be reclaimed, the Cleaner process runs. However, the Cleaner will not start until the following conditions are met: it detects that there are no active data ingests, that two minutes of system idle time have elapsed since the last data file ingest was completed, and that the Replication process is not running (the Cleaner process runs as a lower system priority operation than the Replication process).

To schedule cleaner operations on your system using the CLI:

i **NOTE:** The procedure below is a summary. Please refer to the *QoreStor Command Line Reference Guide* for detailed information on accessing the command line interface for your system as well as using the QoreStor commands.

i **NOTE:** Running the Cleaner while ingesting data reduces system performance. Ensure that you schedule the Cleaner to run when backup or replication is not in progress.

1. Access the QoreStor command line interface.
2. Use the QoreStor command line interface (CLI) to create and delete the cleaner schedule. The available commands are:

```
schedule --add --day <Day of the Week> --start_time <HH:MM> --stop_time
<HH:MM> --cleaner
schedule --delete --day <Day of the Week> --cleaner
```

For full details on running the cleaner schedule commands, help is available by entering:

```
schedule --help
```

Viewing cleaner status

On the **Cleaner** page, you can also view graphs showing Cleaner runtime and bytes processed. You may also use the **schedule --show --cleaner** command to view the cleaner status via the QoreStor command line interface.

Viewing cleaner statistics

To view additional detailed cleaner statistics, you can use the QoreStor CLI **stats --cleaner** command to show the following categories of statistics:

- Last Run Files Processed (number of files processed by Cleaner)
- Last Run Bytes Processed (number of bytes processed by Cleaner)
- Last Run Bytes Reclaimed (number of bytes reclaimed by the Cleaner)
- Last Run Start Time (indicates date and time last Cleaner process started)
- Last Run End Time (indicates date and time last Cleaner process ended)
- Last Run Time To Completion(s) (indicates the number of times that Cleaner process has successfully completed)
- Current Run Start Time (indicates date and time current Cleaner process started)
- Current Run Files Processed (number of files processed by current Cleaner process)
- Current Run Bytes Processed (number of bytes processed by current Cleaner process)
- Current Run Bytes Reclaimed (number of bytes reclaimed by the current Cleaner processed)
- Current Run Phase 1 Start Time (indicates date and time for start of current Cleaner process phase 1)
- Current Run Phase 1 Records Processed (lists the number of data records processed in current Cleaner process phase 1)
- Current Run Phase 1 End Time (indicates date and time for end of current Cleaner process phase 1)
- Current Run Phase 2 Start Time (indicates date and time for start of current Cleaner process phase 2)

- Current Run Phase 2 Records Processed (lists the number of data records processed in current Cleaner process phase 2)
- Current Run Phase 2 End Time (indicates date and time for end of current Cleaner process phase 2)
- Current Run Phase 3 Start Time (indicates date and time for start of current Cleaner process phase 3)
- Current Run Phase 3 Records Processed (lists the number of data records processed in current Cleaner process phase 3)
- Current Run Phase 3 End Time (indicates date and time for end of current Cleaner process phase 3)
- Current Run Phase 4 Start Time (indicates date and time for start of current Cleaner process phase 4)
- Current Run Phase 4 Records Processed (lists the number of data records processed in current Cleaner process phase 4)
- Current Run Phase 4 End Time (indicates date and time for end of current Cleaner process phase 4)

For more information about QoreStor CLI commands, see the *QoreStor Command Line Reference Guide*.

Configuring Secure Connect

The sections below contain information necessary for the proper configuration of Secure Connect. The procedures for configuring Secure Connect differ depending on your plug-in version.

- For OST and RDA plug-in version 4.1.0.265 or later
 - [Managing Secure Connect with OST or RDA plug-in 4.1.0.265 or later](#)
- For OST and RDA plug-in versions prior to 4.1.0.265
 - [Enabling Secure Connect for OST and RDA plug-ins prior to 4.1.0.265](#)
 - [Configuring Secure Connect properties](#)
- For Rapid NFS plug-in version 4.0.3310.0 or later
 - [Installing the Rapid NFS plug-in](#)
- For Rapid CIFS plug-in version 4.0.3233.1 or later
 - [Installing the Rapid CIFS plug-in](#)
- [Adding certificates for Secure Connect](#)

Enabling Secure Connect for OST and RDA plug-ins prior to 4.1.0.265

i **IMPORTANT:** The procedure below is for plug-in versions prior to 4.1.0.265. To enable or disable Secure Connect on plug-in version 4.1.0.265, refer to [Managing Secure Connect with OST or RDA plug-in 4.1.0.265 or later](#).

Secure Connect is enabled through the use of environmental variables on the client machine. No configuration is required on the QoreStor server.

To enable Secure Connect on a Windows client

1. On the client server, press **Win+R** to open the **Run** window.
2. Type **sysdm.cpl** and click **OK**.
3. Click the **Advanced** tab, then **Environment Variables**.
4. In the **System Variables** section, click **New**.
5. In the **Variable name** field, enter **SECURE_CONNECT**.
6. In the Variable value field, enter one of the following:
 - **0** - disables Secure Connect
 - **1** - Secure Connect is enabled, but QoreStor will fallback to an unsecured connection if the Secure Connect server is unavailable.
 - **2** - Secure Connect is enabled. Connection will fail if Secure Connect server is unavailable.
7. Click **OK**, then **OK**.

i **IMPORTANT:** After enabling Secure Connect, you will need to change the BypassPorts configuration in the **sc_client.properties** file. Refer to [Configuring Secure Connect properties](#) for information.

i **IMPORTANT:** After enabling Secure Connect, you must restart the DMA application services.

To enable Secure Connect on a Linux client

1. At the command prompt on the client machine, enter the following command

```
echo 'export SECURE_CONNECT=<0|1|2>' >> ~/.bashrc
```

Where:

- **0** - disables Secure Connect
 - **1** - Secure Connect is enabled, but QoreStor will fallback to an unsecured connection if the Secure Connect server is unavailable.
 - **2** - Secure Connect is enabled. Connection will fail if Secure Connect server is unavailable.
2. Log out of the QoreStor system, then log in.

i **IMPORTANT:** After enabling Secure Connect, you will need change the BypassPorts configuration in the **sc_client.properties** file. Refer to [Configuring Secure Connect properties](#) for information.

i **IMPORTANT:** After enabling Secure Connect, you must restart the DMA application services.

Configuring Secure Connect properties

Before using Secure Connect, ensure that the default port configuration is appropriate for your environment. The ports used by Secure Connect are:

- 9443 - this is the listening port. The Secure Connect server listens for connection requests on this port.
- 10011, 11000 and 9920 - These are the standard Secure Connect communication ports.

By default, the Secure Connect ports are bypassed, which will cause Secure Connect to failback to a normal, unsecured connection. Before using Secure Connect, the **BypassPorts** setting must be set to 0 to enable full communication.

Secure Connect properties can be configured through the **sc_client.properties** file located in the client installation directory.

To configure Secure Connect

1. In the client installation directory, open the **sc_client.properties** file with a text editor.
The default installation directory differs depending on the client type and the OS of the client machine. For example,
 - The RDA client on a Windows machine installs to `C:\Program Files\Quest\RDA\dynlib`
 - The NetVault on a Linux server installs to `/usr/netvault/dynlib/sc_client.properties`
2. Find the entry shown below

```
# A list of ports to be excluded from SecureConnect. Example: 9904,9921-9999,10011
#BypassPorts = 0
BypassPorts = 9920,10011,11000
```
3. Do one of the following:
 - Comment out the line **BypassPorts = 9920, 10011, 11000** by adding a # to the front, then remove the # from `BypassPorts = 0`
 - Delete the listed ports (9920, 10011, 11000) and replace with 0.
4. Save the file.

Managing Secure Connect with OST or RDA plug-in 4.1.0.265 or later

Unless manually disabled, Secure Connect is always running on the QoreStor server. Starting with QoreStor plug-in version 4.1.0.265, Secure Connect is enabled by default on the client machine. Review the sections below for the procedures to check Secure Connect status or disable and enable Secure Connect.

The commands below can be executed both on the QoreStor server and the client machines. In both cases, the **sc_manager** command must be executed from the directory that includes the **sc.client.properties** file. By default this is:

- On the QoreStor server `/opt/qorestor/bin`

i | **NOTE:** When configuring Secure Connect on the QoreStor server, the changes made are applicable only for container or optimized replication in which the QoreStor instance is a source.

- For client machines, this is the plug-in installation directory. For example, for NetVault Backup:
 - Linux clients - `/usr/local/ocarda`
 - Windows clients - `C:\Program Files\Quest\RDA\Dynlib`

i | **IMPORTANT:** The procedures below use the **sc_manager** command which must be executed by the **root** account.

Checking Secure Connect status

To check the status of Secure Connect

1. Execute the command **sc_manager status** according to one of the methods below:

- Run **sc_manager** from the directory containing **sc_client.properties**.

```
sc_manager status
```

- Run **sc_manager** from any directory, using the path to the **sc_client.properties**.

```
/opt/qorestor/bin/sc_manager status --property /opt/qorestor/bin/sc_client.properties
```

```
SecureConnect.enabled = true
```

2. The status of Secure Connect will be displayed:

```
SecureConnect.enabled = true
```

Disabling Secure Connect

To disable Secure Connect

1. Execute the **sc_manager disable** command as described below:

- Run **sc_manager** from the directory containing **sc_client.properties**.

```
sc_manager disable
```

- Run **sc_manager** from any directory, using the path to the **sc_client.properties**.

```
/opt/qorestor/bin/sc_manager disable --property /opt/qorestor/bin/sc_client.properties
```

2. The status of Secure Connect will be displayed as confirmation:

```
SecureConnect.enabled = false
```

3. After disabling Secure Connect, a service restart must be performed.

- If you disabled Secure Connect on the QoreStor server, restart the QoreStor services using the commands:

```
/opt/qorestor/bin/ctrlrpc -p 9901 node.stop  
/opt/qorestor/bin/ctrlrpc -p 9901 node.start
```

- If you disabled Secure Connect on the client machine, services of the DMA application on that machine need to be restarted.

Enabling Secure Connect

To enable Secure Connect

1. Execute the `sc_manager enable` command as described below:
 - Run **sc_manager** from the directory containing **sc_client.properties**.

```
sc_manager enable
```
 - Run **sc_manager** from any directory, using the path to the **sc_client.properties**.

```
/opt/qorestor/bin/sc_manager enable --property /opt/qorestor/bin/sc_client.properties
```
2. The status of Secure Connect will be displayed as confirmation:

```
SecureConnect.enabled = true
```
3. After enabling Secure Connect, a service restart must be performed.
 - If you enabled Secure Connect on the QoreStor server, restart the QoreStor services using the commands:

```
/opt/qorestor/bin/ctrlrpc -p 9901 node.stop  
/opt/qorestor/bin/ctrlrpc -p 9901 node.start
```
 - If you enabled Secure Connect on the client machine, services of the DMA application on that machine need to be restarted.

Adding certificates for Secure Connect

The QoreStor Secure Connect feature requires custom certificates on both the client and QoreStor server machine.

i | **NOTE:** The certificates on both the client machine and QoreStor server must be from the same certificate authority.

Adding a Secure Connect certificate - Windows Client

1. Prepare custom certificates chain and install them to the certificate store using the Microsoft Management Console (MMC) **Certificates** snap-in.
 - a. Install the **Root** certificate to **Trusted Root Certification Authorities**.
 - b. If necessary, install the **Intermediate** certificate to **Intermediate Certification Authorities**.
 - c. Install the **Server** certificate to **Personal**.
2. In the client installation directory, open the **sc_client.properties** file with a text editor.

3. Edit the entries below:

- **openssl.client.caConfig** - The path to the file of the trusted root certificate or directory containing the trusted root certificates chain. For specifying directory path, be sure that directory contains certificates in the PEM format and symbolic links to the certificate files, created by the **c_rehash** utility.
- **openssl.client.certificateFile** - The path to the file containing the server's or client's certificate in PEM format.
- **openssl.client.privateKeyFile** - The path to the file containing the private key for the certificate in PEM format.

Example in case there is the chain of 3 certificates (root, intermediate, server), private key and they are located in the same directory as **sc_client.dll**:

- `openssl.client.caConfig = ${application.configDir}`
- `openssl.client.certificateFile = ${application.configDir}server-certificate-name.pem`
- `openssl.client.privateKeyFile = ${application.configDir}privat-key-name.key`

Example in case there is the chain of 2 certificates (root, server), private key and they are located at `C:\certificates`:

- `openssl.client.caConfig = C:\certificates\root-certificate-name.pem`
- `openssl.client.certificateFile = C:\certificates\server-certificate-name.pem`
- `openssl.client.privateKeyFile = C:\certificates\privat-key-name.key`

4. Make **c_rehash** for the certificates:

- a. Download perl from <https://www.activestate.com/ActivePerl>.
- b. Download the perl script **c_rehash**, stored inside OpenSSL (<https://wiki.openssl.org/index.php/Binaries>)
- c. Set the new **openssl** environment variable with the path to openssl.
- d. Run the command prompt.
- e. Use **perl.exe** with **path_to_the_c_rehash** and **path_to_the_cert_dir** arguments (e.g. `perl.exe C:\<path to the c_rehash> C:\<path to the certificates directory>`)

5. When Secure Connect is used with any DMA - restart DMA services.

i | **NOTE:** If certificate validation fails, the connection between client and server will fail back to a normal connection.

Adding a Secure Connect certificate - Linux Client and QoreStor server

1. Prepare custom certificates chain
2. Place the certificate to be trusted (in PEM format) in `/etc/pki/ca-trust/source/anchors/` and run `sudo update-ca-trust` at the prompt.
If the certificate is in OpenSSL's extended BEGIN TRUSTED CERTIFICATE format, place it in `/etc/pki/ca-trust/source` and run `sudo update-ca-trust`.

3. Make **c_rehash** for the certificates:
 - a. Install the **openssl-perl** package.
 - b. Run `c_rehash <path-to-the-folder-with-certificates>`.
4. In the client installation directory, open the **sc_client.properties** file with a text editor.
5. Edit the entries below:
 - a. **openssl.client.caConfig** - The path to the file of the trusted root certificate or directory containing the trusted root certificates chain. For specifying directory path, be sure that directory contains certificates in the PEM format and symbolic links to the certificate files, created by the `c_rehash` utility.
 - b. **openssl.client.certificateFile** - The path to the file containing the server's or client's certificate in PEM format.
 - c. **openssl.client.privateKeyFile** - The path to the file containing the private key for the certificate in PEM format.

Example in case there is the chain of 3 certificates (root, intermediate, server), private key and they are located in the same directory with `sc_client.so`, server side:

 - `openssl.server.caConfig = ${application.configDir}`
 - `openssl.server.certificateFile = ${application.configDir}server-certificate-name.pem`
 - `openssl.server.privateKeyFile = ${application.configDir}privat-key-name.key`

Example in case there is the chain of 2 certificates (root, server), private key and they are located at `/usr/certificates` on the client machine:

 - `openssl.client.caConfig = /usr/certificates/root-certificate-name.pem`
 - `openssl.client.certificateFile = /usr/certificates/server-certificate-name.pem`
 - `openssl.client.privateKeyFile = /usr/certificates/privat-key-name.key`
6. When Secure Connect is used with any DMA - restart DMA services.

i | **NOTE:** If certificate validation fails, the connection between client and server will fail back to a normal connection.

Enabling MultiConnect

Before using MultiConnect, ensure that the default port configuration is appropriate for your environment. The port used by MultiConnect is:

- 11000 - This is the standard MultiConnect communication port for backup.
- 9920 - This is the standard MultiConnect communication port for managed replication.

To enable Secure Connect on a Windows client

1. On the client server, press **Win+R** to open the **Run** window.
2. Type **sysdm.cpl** and click **OK**.

3. Click the **Advanced** tab, then **Environment Variables**.
4. In the **System Variables** section, click **New**.
5. In the **Variable name** field, enter **REMOTE_CLNT_MAX_CONNS**.
6. In the **Variable value** field, enter one of the following:
 - **4** - establishes 4 connections.
 - **8** - establishes 8 connections.
 - **16** - establishes 16 connections.
7. Click **OK**, then **OK**.
8. Restart the DMA services for the change to take effect.

To enable MultiConnect on a Linux client

1. At the command prompt on the client machine, enter the following command

```
echo 'export REMOTE_CLNT_MAX_CONNS=<4|8|16>' >> /etc/profile
```

Where:

- **4** - establishes 4 connections.
 - **8** - establishes 8 connections.
 - **16** - establishes 16 connections.
2. Restart the DMA services for the change to take effect.

To enable MultiConnect between QoreStor servers

1. At the command prompt on the source machine, enter the following command

```
echo 'export REPL_CLNT_MAX_CONNS=16' >> /etc/oca/oca.cfg
```

2. Restart the **ocards** service for the change to take effect.

Configuring and using Rapid NFS and Rapid CIFS

Rapid NFS and Rapid CIFS enable write operation acceleration on clients that use NFS and CIFS file system protocols. Similar to OST and RDS, these accelerators allow for better coordination and integration between QoreStor backup, restore, and optimized duplication operations with Data Management Applications (DMAs) such as CommVault, EMC Networker, and Tivoli Storage Manager. For the current list of supported DMAs, see the *QoreStor Interoperability Guide*.

Rapid NFS is a new client file system type that ensures that only unique data is written to QoreStor. It uses user space components and file system in user space (FUSE) to accomplish this. Metadata operations such as file creates and permission changes go through the standard NFS protocol, whereas write operations go through Rapid NFS.

Rapid CIFS is a Windows-certified filter driver that also ensures that only unique data is written to QoreStor. All chunking and hash computations are done at the client level.



NOTE: The supported DMAs listed in the QoreStor *Interoperability Guide* are the DMAs that have been **tested and qualified** with Rapid NFS and Rapid CIFS. You can use Rapid NFS and Rapid CIFS with other DMAs, but those products have not been tested and qualified with Rapid NFS or Rapid CIFS.

Rapid NFS and Rapid CIFS benefits

When Rapid NFS and Rapid CIFS are used with QoreStor they offer the following benefits:

- Reduce network utilization and DMA backup time
 - Chunk data and perform hash computation on the client; transfer chunked hash files on the back-end
 - Reduce the amount of data that must be written across the wire
- Improve performance
- Support DMAs such as CommVault, EMC Networker, and Tivoli Storage Manager. For the current list of supported DMAs, see the *QoreStor Interoperability Guide*.
- Compatible with existing NFS and CIFS clients — just need to install a plug-in (driver) on the client
 - Can use Rapid NFS and Rapid CIFS to accelerate I/O operations on any client — including a client that uses home-grown backup scripts
 - Can service multiple and concurrent media server backups

Best practices: Rapid NFS

This topic introduces some recommended best practices for using Rapid NFS operations with QoreStor.

- Containers must be of type NFS/CIFS

RDA containers cannot use Rapid NFS. If you have existing NFS/CIFS containers, you do not need to create new containers to use Rapid NFS; you can install the plug-in (driver) to existing clients.
- The Rapid NFS plug-in (driver) must be installed on client systems

After the plug-in is installed, write operations will go through Rapid NFS while metadata operations such as file creates and permission changes will go through the standard NFS protocol. Rapid NFS can be disabled by uninstalling the plug-in.
- Markers must be set on the client, not in the QoreStor GUI
- If you are using a DMA that supports a marker, should explicitly set it. Your containers should have the marker type of None until you set the marker using the Mount command on the client (after installing the Rapid NFS plug-in).

- For existing containers, re-set the marker by doing the following:

For example, if you wanted to set the CommVault marker (cv):

```
mount -t rdnfs 10.222.322.190:/containers/backup /mnt/backup -o
marker=cv
```

Mount command usage:

```
rdnfs [nfs mount point] [roach mount point] -o marker=[marker]
```

where:

nfs mount point = Already mounted nfs mountpoint

roach mount point = A new mount point

marker = appassure, arcserve, auto, cv, dump, hdm, hdpd, nw, or tsm

- Your QoreStor system must meet the minimum configuration
Rapid NFS is available on a QoreStor system and a client with a minimum of 4 CPU cores running at a minimum of 4 GHz cumulative processing power and 2 GB memory. Kernels must be 2.6.14 or later. For a list of supported operating systems, see the *QoreStor Interoperability Guide*. If you update your operating system, you must update your Rapid NFS plug-in as well. Updates are available on the Quest Support site.
- Rapid NFS is stateful
If the QoreStor system goes down, the connection will terminate. DMAs will restart from the last checkpoint.
- Rapid NFS and passthrough mode
If Rapid NFS mode fails for any reason, QoreStor falls back to regular NFS mode automatically. For details, see [Monitoring Performance](#).
- Rapid NFS performance considerations
When using Rapid NFS on your client, Quest recommends that you do not run other protocols to the QoreStor system in parallel, as this will adversely affect your overall performance.
- Rapid NFS acceleration constraints
 - Rapid NFS does not support:
 - Direct I/O memory
 - Mapped files
 - File path size greater than 4096 characters
 - File write locks across clients

i **NOTE:** If the client and server do not have the same times, the times seen will not match typical NFS behavior due to the nature of file system in user space (FUSE).

Best practices: Rapid CIFS

This topic introduces some recommended best practices for using Rapid CIFS operations with QoreStor.

- Containers must be of type NFS/CIFS
 - RDA containers cannot use Rapid CIFS. If you have existing NFS/CIFS containers, you do not need to create new containers to use Rapid CIFS; you can install the plug-in (driver) to existing clients.

- The Rapid CIFS plug-in (driver) must be installed on client systems
After the plug-in is installed, write operations will go through Rapid CIFS while metadata operations such as file creates and permission changes will go through the standard CIFS protocol. Rapid CIFS can be disabled by uninstalling the plug-in.
- Your QoreStor system must meet the minimum configuration
Rapid CIFS is available with a QoreStor system and a client with a minimum of 4 CPU cores running at a minimum of 4 GHz cumulative processing power and 2 GB memory. For a list of supported operating systems, see the *QoreStor Interoperability Guide*.
If you update your operating system, you must update your Rapid CIFS plug-in as well. Updates are available on the Quest Support site.
- Rapid CIFS is stateful
If the QoreStor system goes down, the connection will terminate. DMAs will restart from the last checkpoint.
- Rapid CIFS and passthrough mode
If Rapid CIFS mode fails for any reason, the QoreStor system falls back to regular CIFS mode automatically.
- Rapid CIFS acceleration constraints
Rapid CIFS does not support:
 - NAS functionality
 - Optlocks (but supported if a single client is writing)
 - Byte-range locks
 - Optimization of very small files (less than 10 MB). File size can be adjusted using configuration settings.
 - FILE_NO_IMMEDIATE_BUFFERING and FILEWRITE_THROUGH operations (sent via CIFS only).
 - File path size greater than 4096 characters

Installing the Rapid NFS plug-in

The QoreStor NFS plug-in must be installed on to the media server type you choose (for supported operating systems and DMAs, see the *QoreStor Interoperability Guide*). The plug-in software enables integration between QoreStor data storage operations and the supported data management applications (DMAs). Before you install, make sure you adhere to the Best Practices covered in another topic in this chapter.

The plug-in must be installed on the designated Linux-based media server in the following directory, **/usr/opensv/lib/**. The plug-in is installed using a self-extracting installer that installs the Rapid NFS plug-in and all of its related components. The installer supports the following modes, with the default being Help (-h):

- Help (-h)
- Install (-install)
- Upgrade (-upgrade)
- Uninstall (-uninstall)
- Force (-force)

```
$> ./QuestRapidNFS-xxxxx-xxxxx-x86_64.bin -help
Quest plug-in installer/uninstaller
usage: QuestRapidNFS-xxxxx-xxxxx-x86_64.bin [ -h ] [ -install ] [ -uninstall ]
-h                : Displays help
```



```
-install      : Installs the plug-in
-upgrade     : Upgrades the plug-in
-uninstall   : Uninstalls the plug-in
-force       : Forces the installation of the plug-in
```

Downloading the Rapid NFS Plug-in

You can download the plug-in installer from the Quest website:

- Go to support.quest.com/qorestor, select your specific QoreStor version, and then navigate to Software Downloads.
- Locate the Rapid NFS plug-in and download it to your system.

Enabling Secure Connect

Starting with the Rapid NFS plug-in version 4.0.3.3, the plug-in installation script includes the option to install and enable Secure Connect. Secure Connect is comprised of a set of client and server components that create a resilient and secure communication channel for use by WAN-connected clients. The server components are installed and enabled by default during the installation of the QoreStor server.

If you have WAN-connected Rapid NFS clients and choose to install Secure Connect, you can do so by adding the **sc** parameter to the mount command, as described in step 7 in the installation procedure.

Installing the plug-in

To install the Rapid NFS plug-in, follow the steps below.

i | **NOTE:** The plug-in needs to be installed on client systems to support client-side deduplication.

1. Download `QuestRapidNFS-4.0.3317.0-x86_64.bin.gz` from the website.
2. Unzip the package.

```
unzip QuestRapidNFS-4.0.3317.0-x86_64.bin.gz
```

3. Assign execute bit to change the permission of the binary package:

```
chmod +x QuestRapidNFS-4.0.3317.0-x86_64.bin
```

4. Install the Rapid NFS package. Before installing, remove the stale NFS entry.

```
QuestRapidNFS-4.0.3317.0-x86_64.bin -install
```

5. Load the file system in user space (FUSE) module, if not already loaded:

```
modprobe fuse
```

6. Create a directory on the client. For example:

```
mkdir /mnt/backup
```

7. Mount Rapid NFS as a file system type using the mount command. For example:

```
mount -t rdnfs 10.0.0.1:/containers/backup/mnt/backup
```

To enable Secure Connect, mount Rapid NFS using the **sc** flag, as shown below:

```
mount -t rdnfs 10.0.0.1:/containers/backup/mnt/backup sc,user=backup_
user,password=<backup_user password>
```

If you are using a DMA that supports a marker, set the marker by using **-o** in the mount command. For example, if you wanted to set the CommVault marker (**cv**):

```
mount -t rdnfs 10.0.0.1:/containers/backup /mnt/backup -o marker=cv
```

i | **NOTE:** If you want to do a mount on AIX, you must set the `nfs_use_reserved_ports` and `portcheck` parameters first. The parameters cannot be set to 0. For example: `root@aixhost1 / # nfso -po portcheck=1 root@aixhost1 / # nfso -po nfs_use_reserved_ports=1`

To ensure that the plug-in is running successfully, check the log file at: `tail -f /var/log/oca/rdnfs.log`.

Installing the Rapid CIFS plug-in

The Rapid CIFS plug-in must be installed on to the media server type you choose (for supported operating systems and DMAs, see the *QoreStor Interoperability Guide*). The plug-in software enables integration between QoreStor data storage operations and the supported data management applications (DMAs). Before you install, make sure you adhere to the Best Practices covered in another topic in this chapter.

Downloading the Rapid CIFS Plug-in

You can download the plug-in installer from the Quest website as follows

- Go to support.quest.com/qorestor, select your specific QoreStor version, and then navigate to Software Downloads.
- Locate the Rapid CIFS plug-in and download it to your system.

After it is downloaded, follow the steps below to run the plug-in installer to install the plug-in on your designated media server.

Enabling Secure Connect

Secure Connect is comprised of a set of client and server components that create a resilient and secure communication channel for use by WAN-connected clients. The server components are installed and enabled by default during the installation of the QoreStor server. Starting with the Rapid CIFS plug-in version 4.0.3.2, the plug-in installer includes the option to install and enable Secure Connect.

Installing the plug-in

To install the Rapid CIFS plug-in, follow the steps below.

i | **NOTE:** The plug-in needs to be installed on client systems to support client-side deduplication.

1. On the media server, map a network share to your CIFS-enabled container.
2. Download the plug-in installer from the website, as detailed previously.
3. Open a command prompt with the "Run as Administrator" option selected. To do this using the Windows Start menu, click **Start** → **All Programs** → **Accessories**. Right-click **Command Prompt** and select **Run as Administrator**.
This gives all the required privileges to install/copy the driver files to the Windows drivers folder.
4. Run `QuestRapidCIFS-4.0.3317.0.exe`.
5. When prompted, select **Install a Secure Connection** to install Secure Connect.
Secure Connect ensures backups to QoreStor are completed in spite of slow or unreliable WAN connections. When selecting this option, you will be prompted for additional configuration information required to make Secure Connect function correctly.
6. At the **Configure Secure Connect** page, complete the dialog using the IP or fully qualified domain name (FQDN) of the QoreStor server and appropriate credentials.
The user account used must have the CIFS role assigned.

i **NOTE:** The **Configure Secure Connect** operation is not supported for CIFS containers on DR Series appliances. DR Series appliances do not contain the required Secure Connect server component. This operation is available only for QoreStor instances. For CIFS containers on DR Series appliances, connect using the Rapid CIFS plug-in and the DR Series host name.

i **NOTE:** The value entered in the **Display Name** field must **not** match the hostname of the QoreStor server.

To ensure that the plug-in is running successfully, check the Windows Event log file.

Monitoring performance

This procedure describes how to monitor performance by viewing Rapid NFS and Rapid CIFS usage graphs. Before you view usage graphs, make sure that the appropriate accelerator is active by viewing the Container Statistics in the QoreStor GUI.

To monitor Rapid NFS and Rapid CIFS performance:

1. In the QoreStor GUI, click **Dashboard**.
2. In the Actions menu in the upper right corner of the page, click **Detailed Graphs**.
3. Select a time range (if needed) and click **Apply**.
4. Click the **Protocols** tab.
Under **NFS Usage** and **CIFS Usage**, there is an **XWrite** checkbox. This checkbox represents the accelerator activity.
5. In the desired usage graph pane, select the **XWrite** checkbox to view the accelerator performance over time.

If you have Rapid NFS enabled, you can use the command line to view statistics, throughput, and the plug-in version by running the `ru` utility on the client, as follows:

```
ru --mpt=[rdnfs mount point] | --pid=[process ID of rdnfs] --show=[name|version|parameters|stats|performance]
```

If you have Rapid CIFS enabled, you can use the command line to view aggregate statistics (even while a backup job is running) using the following command:

```
\Program Files\Quest\Rapid CIFS\rdcifstl.exe stats -s
```

Uninstalling the Rapid NFS plug-in

Use the following procedure to remove the Rapid NFS plug-in from a Linux-based media server. After you uninstall the plug-in, Rapid NFS will be disabled and “inactive” will be shown next to **NFS Write Accelerator** on the **NFS Connection Configuration** pane on the **Container Statistics** page.

i | **NOTE:** You should retain the Rapid NFS plug-in installer on the media server in case you need to use it to reinstall the plug-in. It is usually located in `/opt/quest/QoreStor/RDNFS/scripts`.

To uninstall the Rapid NFS plug-in on Linux:

1. Stop the Data Management Application (DMA) backup service before using the `-uninstall` option. The Rapid NFS plug-in installer returns an error if the DMA service is running when attempting to uninstall the plug-in.
2. Run the Rapid NFS plug-in installer (usually located in `/opt/Quest/QoreStor/RDNFS/scripts`) with the `-uninstall` option, which uninstalls the plug-in, using the following command:

```
$> ./QuestRapidNFS-xxxxx-x86_64.bin -uninstall
```

i | **NOTE:** You must stop the DMA service before uninstalling the Rapid NFS plug-in (you are also required to use the Rapid NFS plug-in installer to uninstall the plug-in).

3. Check that the plug-in is uninstalled by viewing the usage graph in the GUI; it should not indicate any **XWrite** activity.

Uninstalling the Rapid CIFS plug-in

Use the following standard Microsoft Windows uninstall process to remove the Rapid CIFS plug-in from a Windows-based media server. After you uninstall the plug-in, Rapid CIFS will be disabled and “inactive” will be shown next to CIFS Write Accelerator on the CIFS Connection Configuration pane on the Container Statistics page.

Alternatively, if you want to disable (but not uninstall) the plug-in, you can run the following Rapid CIFS utility command. The utility is located in `C:\Program Files\Quest\Rapid CIFS`.

```
rdcifstl.exe driver -d
```

i | **NOTE:** Replace this text with a description of a feature that is noteworthy.

To uninstall the Rapid CIFS plug-in on Windows:

1. Click **Start**, and click **Control Panel**.
2. Under **Programs and Features**, click **Uninstall a program**.
3. Locate the Rapid CIFS plug-in in the listed of installed programs, right-click, and select **Uninstall**.
4. Click **Yes** to uninstall the Rapid CIFS plug-in.

Configuring and using VTL

This topic introduces Virtual Tape Libraries (VTLs) and related concepts and tasks. Refer to the subsequent topics and procedures in this section for more information.

Understanding VTL

A Virtual Tape Library (VTL) is an emulation of a physical tape library on a disk-based deduplication and compression system such as QoreStor. The tape library is exposed to a Data Management Application (DMA) as if it is a physical library with tape drives and cartridges, which the application uses for backup. Because a VTL completely emulates a standard library, the introduction of virtual tape is seamless and transparent to existing tape backup/recovery applications. The management of the library, including the drives and tapes, is done by the DMA using SCSI commands. For details on the applications supported, see the *QoreStor Interoperability Guide*.

Terminology

This topic introduces and briefly defines some basic VTL terminology used throughout the QoreStor documentation.

Term	Description
Library	A library is an emulation of a physical tape library and shares the same characteristics such as media changer, tape drives, and slots (cartridge slots).
Tape Drive	A Tape drive is a logical unit which is part of the emulated library. The media or cartridge is loaded in the Tape drives to be accessed by the Data Management application.
Tapes/Media/Cartridges	Tapes are represented as files and are units within the VTL where data is actually written. Tapes are loaded into a Tape Drive before being accessed.
Slots	Tapes are parked in Slots before they are retrieved by the data management application for access.

Supported virtual tape library access protocols

QoreStor supports the following virtual tape library (VTL) tape access protocols.

- Network Data Management Protocol (NDMP)
- Internet Small Computer System Interface (iSCSI)

NDMP

The Network Data Management protocol (NDMP) is used to control data backup and recovery between primary and secondary storage in a network environment. For example, a NAS server (Filer) can talk to a tape drive for the purposes of a backup.

You can use the protocol with a centralized data management application (DMA) to back up data on file servers running on different platforms to tape drives or tape libraries located elsewhere within the network. The protocol separates the data path from the control path and minimizes demands on network resources. With NDMP, a

network file server can communicate directly to a network-attached tape drive or virtual tape library (VTL) for backup or recovery.

The QoreStor VTL container type is designed to work seamlessly with the NDMP protocol.

iSCSI

iSCSI or **Internet Small Computer System Interface** is an Internet Protocol (IP)-based storage networking standard for storage subsystems. It is a carrier protocol for SCSI. SCSI commands are sent over IP networks by using iSCSI. It also facilitates data transfers over intranets and to manage storage over long distances. iSCSI can be used to transmit data over LANs or WANs.

In iSCSI, clients are called *initiators* and SCSI storage devices are *targets*. The protocol allows an *initiator* to send SCSI commands (*CDBs*) to the *targets* on remote servers. It is a storage area network (SAN) protocol, allowing organizations to consolidate storage into data center storage arrays while providing hosts (such as database and web servers) with the illusion of locally attached disks. Unlike traditional Fibre Channel, which requires different cabling, iSCSI can be run over long distances using existing network infrastructure.

iSCSI is a low-cost alternative to Fibre Channel, which requires dedicated infrastructure except in FCoE (Fibre Channel over Ethernet). Note that the performance of an iSCSI SAN deployment can be degraded if not operated on a dedicated network or subnet

The VTL container type is designed to work seamlessly with the iSCSI protocol. For details, see [Creating a VTL type container](#).

VTL and QoreStor specifications

This topic describes key specifications of VTL support in QoreStor.

- **Supported VTL Types** — QoreStor supports two types of virtual tape libraries.
 - Standard emulation of StorageTek L700 library
 - Quest OEM version of the StorageTek L700 library

i **NOTE:** The Quest type VTL is supported only with VeritasBackup Exec and Netbackup data management applications (DMAs).

i **NOTE:** Refer to the documentation for your specific QoreStor version, which includes DMA best practices whitepapers and the latest *QoreStor Interoperability Guide*, for a complete list of the supported DMAs. Visit the following site and select your specific QoreStor to download documentation: support.quest.com/qorestor.

- **Number of Tape Drives** — Each tape library contains 10 tape drives of the type IBM-LTO-4 ('ULT3580-TD4')

- **Tapes or Media Sizes**— Each library initially is created with 60 slots housing 60 tape media of the default size of 800GiB, which is the equivalent of an LTO4 tape.

You can add additional tapes to the library as needed by editing the container in the GUI or by using the following CLI command:

```
vtl --update_carts --name <name> --add --no_of_tapes <number>
```

i **NOTE:** For more information about using the CLI, see the *QoreStor Command Line Interface Reference Guide*.

A library can only contain tapes of the same size. For example, if the library is originally created with 10 tapes of size 10GB, additional tapes of size 10GB can only be added.

The table below details the tape size and capacity configurations supported by each QoreStor installation type.

Table 9: Supported tape configurations per installation mode

Tape	Large installation		Standard installation		Cloud-Optimized installation	
	Size	Max number of slots supported	Size	Max number of slots supported	Size	Max number of slots supported
LTO-4	800GB	2000	800GB	1000	800GB	500
LTO-4	400GB	4000	400GB	2000	400GB	1000
LTO-4	200GB	8000	200GB	4000	200GB	2000
LTO-4	100GB	10000	100GB	5000	100GB	2500
LTO-4	50GB	10000	50GB	5000	50GB	2500
LTO-4	10GB	10000	10GB	5000	10GB	2500

- **Maximum Number of DMAs or Initiators Supported** — A tape library can be accessed by one DMA or iSCSI initiator at a time.

Guidelines for configuring VTL

The overall steps and recommended guidelines for using and configuring a virtual tape library (VLT) with QoreStor are described below.

Plan your Environment

Determine the following before creating a container of type VTL.

- Identify the Data Management Application (DMA) that you will be using to back up data. Refer to the *QoreStor Interoperability Guide* for a complete list of the supported DMAs.
- For the NDMP protocol, determine the filer that will be backed up using NDMP Refer to the *QoreStor Interoperability Guide* for a list of the supported Filers and Operating systems.
- For the iSCSI protocol, determine the iSCSI initiator's properties – This is the DMA IP, hostname or IQN of

the software initiator on the operating system.

- Assess the estimated size of full and incremental backups and retention periods.

i **NOTE:** The size of the full and incremental backups will determine the tape capacity size that you set. You should use a larger tape size for full backups and a smaller size for incremental backups that have smaller retention periods. Note that faster expiration periods of incremental backups residing on smaller tapes results in the release of space back to the system for future backups.

Create Containers of Type VTL

- Determine the VTL library type (NDMP or iSCSI) that you should be using as per the suggested type in the best practices guide of your preferred DMA.
Refer to the QoreStor documentation, which includes DMA best practices whitepapers for your specific QoreStor version at support.quest.com/qorestor.
- When creating the container in the GUI or by using the CLI, you will need to set the connection type of either NDMP or iSCSI. You need to provide either the DMA IP/hostname for NDMP or the IP/hostname or IQN for an iSCSI connection type.
Refer to the topics, [Creating Storage Containers](#) and [Creating a VTL Type Container](#), for detailed instructions about creating containers. Refer to the *QoreStor Command Line Interface Guide* for details about the CLI commands for creating containers.

Authentication/User Management Considerations

- You can use the following commands to view user information for the iSCSI user: `iscsi_user`, and NDMP user: `ndmp_user`.
 - `iscsi --show`
 - `ndmp --show`

Refer to the *QoreStor Command Line Reference Guide* for more details about using these commands.

- For iSCSI, you need to set the system-wide CHAP account for the QoreStor system. You can add this user on the Users page in the QoreStor GUI. See the topic, [Adding a User](#), for instructions for adding an iSCSI user and password.
- For NDMP, you can set the password for `ndmp_user` by using the Users page in the QoreStor GUI. These credentials are needed for configuring the NDMP-VTL in the DMA. See the topic, [Adding a User](#), for instructions for adding an NDMP user and password.

Verify the Tape Library Creation

You can easily check that the library has been created and is available for use by using the following commands.

- Check the container properties by executing the following command:
`container --show -verbose`
 - Upon initial addition of the connection, the NDMP/iSCSI connection status shows as 'Added'. At this time, the library is not officially created.
 - After a few minutes, the NDMP/iSCSI connection status changes to "Available". This status indicates that the library is online, and the tape drives and media is available for usage.
- To check the status of the virtual tape library and all the tapes in the library, you can execute one of the following commands:
 - `vtl -show`
 - `vtl --show --name <container_name> --verbose`

Configure the Library in the DMA

See the QoreStor documentation, which includes DMA best practices whitepapers for your specific QoreStor version at:

support.quest.com/qorestor.

Configuring and Using Encryption at Rest

This chapter introduces the concept of Encryption at Rest as used by QoreStor as well as related concepts and tasks.

i | **NOTE:** Due to export regulations, the encryption at rest feature is not available in certain markets, and, therefore, may not be available in your locale.

Understanding Encryption at Rest

Data that resides in QoreStor can be encrypted. When encryption is enabled, QoreStor uses the Industry standard FIPS 140-2 compliant 256-bit Advanced Encryption Standard (AES) encryption algorithm for encrypting and decrypting user data. The content encryption key is managed by the key manager, which operates in either a **Static** mode or an **Internal** mode. In **Static** mode, a global, fixed key is used to encrypt all data. In **internal** mode, key lifecycle management is performed in which the keys are periodically rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7 days. This rotation period is user-configurable and can be specified in days.

A user-defined passphrase is used to generate a pass phrase key, which is used to encrypt the content encryption keys. It is mandatory to define a passphrase to enable encryption. The system supports up to a limit of 1023 different content encryption keys. All streams of a data-store are encrypted or re-encrypted with the same content encryption key. QoreStor statistics report the amount of data encrypted and decrypted bytes consistently.

Encryption at Rest Terminology

This topic introduces and briefly defines some basic encryption at rest terminology used in QoreStor documentation.

Term	Description
Passphrase	A passphrase is a sequence of words or other text used to control access to data, similar to a password in usage, but is generally longer for added security. The QoreStor passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.
Content encryption key	The key used to encrypt the data. The content encryption key is managed by the key manager, which operates in either a static mode or an internal mode. The system supports up to a limit of 1023 different content encryption keys.

Term	Description
Key management mode	The mode of key lifecycle management as either static or internal.
Static mode	A global mode of key management in which a fixed key is used to encrypt all data.
Internal mode	A mode of key lifecycle management in which the keys are periodically generated and rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7 days. This rotation period is user-configurable and can be specified in days.

Encryption at Rest and QoreStor Considerations

This topic describes key features and considerations of using Encryption at Rest in QoreStor.

- **Key Management** — In internal mode there is a maximum limit of 1023 keys. By default when encryption is enabled on the system, the key rotation period is set to 30 days. Users can later change the key rotation period from 7 days to 70 years, while configuring internal mode of encryption.
- **Performance Impacts** — Encryption should have minimal to zero impact on both backup and restore workflows. It should also have no impact on the replication workflows.
- **Replication** — Encryption must be enabled on both the source and target QoreStor systems to store encrypted data on the systems. This means that encrypted data on the source does not automatically imply that when it is replicated to the target it will be encrypted unless encryption is explicitly turned 'ON' on the target QoreStor system.
- **Security Considerations for Passphrase and Key Management** —
 - A passphrase is very important part of the encryption process on the QoreStor system as the passphrase is used to encrypt the content encryption key or keys. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.
 - The administrator should closely consider security requirements to drive the decision for selecting the mode of key management for the QoreStor system.
 - The Internal mode is more secure than the Static mode since the keys are periodically changed. Key rotation can be set to 7 days minimum.
 - Key modes can be changed at any time during the lifetime of the QoreStor system; however, changing the key mode is a significant operation to undertake as all encrypted data must be re-encrypted.
 - Content encryption keys are stored in their encrypted form in a primary keystore, which is maintained on the same enclosure as the data-stores. For redundancy purposes, a backup copy of the primary keystore is stored on the system in the root partition, separate from the data-store partitions.

Understanding the encryption process

The overall steps for how Encryption at Rest is enabled and used in QoreStor are described below.

1. **Enabling encryption.**

Encryption is disabled by default on QoreStor. An administrator can enable encryption by using the GUI or CLI.

Encryption is set at the storage group level.

2. **Setting a passphrase and setting the mode.**

When defining encryption for a storage group, a passphrase is set. This passphrase is used to encrypt the content encryption keys, which adds a second layer of security to the key management. At this time, the mode is also set. The default key management mode is “internal” mode, in which key rotation happens periodically as specified by the set key rotation period.

3. **Encryption process.**

After encryption is enabled, the data in the storage group that gets backed up is encrypted and is kept encrypted until it is expired and cleaned by the system cleaner. Note that the encryption process is irreversible.

4. **Encryption of pre-existing data.**

Any pre-existing data will also be encrypted using the currently set mode of key management. This encryption occurs as part of the system cleaner process. Encryption is scheduled as the last action item in the cleaner workflow. You must launch the cleaner manually using the maintenance command to reclaim space. It then encrypts all pre-existing unencrypted data. The cleaner can also be scheduled as per the existing pre-defined cleaner schedule.

i **NOTE:** The cleaner can take some time to start the encryption process if the system is nearing full system capacity. Encryption starts only after the cleaner processes data slated for cleaning and the related logs. This ensures that space reclamation is prioritized when free space is low and also ensures that data stores are not redundantly encrypted.

Refer to the QoreStor *Command Line Interface Reference Guide* for information about the CLI commands used for encryption.

Configuring email alert settings

Using the QoreStor CLI, you can configure email notifications that are sent when a QoreStor Alert occurs. The email alert service is disabled by default, and must be properly configured before the service can be enabled.

To begin using email alerts, perform the actions below :

- Configure the email alerts service using the command **email_alerts --configure**.
 - To configure email alerts, you will need to have:
 - The SMTP Relay FQDN or IP address
 - The sender's name
 - A list of email recipients' email addresses.
 - [Optional] a list of email addresses to be CC'ed
 - [Optional] a list of email addresses to be BCC'ed
- Enable the email alerts service using the command **email_alerts --enable**.

i | **NOTE:** Refer to the *QoreStor Command Line Reference Guide* for more information on using the CLI.

Managing containers

In QoreStor, data is stored in containers, which are stored in storage groups. Some containers function like a shared file system. These types of containers can be assigned a specific connection type, for example, NFS/CIFS or RDA (including both OST and RDS clients). These containers are then accessed via NFS, CIFS, and RDA protocols.


In QoreStor you can manage your storage groups and data containers, including viewing storage groups and containers, creating new storage groups and containers, modifying or deleting them, moving data into containers, and viewing current statistics. Management for containers can be done either through the GUI or the command line.

i **NOTE:** If only the DefaultGroup storage group exists on your system, all containers you create are automatically added to that group. You can create custom storage groups, and then when you create a container, you can specify that it be added to the custom storage group. For more information about storage groups, see the topic, “Managing Storage Groups.”

Viewing containers

You can easily view a list of containers in your QoreStor instance on the Storage Containers page, or by using the **container** command in the QoreStor CLI.

Viewing containers in the GUI

1. In the navigation menu, click **Containers**. The **Containers** page is displayed.
2. You can view the following columns of information about the containers.
 - **Container**—The name of the container.
 - **Path**—The path for the container.
 - **Marker**—The marker type that supports your Data Management Application (DMA).
 - **Connection**—The connection type/access protocol for the container:
 - NFS
 - CIFS
 - RDA
 - OST
 - **Cloud Tiering Policy**—The status of whether the container is connected to a cloud container. If a cloud container link is not configured, **Enable Cloud Tiering Policy** will be displayed.
 - **Archive Tiering Policy**—The status of whether the container is connected to an archive tier. If an archive tier link is not configured, **Enable Archive Tiering Policy** will be displayed.
 - **Ellipsis icon** —Provides additional options as listed below:
 - Details
 - Enable Cloud Tiering Policy
 - Enable Archive Tiering Policy
 - Edit
 - Delete

Viewing containers via the CLI

To view the list of containers, follow these steps.

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. To view the containers on this QoreStor instance, use the command


```
container --show [--name <name>] [--verbose]
```

Refer to the QoreStor Command Line Reference Guide for more information.

Viewing container statistics

In the QoreStor GUI, you can view statistics about a selected container. All statistics displayed represent specific information about the backup data, throughput, replication, marker type, and connection type for the selected container. The displayed statistics will vary depending upon the connection type used by the specified container.

To display container statistics for a selected container, complete the following steps.

1. In the navigation menu, click **Containers**. The **Containers** page is displayed.
2. In the list of containers, find the container for which you want to view statistics, and then click the  (ellipsis icon) in the upper-right corner of the container's information pane.
3. Click **Details**.
4. The **Container details** page contains the following sections:
 - In the **Active Files**, **Active Bytes**, and **Throughput** charts, you can view current statistics for the container.
 The **Active Files** chart displays the number of active files ingested based on time (in minutes), and the **Active Bytes** displays the number of active bytes ingested based on time (in minutes).
 The **Throughput** chart displays the number of read data in Mebibytes/per second (MiB/s) based on time (in minutes), and the number of write data in MiB/s based on time (in minutes).

i **NOTE:** The values in the **Active Files**, **Active Bytes**, and **Throughput** charts refresh automatically every 15 seconds.
 - In the **Connection** pane, you can view information about the configured connection type for the selected container. The type of information displayed can be different depending on the connection type. For example, for an RDS container, the following information is displayed:
 - Type
 - Enabled
 - Status
 - Capacity
 - In the **Inbound Stats** and **Outbound Stats** panes, you can view detailed information on the inbound throughput, and outbound throughput.
 - The **Client Stats** pane lists ingest and network information.

Displaying container statistics by using the CLI

An alternate method for viewing container statistics is by using the QoreStor CLI command: `stats --container --name <container name>`

This command shows the following information:

- Container Name (name of the container)
- Container ID (ID associated with container)
- Total Inodes (total number of data structures in container)
- Read Throughput (read throughput rate in Mebibytes or MiB/s for container)
- Write Throughput (write throughput rate in MiB/s for container)
- Current Files (current number of files in container)
- Current Bytes (current number of ingested bytes in container)
- Cleaner Status (current space reclamation process status for the selected container)

For more information on QoreStor CLI commands, see the *QoreStor System Command Line Reference Guide*.

Creating a container

For more information about storage groups, see [Managing local storage](#)

i | **NOTE:** QoreStor does not support container names that begin with a number.

Containers can be accessed using the following connection types:

- **NFS**
- **CIFS**
- **Quest Rapid Data Storage (RDS)**
- **Object (S3 compatible)**
- **Veritas OpenStorage Technology(OST)**
- **Virtual tape library (VTL)**

Refer to the sections below for instructions on creating containers:

- [Creating an OST or RDS connection type container](#)
- [Creating an NFS or CIFS connection type container](#)
- [Creating an Object container](#)
- [Creating a VTL type container](#)

Creating an OST or RDS connection type container

To create an OST or RDS connection type container, follow these steps:

1. In the navigation menu, click **Containers**. The **Containers** page is displayed.
2. Click **Add Container**.
3. For the container **Name**, type the name of the container, and then click **Next**.
Container names cannot exceed 32 characters in length, must start with a letter, and can be composed of any combination of the following characters:
 - A-Z (uppercase letters)
 - a-z (lowercase letters)
 - 0-9 (numbers). Do not start a container name with a number.
 - dash (-) or underscore (_) special characters

i | **NOTE:** QoreStor does not support the use of the following special characters in container names: /, #, or @.
4. In the **Storage Group** drop-down, select the Storage Group for this container.
5. For **Protocol**, select **Rapid Data Storage (RDS)** or **Veritas OpenStorage (OST)** as appropriate.

6. Click **Next**.
7. On the **User Access Control** page, select the appropriate permissions for the displayed user accounts. Refer to [Configuring User Access Controls](#) for more information.
8. If you selected **RDS**, **LSU Capacity** is set to **Unlimited** by default. If you selected **Veritas OpenStorage (OST)**, for **LSU Capacity** select one of the following options allowed per container:
 - **Unlimited** — To define the allowed amount of incoming raw data per container (based on the physical capacity of the container).
 - **Quota**: To define a set limit in Gibibytes (GiB) for incoming raw data allowed per container.
9. Click **Finish**.

i **NOTE:** To add a container through the command line, use the command:

```
container --add --name <name> [--group_name <name>]
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

Configuring User Access Controls

QoreStor allows you to specify user access controls for individual RDA containers. User access controls allows for multiple containers of the same type while ensuring that access to each container is isolated to specific users. User access controls (UACs) can be set at the container level to assign RWD (read-write-delete) or RW (read-write) permissions on that container to individual user accounts. Data within the containers can be access or deleted by users with both permission types, but the container can only be deleted by a user with RWD permissions.

The **backup_user** account is assigned by default to RDA containers, and is granted RWD permissions. Additional user access can be configured through the GUI or CLI.

i **NOTE:** User Access Controls is currently only supported on RDA containers.

Requirements for using User Access Controls

- The user account to which access is going to be assigned should be created before creating the container or configuring UAC.

To configure User Access Controls

1. In the navigation menu, click **Containers**. The **Containers** page is displayed.
2. In the list of containers, find the container for which you add user access controls, and then click **User Access Control**.
3. The **backup_user** account is listed by default. To configure other accounts with permissions, use the **Search** field to find the account. Click the desired account to add it to the users list.
4. For each listed account, select the appropriate permissions. Options are:
 - **Read/Write** - gives the account read and write permissions on the container.
 - **Read/Write/Delete** - gives the account read, write, and delete permissions on the container.
5. Click **Finish**.

NOTE: To add user access controls to a container through the command line, use the command:

```
container --add --name <name> [--group_name <name>] container --add_uac --name <name> --user <user name> --mode <RW|RWD>
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

Creating an NFS or CIFS connection type container

To add an NFS or a CIFS connection type container, complete the following steps:

1. In the navigation menu, click **Containers**. The **Containers** page is displayed.
2. Click **Add Container**.
3. For the container **Name**, type the name of the container, and then click **Next**.
Container names cannot exceed 32 characters in length, must start with a letter, and can be composed of any combination of the following characters:

- A-Z (uppercase letters)
- a-z (lowercase letters)
- 0-9 (numbers). Do not start a container name with a number.
- dash (-) or underscore (_) special characters

NOTE: QoreStor does not support the use of the following special characters in container names: /, #, or @.

4. In the **Storage Group** drop-down, select the Storage Group for this container.
5. For **Protocol**, select **NAS (NFS, CIFS)**.
6. Click **Next**.

7. For **Marker Type**, select the appropriate marker that supports your Data Management Application (DMA).
 - **Auto** — Automatically detects CommVault, Tivoli Storage Manager (TSM), ARCserve, and HP Data Protector marker types. In addition, select this option if you need to support EMC Networker 2.0.
 - **ARCserve**—Supports the ARCserve marker.
 - **BridgeHead** — Supports the BridgeHead HDM marker.
 - **CommVault**—Supports the CommVault marker.
 - **HP DataProtector**—Supports the HP Data Protector marker.
 - **Networker** — Supports EMC Networker 3.0. If you need to support EMC Networker 2.0, select Auto.

 - **Time Navigator**—Supports the Time Navigator marker.
 - **TSM**—Supports the TSM marker.
 - **Unix Dump** — Supports the Amanda marker, among others.

i **IMPORTANT:** Improper marker selection can result in non-optimal savings. As a best practice, if you have only one type of DMA with traffic directed to a container, it is best to select the marker type that supports your DMA (for example, **BridgeHead**, **Auto**, or another). Conversely, as a best practice, if you have traffic from a DMA that is not one of the supported marker types, it is best to disable marker detection for the container by selecting the **None** marker type.

8. For **Access Protocols**, select **NFS** and **CIFS** as appropriate.
(Use **NFS** to back up UNIX or LINUX clients. Use **CIFS** to back up Windows clients.)
9. Click **Next**.

10. If you selected **NFS** as the connection type, configure NFS access as follows. For CIFS connections, proceed to **step 11**.
 - **NFS Options** — Defines the type of access to the container. Select one of the following options.
 - **Read Write Access** — To allow read-write access to the container.
 - **Read Only Access** — To allow read-only access.
 - **Root Mapping**— Select one of the following options from the drop-down list to define the user level you want mapped to this container.
 - **Root** — to specify a remote user with root access to read, write, and access files on the system.
 - **Nobody** — to specify a user on the system without root access permissions.
 - **Administrator** — to specify the system administrator.
 - **NFS Client Access** — Define the NFS client(s) that can access the NFS container or manage the clients that can access this container by selecting one of the following options.
 - **Open (allow all clients)** — To allow open access for all clients to the NFS container you create. (Select this option *only* if you want to enable access for all clients to this NFS container.)
 - **Create Client Access List** — To define specific clients that can access the NFS container. In the Client FQDN or IP text box, type the IP address (or FQDN hostname) and click the Add icon. The “added” client appears in the Allow Clients list box. (To delete an existing client from this list box, select the IP address (or FQDN hostname) of the client you want to delete, and click the Delete icon. The “deleted” client disappears from the list box.)
11. If you selected **CIFS** as the connection type, configure CIFS access as follows.
 - **Client Access** — Define the CIFS client(s) that can access the container or manage the clients that can access this container by selecting one of the following options.
 - **Open (allow all clients)** — To allow open access for all clients to the container you create. (Select this option *only* if you want to enable access for all clients to this container.)
 - **Create Client Access List** — To define specific clients that can access the container. In the Client FQDN or IP text box, type the IP address (or FQDN hostname) and click the Add icon. The “added” client appears in the Allow Clients list box. (To delete an existing client from this list box, select the IP address (or FQDN hostname) of the client you want to delete, and click the Delete icon. The “deleted” client disappears from the list box.)

i **NOTE:** The QoreStor administrator that manages the system has a different set of privileges than does the CIFS administrator user. Only the QoreStor administrator can change the password for the CIFS administrator user. To change the password that allows access for the CIFS administrator user, use the `authenticate --set --user administrator` commands. For more information, see the *QoreStor Command Line Reference Guide*.
12. Click **Next**.
A Configuration Summary of the options you selected for creating the container appears.
13. Click **Finish**.

Creating an Object container

Adding an object container can be accomplished through the QoreStor UI or via the **object_container** command in the QoreStor CLI. Refer to the *QoreStor Command Line Reference Guide* for more information on the **object_container** command.

i | **NOTE:** QoreStor object container does not support object lifecycle management, which means transitioning storage classes or server side expiration of objects is not supported.

To create an object container

1. In the navigation menu, click **Containers**.
2. On the **Containers** pane, click **Add Container**. The Add Container dialog will be displayed.
3. In the Protocol field, select **Object (S3 Compatible)**. The **Name** and **Storage Group** are populated by default.
4. Click **Next**.
5. To apply encryption, select **Encryption** and enter the following:
 - **Passphrase** — the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.

i | **NOTE:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.

- **Confirm Passphrase** — re-enter the passphrase used above.
- **Encryption Mode** — Select either **static** or **internal**.
 - **static** - A global mode of key management in which a fixed key is used to encrypt all data.
 - **internal** - A mode of key lifecycle management in which the keys are periodically generated and rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7 days. This rotation period is user-configurable and can be specified in days.

i | **NOTE:** Refer to [Configuring and Using Encryption at Rest](#) for more information about encryption.

6. Optionally, configure a **Quota** by entering an amount and setting the unit (GiB or TiB). If no value is set, the quota will be unlimited.
7. Optionally, select **Use HTTP instead of HTTPS**. To use an HTTP connection, you must also follow the steps below:
 - a. On the QoreStor server, copy the `aws.conf` file to a new location:

```
cp /etc/oca/aws.conf.oca /etc/oca/aws.conf
```
 - b. Open the `aws.conf` file and update the endpoint connection protocol to `http`:

```
vi /etc/oca/aws.conf
```

Find the line containing **AWS_ENDPOINT_PROTOCOL** and set the value to **http**.

8. **i** **NOTE:** The QoreStor implementation of object storage uses a self-signed certificate. If your data management application requires third party certificates, you must use HTTP to connect to the object container.
9. Click **Next**
10. Review the summary and click **Finish**.

When the process is completed and the object container has been added to QoreStor, you will see the storage group **ObjectContainer** and the container **ObjectStorageGroup** added to the **Storage Groups** and **Container** pages, respectively. See the topics below for information on working with object storage.

- [Creating a bucket](#)
- [Setting user policy](#)
- [Editing an Object Tier](#)

Adding an object container through the command line

To add an object container, complete the following steps.

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Add an object tier using the command

```
object_container --add [--quota <Quota value in GiB or TiB>][--use_http <yes|no>]
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

3. To apply encryption to the data in this object tier, use the command:

```
object_container --encryption [--set <ON | OFF>] [--mode <static|internal> <--interval <7 days to 70 years>]
```

- i** **NOTE:** Due to export regulations, the encryption at rest feature is not available in certain markets, and, therefore, may not be available in your locale. For more information about recommended guidelines for encryption, see [Understanding Encryption at Rest](#)
- i** **NOTE:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.
- i** **NOTE:** After encryption is enabled, all of the data that is backed up is encrypted and is kept encrypted until it is expired and cleaned by the system cleaner. **Note that encryption is an irreversible process.**
- i** **NOTE:** When QoreStor is installed in Object direct mode, only Static encryption is supported.

For more information, refer to the *QoreStor Command Line Reference Guide*.

4. After creating an object container, you must configure user access for the container. By default, the **backup_user** account is configured with the object role and read/write access. To set the user policy for additional user accounts, use the command:

```
object_container --policy [--set] [--policy_type <readonly|readwrite|none>] --name <user name> [--show] --name <user name>
```

i **IMPORTANT:** The **backup_user** and password are to be used as access key and secret key respectively when connecting to QoreStor from the S3 clients. The default values are:

Access key: backup_user

Secret key: St0r@ge!

To see the S3 endpoint, use the command **object_container CLI /opt/qorestor/bin/object_container --show --endpoint**

The endpoint is displayed in the format **https://<QoreStor IP address>:9000**

Make sure port 9000 is allowed for access through the firewall.

Creating a VTL type container

i **NOTE:** For more information on using VTL containers, see [Configuring and using VTL](#).

To create a virtual tape library (VTL) type container, complete the following steps.

i **NOTE:** The number of supported VTL containers varies depending on the QoreStor installation mode. Refer to the *QoreStor Interoperability Guide* for more information.

1. In the navigation menu, click **Containers**. The **Containers** page is displayed.
2. Click **Add Container**.
3. For **Name**, type the name of the container.

i **NOTE:** QoreStor does not support spaces or the following special characters in container names: /, #, or @. VTL container names cannot exceed 32 characters in length, must start with a letter, and can be composed of any combination of the following characters:

- A-Z (uppercase letters)
- a-z (lowercase letters)
- 0-9 (numbers). (Do not start a container name with a number.)
- underscore (_) special characters
- hyphen (-) special character

i **NOTE:** iSCSI VTL containers do not support the following characters:

- ASCII CONTROL CHARACTERS and SPACE through ,
- ASCII /
- ASCII ; through @
- ASCII [through `
- ASCII { through DEL

4. For **Protocol**, select **Virtual Tape Library (VTL)**.

5. Click **Next**.
6. For **Robot Model**, select the type of virtual tape library for the VTL container.
 - STK L700—This is the standard emulation of the StorageTek L700 library.
 - QUEST DR_L700 - This is a Quest OEM version of StorageTek L700 library.

i **NOTE:** The Quest version of the VTL is supported only with Symantec Backup Exec and Netbackup data management applications (DMAs).

7. For **Tape Size**, select the size of the tapes for your tape library from one of the following options.
 - 800 GB
 - 400 GB
 - 200 GB
 - 100 GB
 - 50 GB
 - 10 GB

i **NOTE:** Creating a VTL container type creates a tape library of type Storage Tek L700 with 10 tape drives of type IBM Ultrium LTO-4 and 60 tape slots holding 60 tapes. Additional tapes can be added as required. For more information, see [VTL and QoreStor specifications](#).

8. For **Access Protocol**, select one of the following options. Each protocol has different configuration requirements, as listed below.

- **NDMP**

- Enter DMA's **FQDN or IP address** that will access the VTL container.
- For **Marker Type**, select the appropriate marker that supports your DMA from the options below:
 - **None** — Disables marker detection for the container.
 - **Auto** — Automatically detects CommVault, Tivoli Storage Manager (TSM), ARCserve, and HP Data Protector marker types. In addition, select this option if you need to support EMC Networker 2.0.
 - **ARCserve**—Supports the ARCserve marker.
 - **BridgeHead** — Supports the BridgeHead HDM marker.
 - **CommVault**—Supports the CommVault marker.
 - **HP DataProtector**—Supports the HP Data Protector marker.
 - **Acronis** —Supports the Acronis marker
 - **Networker** — Supports EMC Networker 3.0. If you need to support EMC Networker 2.0, select Auto.
 - **TSM**—Supports the TSM marker.
 - **Unix Dump** — Supports the Amanda marker, among others.

- **iSCSI**

- Enter the **FQDN, IQN, or IP address** of the iSCSI initiator that can access the VTL container.
- For **Marker Type**, select the appropriate marker that supports your DMA from one of the following options:

i **NOTE:** Improper marker selection can result in non-optimal savings. As a best practice, if you have only one type of DMA with traffic directed to a container, it is best to select the marker type that supports your DMA. Conversely, as a best practice, if you have traffic from a DMA that is not one of the supported marker types, it is best to disable marker detection for the container by selecting the None marker type.

- **None** — Disables marker detection for the container.
- **Auto** — Automatically detects CommVault, Tivoli Storage Manager (TSM), ARCserve, and HP Data Protector marker types. In addition, select this option if you need to support EMC Networker 2.0.
- **ARCserve**—Supports the ARCserve marker.
- **BridgeHead** — Supports the BridgeHead HDM marker.
- **CommVault**—Supports the CommVault marker.
- **HP DataProtector**—Supports the HP Data Protector marker.
- **Acronis** —Supports the Acronis marker
- **Networker** — Supports EMC Networker 3.0. If you need to support EMC Networker 2.0, select Auto.
- **TSM**—Supports the TSM marker.
- **Unix Dump** — Supports the Amanda marker, among others.

- **No Access.**

i **NOTE:** QoreStor allows you to create a VTL container type without configuring it with a specific protocol (that is, by selecting **No Access**). You can configure the container at a later date.


9. Click **Next**.

A summary of the options you selected for creating the container appears.

10. Click **Finish**.

Viewing VTL tape information

Once you have created a virtual tape library (VTL) type container, you can view the detailed tape information of the VTL. This includes information about the vendor and model information for medium changer and tape drives. To view VTL information, complete the following steps.

1. In the navigation menu, click **Containers**. The **Containers** page is displayed.
2. In the list of containers, find the container for which you want to view statistics, and then click the  (ellipsis icon) in the upper-right corner of the container's information pane.
3. Click **Details**.

4. You can view the following information:

- Container Details
 - Number of Tape Drives
 - Library ID
 - Tape Size
 - is OEM
 - Container Path
 - Marker
 - Created On
- Connection
 - Enabled
 - Status
 - Cartridges Available

Adding a Cloud Tiering policy

Once a cloud tier is created, you must enable a cloud tiering policy for a container before that container can be replicated to the cloud. Refer to [Adding a Cloud Tier](#) for more information.

1. In the navigation menu, click **Containers**. The **Containers** page is displayed.
2. In the list of containers, find the correct container and then click **Enable Cloud Tiering Policy**.

3. In the **Enable Cloud Tiering Policy** page, enter the following information:
 - **Cloud Policy**-- allows you to configure the amount of time that files must be idle before being sent to the cloud as well as how long to keep a local copy of the files. The configured times should be less than the backup expiry or retention time configured in the backup application. When the backup is expired by the backup application, the files corresponding to the backup are removed from local storage and cloud storage.
 - **Idle time before cloud migration**--Specify the number of hours files must be idle before being sent to the cloud.
 - **On-Prem Retention Age**--Specify the number of hours files will be kept locally after they are sent to the cloud.

Click on **Advanced Options** to view the following:

i | **NOTE:** The Advanced Options settings are not supported for object containers.

- **Folder Paths**--files can be included or excluded based on their location.
 - **Include**--only files in the listed directories will be included for replication.
 - **Exclude**-- all files except those in the listed directories will be replicated.
 - **File Extensions/Regular Expressions**--files can be included or excluded based on their extension or by regular expressions. Refer to [Using regular expressions](#) for more information.
 - **Include**--only files with the specified extensions will be included for replication.
 - **Exclude**--all files except those with the specified extensions will be replicated.
 - **Include Regular Expression**-- includes only files matching the entered regular expression.
 - **Exclude Regular Expression**-- excludes only files matching the entered regular expression.
4. Click **Enable**.

i | **NOTE:** To add a cloud tiering policy through the command line, use the command **container --cloud_policy**. Refer to the *QoreStor Command Line Reference Guide* for more information.

Using regular expressions

QoreStor provides an option to select files for inclusion (or exclusion) based file names, character sets, and extensions using regular expressions.

Example expressions

- To include all the files with filename starting with "BackupImage" and having extension .tar, .gz, or .zip.
^Backupimage.*(zip|tar|gz)
- To perform a simple match of backup images with IMG | HDR | META
(IMG|HDR|META)

- Support for complex regex patterns using character class , meta sequence, and range
 - To match files with filenames starting with **[abn]** and having file extension .txt, or.log
^[abn]\S*. (txt|log)
 - To match file names with only alphanumeric characters. For example, the expression below matches *test1* , *f123file* etc.,
[:alnum:]]+
 - Archive series of log files. For example, the expression below matches the first five logs of **ocafsd** & **aws** logs
ocafsd[1-5].log|aws[1-5].log

Limitations

The current implementation of regular expressions does not support the use of global modifiers such as */g* or */i*. In order to perform case-insensitive matching, a combination of character classes may be used. For example, the expression below can be used to find all combinations of quest, QUEST, QuEst , QUesT, etc.

[Qq][Uu][Ee][Ss][Tt]

Adding an Archive Tiering Policy

Once an archive tier is created, you must enable an archive tiering policy for a container before that container can be archived to the cloud. Refer to [Adding a Cloud Tier](#) for more information.

Archive tiering is available for RDA, VTL, and Object container types.

1. In the navigation menu, click **Containers**. The **Containers** page is displayed.
2. On the **Containers** pane, find the container you wish to archive. Click the ellipses icon, and click **Enable Archive Tiering Policy**.

3. In the **Enable Archive Tiering Policy** page, enter the following information:
 - **Archive Policy**-- allows you to configure the amount of time that files must be idle before being sent to the cloud as well as how long to keep a local copy of the files.
 - **Idle time before archive migration**--Specify the number of hours files must be idle before being archived.
 - **On-Prem Retention Age**--Specify the number of hours files will be kept locally after they are archived.

Click on **Advanced Options** to view the following:

- **Folder Paths**--files can be included or excluded based on their location.
 - **Include**--only files in the listed directories will be included for replication.
 - **Exclude**-- all files except those in the listed directories will be replicated.
 - **File Extensions/Regular Expressions**--files can be included or excluded based on their extension or by regular expressions. Refer to [Using regular expressions](#) for more information.
 - **Include**--only files with the specified extensions will be included for replication.
 - **Exclude**--all files except those with the specified extensions will be replicated.
 - **Include Regular Expression**-- includes only files matching the entered regular expression.
 - **Exclude Regular Expression**-- excludes only files matching the entered regular expression.
4. Click **Enable**.

Deleting a container

Deleting a container through the GUI

To delete an existing container that contains data, complete the following steps.

CAUTION: Before deleting a container, you should first carefully consider whether you need to preserve the data in the container. Before deleting any QoreStor container that contains deduplicated data, you should take steps to preserve this data using another means of long-term retention. Once a container is deleted, the deduplicated data cannot be retrieved.

1. On the navigation menu, click **Storage Groups**. Select the storage group that contains the container you want to delete. (If you are only using the DefaultGroup storage group you do not need to select a group.)
2. In the list of containers, select the container you want to delete, and then click the **Delete** icon.
3. In the **Warning** dialog box, click **Yes** to confirm the deletion.

Deleting a container through the command line

To delete an existing container that contains data, complete the following steps.

1. (missing or bad snippet)
2. Delete a container with the command

```
container --delete --name <name> [--delete_files]
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

Managing local storage

To organize your data, you can easily create storage groups and create containers within those storage groups on your QoreStor system. A storage group allows you to create separate storage policies for different data groups and the different capacities utilized on a single QoreStor. You can also create and organize storage groups for the different organizations in your enterprise, such as Engineering, Sales, Finance, and so on.

After initialization, QoreStor contains a single default storage group, named DefaultGroup.

Refer to these important notes about storage groups.

- Only administrator users can create storage groups.
- Data/containers cannot be moved between storage groups.
- Deduplication is defined at the storage group level and is not global to the appliance.
- Encryption is defined separately for each storage group.
- Compression is defined separately for each storage group.
- The system cleaner cannot be run on a single storage group; only at the system level.
- Before you can delete a storage group, you must delete all containers contained in that storage group.
- A filesystem scan can be run on a single storage group.


To view the Storage Groups page, on the left navigation menu, click **Local Storage > Storage Groups** in the QoreStor navigation pane.

i | **NOTE:** This section refers to using QoreStor with local storage. Please see [Managing cloud storage](#) for information on cloud and archive tiers as well as object storage.

Viewing storage group information

In the QoreStor GUI you can easily view all of your storage groups on the Storage Groups page.

To view storage groups, complete the following steps.

1. In the navigation menu, click **Local Storage** to expand the menu, then **click Storage Groups**.
2. On the **Storage Groups** page you can view the following columns of information about your storage groups.
 - **Name**—Displays the name of the Storage Group.
 - **Encryption**—Displays whether Encryption is turned On or Off.
 - **Compression**—Displays the compression type as either Fast or Best.
 - **Containers**—Displays the number of containers in this storage group. You can click this number, which links to the Containers page for the storage group.
3. In the list of storage groups, find the storage group for which you want to view statistics, and then click the  (ellipsis icon) in the upper-right corner of the information pane.
4. Click **Details**. A page for the selected storage group is displayed, showing the following:
 - **Summary**— Provides summary data for the storage group, including:
 - Name
 - Compression Mode
 - Number of Containers
 - Encryption status
 - Storage group metadata
 - Record Cleaner—
 - **Throughput**—Displays the number of read data in Mebibytes/per second (MiB/s) based on time (in minutes), and the number of write data in MiB/s based on time (in minutes)
 - **Statistics**—Lists the following statistics for the storage group.
 - Cleaner Status
 - Total Inodes
 - Current Files
 - Current Bytes
 - Decrypted Bytes
 - Post Compression Bytes
 - Post Dedupe Bytes
 - Post Encryption Bytes
 - Compression Savings
 - Dedupe Savings
 - Total Savings
 - **Processed Cleaner**—
 - **Log Cleaner**—

Adding a storage group

You can add a storage group to QoreStor through either the QoreStor GUI or the command line interface. In both cases, when creating a storage group you define the name and compression level.

Adding a storage group through the GUI

To add a storage group, complete the following steps.

1. In the navigation menu, click **Local Storage** to expand the menu, then click **Storage Groups**.
2. Click **Add Storage Group**. The Add a Storage Group pane is displayed.
3. In the **Name** field, enter a name for the storage group.
4. Select a **Compression Type** from the drop-down list:
 - **Fast** — Results in shorter backup time, but with less space savings.
 - **Best** — Provides the highest space savings, but with a longer backup time.
5. Optionally, configure a **Quota** by entering an amount and setting the unit (GiB or TiB). If no value is set, the quota will be unlimited.

i | **NOTE:** Quotas define the limit for limit for physical capacity usage. Once reached, data ingests are not allowed until space is recovered through savepoint expiration and cleaner operations.

6. To apply encryption, select **Encryption** and enter the following:
 - **Passphrase** — the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.

i | **NOTE:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.

- **Confirm Passphrase** — re-enter the passphrase used above.
- **Encryption Mode** — Select either **static** or **internal**.
 - **static** - A global mode of key management in which a fixed key is used to encrypt all data.
 - **internal** - A mode of key lifecycle management in which the keys are periodically generated and rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7 days. This rotation period is user-configurable and can be specified in days.

i | **NOTE:** Refer to [Configuring and Using Encryption at Rest](#) for more information about encryption.

i **NOTE:** Due to export regulations, the encryption at rest feature is not available in certain markets, and, therefore, may not be available in your locale. For more information about recommended guidelines for encryption, see [Understanding Encryption at Rest](#)

i **NOTE:** After encryption is enabled, all of the data that is backed up is encrypted and is kept encrypted until it is expired and cleaned by the system cleaner. **Note that encryption is an irreversible process.**

7. Click **Add**

Adding a storage group through the command line

To add a storage group, complete the following steps.

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Add a new storage group using the command

```
storage_group --add --name <name> [--compression_mode <fast|best>] [--quota <Quota value in GiB or TiB>]
```

Refer to the *QoreStor Command Line Reference Guide* for more information

3. To apply encryption to the data in this storage group, use the command:

```
storage_group --encryption --name <name> [--set <ON | OFF>] [--mode <static|internal> <--interval <7 days to 70 years>]
```

For more information, refer to the **Storage Group commands** section of the *QoreStor Command Line Reference Guide*.


i **NOTE:** Due to export regulations, the encryption at rest feature is not available in certain markets, and, therefore, may not be available in your locale. For more information about recommended guidelines for encryption, see [Understanding Encryption at Rest](#)

i **NOTE:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.

i **NOTE:** After encryption is enabled, all of the data that is backed up is encrypted and is kept encrypted until it is expired and cleaned by the system cleaner. **Note that encryption is an irreversible process.**

Modifying a storage group

To modify a storage group via the user interface, complete the following steps

1. In the navigation menu, click **Local Storage** to expand the menu, then click **Storage Groups**.
2. Find the desired storage group from the displayed list. Click the  (ellipsis icon) in the upper-right corner of the storage group's information pane.
3. Click **Edit**.
4. For Storage Optimization, select a **Compression Type** from the drop-down list as needed:
 - **Fast**— Results in shorter backup time, but with less space savings.
 - **Best** — Provides the highest space savings, but with a longer backup time.
 - Optionally, configure a **Quota** by entering an amount and setting the unit (GiB or TiB). If no value is set, the quota will be unlimited. If a quota is currently set, you may increase or decrease the quota value (provided the decreased quota is not less than the current used capacity on the storage group). Once a quota is set, it can be reset to the default value of unlimited.

NOTE: Quotas define the limit for physical capacity usage. Once reached, data ingests are not allowed until space is recovered through savepoint expiration and cleaner operations.
5. You can modify the following **Encryption** settings:

NOTE: For more information about recommended guidelines for setting up encryption, see the topic, [Configuring and Using Encryption at Rest](#).

NOTE: Due to export regulations, the encryption at rest feature is not available in certain markets, and, therefore, may not be available in your locale.

 - **Passphrase**—Enter the passphrase to be used to encrypt content encryption keys. (The passphrase string can take up to 255 characters. And, alphanumeric and special characters can be entered as part of the passphrase string.)
 - **Confirm Passphrase**—Re-enter the encryption passphrase.
 - **Encryption**—Next to **Encryption**, select or clear as needed.
 - **Encryption Mode**—Select the mode of key lifecycle management from one of the following options:
 - **Static**—A global, fixed key is used to encrypt all data.
 - **Internal**—Content encryption keys are generated and rotated on a specified period of days.
6. Click **Update**.

To modify a storage group via the CLI, complete the following steps

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Modify your storage group using the commands below. Refer to the *QoreStor Command Line Reference Guide* for more information.


```
storage_group --show [--name <name>] [--verbose]
storage_group --update --name <name> [--compression_mode <fast|best>] [--quota
<Quota value in GiB or TiB>]
storage_group --encryption --name <name> [--set <ON | OFF>] [--mode
<static|internal> <--interval <7 days to 70 years>]
storage_group --setpassphrase --name <name>
```


Deleting a storage group

Before you can delete a storage group, you must first delete the containers in the storage group. See [Deleting a container](#) for more information.

Deleting a storage group from the GUI

To delete a storage group, complete the following steps.

1. In the navigation menu, click **Local Storage** to expand the menu, then click **Storage Groups**.
2. Find the desired storage group from the displayed list. Click the  (ellipsis icon) in the upper-right corner of the storage group's information pane.
3. Click **Delete**.

 **NOTE:** You cannot delete the DefaultGroup storage group.

4. When prompted to confirm, click **Delete**.

Deleting a storage group from the CLI

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Delete your storage group using the command below. Refer to the *QoreStor Command Line Reference Guide* for more information.

```
storage_group --delete --name <name>
```

Configuring a Performance Tier

Before configuring a performance tier, ensure that you have reviewed the requirements and limitations below.

- Only one volume can be mapped to a performance tier.
- Your performance tier volume must be mapped to high-performance storage.
- Your performance tier volume must be mapped to an XFS file system.
- An existing QoreStor repository may not be mapped to a performance tier.
- Once a performance tier has been created, the storage path cannot be changed.
- Only one performance tier can be added to QoreStor.
- Currently, it is not possible to delete the performance tier.
- The mount location for the high-performance storage must be added to your QoreStor system's file systems table (*fstab*) to mount the storage automatically when the server reboots.
Add mount location to */etc/fstab* using the **noatime** and **dirsync** mount options


```
echo '<storage path> /perf01 xfs defaults,noatime,dirsync 0 0' >> /etc/fstab
```

Adding a performance tier

Adding a performance tier can be accomplished through the QoreStor UI or via the `performance_tier` command in the QoreStor CLI. Refer to the *QoreStor Command Line Reference Guide* for more information on the `performance_tier` command.

To add a performance tier

Before adding a performance tier, ensure that the storage is mounted to the QoreStor server as an XFS filesystem. Refer to [Guidelines for configuring additional storage](#) for additional guidelines and requirements.

1. In the navigation menu, click **Local Storage** to expand the menu, then click **Performance Tier**.
2. Click **Add Performance Tier**.
3. Enter the mount path for the performance tier volume.
4. Optionally, click **Test** to ensure this storage meets the performance requirements. You will be prompted that the test can take several minutes, click **Confirm** to continue.
5. Click **Add**.
When a performance tier is added, QoreStor will also create the corresponding storage group "PerformanceTier" mapped to the performance tier storage.
6. A warning will be displayed notifying you that a service restart may be required. Click **Confirm** to continue.
 **NOTE:** QoreStor services will be restarted. You will need to log into the UI once the restart is complete.
7. Once the performance tier is created, you can enable encryption. Refer to [Editing a performance tier](#).

Adding a performance tier through the command line

To add a performance tier, complete the following steps.

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Add a performance tier using the command

```
performance_tier --add --path <enclosure filesystem dir> [--compression_mode <fast|best>] [--quota <Quota value in GiB or TiB>]
```

Refer to the *QoreStor Command Line Reference Guide* for more information

3. To apply encryption to the data in this performance tier, use the command:

```
performance_tier --encryption [--set <ON | OFF>] [--mode <static|internal> <--  
interval <7 days to 70 years>]
```

For more information, refer to the *QoreStor Command Line Reference Guide*.

- i** **NOTE:** Due to export regulations, the encryption at rest feature is not available in certain markets, and, therefore, may not be available in your locale. For more information about recommended guidelines for encryption, see [Understanding Encryption at Rest](#)
- i** **NOTE:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.
- i** **NOTE:** After encryption is enabled, all of the data that is backed up is encrypted and is kept encrypted until it is expired and cleaned by the system cleaner. **Note that encryption is an irreversible process.**

Editing a performance tier

To modify a performance tier via the user interface, complete the following steps

1. In the navigation menu, click **Local Storage** to expand the menu, then click **Performance Tier**
2. Click **Edit Performance Tier**.
3. On the **Edit Performance Tier** page, select or modify the options below, as appropriate:
 - **Unlimited Quota**— This option is selected by default. To set a quota, de-select this option and enter a numeric value (greater than 100) in the **Quota** field. Select the value format (either GiB or TiB). Refer to [Quotas](#) for more information. Once a quota is set, it can be reset to the default value of unlimited.
 - **Encryption**— Select this option to enable encryption on the performance tier.
 - **Change Password**—This is used to generate a pass phrase key, which is used to encrypt the content encryption keys. It is mandatory to define a passphrase to enable encryption.
 - **Encryption Mode**— Select the mode of key lifecycle management from one of the following options:
 - **Static**— A global, fixed key is used to encrypt all data.
 - **Internal**— Content encryption keys are generated and rotated on a specified period of days.
 - **Key Rotation**— Displays the number of key rotation interval days as N/A, or the number that was set for Internal Encryption Mode. If you selected Internal as the mode of key management, select the number of days for key rotation when a new key is to be generated. This option is available only for **Internal** encryption mode.
 - i** **NOTE:** After encryption is enabled, all of the data that is backed up is encrypted and is kept encrypted until it is expired and cleaned by the system cleaner. Encryption is an irreversible process.
4. Click **Update**.

To modify a performance tier via the CLI, complete the following steps

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Modify your performance tier using the command below. Refer to the *QoreStor Command Line Reference Guide* for more information.

```
performance_tier --update [--compression_mode <fast|best>] [--quota <Quota value in GiB or TiB>]
```

```
performance_tier --encryption [--set <ON | OFF>] [--mode < static | internal >] [--interval <7 days to 70 years>]
```

Configuring Object Container

QoreStor's Object container provides an object storage interface which enables customers to write Object data(S3 format) directly to Qore. This allows solutions that leverage an S3-based connection to send data directly to a QoreStor instance instead of Amazon S3 with the added benefits of deduplication, encryption, replication and network optimized data transfer.

Object storage is configured by adding a container with the Object (S3 Compatible) protocol. Doing so will create the **ObjectStorageGroup** storage group. QoreStor supports only one object container at a time.

i | **NOTE:** Object containers internally use an RDA connection.

Creating an Object container

Adding an object container can be accomplished through the QoreStor UI or via the **object_container** command in the QoreStor CLI. Refer to the *QoreStor Command Line Reference Guide* for more information on the **object_container** command.

i | **NOTE:** QoreStor object container does not support object lifecycle management, which means transitioning storage classes or server side expiration of objects is not supported.

To create an object container

1. In the navigation menu, click **Containers**.
2. On the **Containers** pane, click **Add Container**. The Add Container dialog will be displayed.
3. In the Protocol field, select **Object (S3 Compatible)**. The **Name** and **Storage Group** are populated by default.
4. Click **Next**.

5. To apply encryption, select **Encryption** and enter the following:
 - **Passphrase** — the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.

i | **NOTE:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.
 - **Confirm Passphrase** — re-enter the passphrase used above.
 - **Encryption Mode** — Select either **static** or **internal**.
 - **static** - A global mode of key management in which a fixed key is used to encrypt all data.
 - **internal** - A mode of key lifecycle management in which the keys are periodically generated and rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7 days. This rotation period is user-configurable and can be specified in days.

i | **NOTE:** Refer to [Configuring and Using Encryption at Rest](#) for more information about encryption.
6. Optionally, configure a **Quota** by entering an amount and setting the unit (GiB or TiB). If no value is set, the quota will be unlimited.
7. Optionally, select **Use HTTP instead of HTTPS**. To use an HTTP connection, you must also follow the steps below:
 - a. On the QoreStor server, copy the `aws.conf` file to a new location:


```
cp /etc/oca/aws.conf.oca /etc/oca/aws.conf
```
 - b. Open the `aws.conf` file and update the endpoint connection protocol to `http`:


```
vi /etc/oca/aws.conf
```

 Find the line containing `AWS_ENDPOINT_PROTOCOL` and set the value to `http` .
8.

i | **NOTE:** The QoreStor implementation of object storage uses a self-signed certificate. If your data management application requires third party certificates, you must use HTTP to connect to the object container.
9. Click **Next**
10. Review the summary and click **Finish**.

When the process is completed and the object container has been added to QoreStor, you will see the storage group **ObjectContainer** and the container **ObjectStorageGroup** added to the **Storage Groups** and **Container** pages, respectively. See the topics below for information on working with object storage.

- [Creating a bucket](#)
- [Setting user policy](#)
- [Editing an Object Tier](#)

Adding an object container through the command line

To add an object container, complete the following steps.

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Add an object tier using the command

```
object_container --add [--quota <Quota value in GiB or TiB>][--use_http <yes|no>]
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

3. To apply encryption to the data in this object tier, use the command:

```
object_container --encryption [--set <ON | OFF>] [--mode <static|internal> <--interval <7 days to 70 years>]
```

- i** **NOTE:** Due to export regulations, the encryption at rest feature is not available in certain markets, and, therefore, may not be available in your locale. For more information about recommended guidelines for encryption, see [Understanding Encryption at Rest](#)
- i** **NOTE:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.
- i** **NOTE:** After encryption is enabled, all of the data that is backed up is encrypted and is kept encrypted until it is expired and cleaned by the system cleaner. **Note that encryption is an irreversible process.**
- i** **NOTE:** When QoreStor is installed in Object direct mode, only Static encryption is supported.

For more information, refer to the *QoreStor Command Line Reference Guide*.

4. After creating an object container, you must configure user access for the container. By default, the **backup_user** account is configured with the object role and read/write access. To set the user policy for additional user accounts, use the command:

```
object_container --policy [--set] [--policy_type <readonly|readwrite|none>] --name <user name> [--show] --name <user name>
```

- i** **IMPORTANT:** The **backup_user** and password are to be used as access key and secret key respectively when connecting to QoreStor from the S3 clients. The default values are:
Access key: backup_user
Secret key: St0r@ge!
To see the S3 endpoint, use the command **object_container CLI /opt/qorestor/bin/object_container --show --endpoint**
The endpoint is displayed in the format **https://<QoreStor IP address>:9000**
Make sure port 9000 is allowed for access through the firewall.

Creating a bucket

In S3 compatible storage, buckets are organizational containers that store objects. When creating a bucket, you have the option to enable or disable object locking, and select one of the available Object Locking modes. Object

locking settings apply to all objects in the bucket.

- **Governance** mode - prevents users without the appropriate permissions from overwriting or deleting an object version or altering its lock settings. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary. You can also use governance mode to test retention-period settings before creating a compliance-mode retention period.
- **Compliance** mode - prevents objects from being overwritten or deleted by any user during the specified lock period. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode ensures that an object version can't be overwritten or deleted for the duration of the retention period.
- **None** - no restrictions are applied.

i **NOTE:** QoreStor supports a maximum of 100 buckets. The bucket **default-bucket** is created automatically when the object container is created.

To create a bucket

1. In the navigation menu, click **Containers**.
2. On the **Containers** pane, find the object storage container **ObjectContainer**. Click the ellipses icon, and click **Edit**.
3. Click **Create bucket**.
4. Enter a **Name** for your bucket.
5. Optionally, select **Object Locking** and configure
 - **Locking Mode** - select between **Compliance** and **Governance**.
 - **Locking Duration** - select the number and format (days or years) to specify the time that the object lock will be active.

i **IMPORTANT:** The **Object Locking** status of a bucket cannot be changed once the bucket is created. To ensure flexibility in the future, you may set the object locking status to **enabled**, but the locking mode to **None**. If the locking mode is set to **disabled**, you will not be able to edit the bucket settings in the future

6. Click **Save**.

Editing bucket settings

The settings for existing buckets can be edited on the **Object Storage** page. When changing bucket settings using this procedure, the changes are applied to new objects. To change retention settings on existing objects, refer to [Changing bucket retention](#).

To edit bucket settings

1. On the **Containers** pane, find the object storage container **ObjectContainer**. Click the ellipses icon, and click **Edit**.
2. In the Buckets section, find the desired bucket. Right-click on the ellipsis icon and click **Bucket Settings**.

3. In the **Locking Mode** section, select from one of the options below:
 - **Compliance** - prevents objects from being overwritten or deleted by any user during the specified lock period. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode ensures that an object version can't be overwritten or deleted for the duration of the retention period.
 - **Governing** - prevents users without the appropriate permissions from overwriting or deleting an object version or altering its lock settings. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary. You can also use governance mode to test retention-period settings before creating a compliance-mode retention period.
 - **None** - provides no object locking.

i **IMPORTANT:** Changes in the locking mode are applied to files written to the container after the change was applied. Existing files are locked according to the locking method in place at the time they were added to the container.

4. In the **Locking Duration** field, select the number and format (days or years) to specify the time that the object lock will be active.
5. Click **Update**.

Changing bucket retention

To change retention settings for existing objects, follow the procedures below. To change the default bucket settings for new objects, refer to [Editing bucket settings](#)

To change bucket retention settings

1. On the **Containers** pane, find the object storage container **ObjectContainer**. Click the ellipses icon, and click **Edit**.
2. In the Buckets section, find the desired bucket. Right-click on the ellipsis icon and click **Change Retention**.
3. [Optional] In the **Prefix** section, enter the folder prefix. This will limit retention changes to objects in the specified folder.
4. In the **Locking Mode** section, select from one of the options below:
 - **Compliance** - prevents objects from being overwritten or deleted by any user during the specified lock period. When an object is locked in compliance mode, its retention mode can't be changed, and its retention period can't be shortened. Compliance mode ensures that an object version can't be overwritten or deleted for the duration of the retention period.
 - **Governing** - prevents users without the appropriate permissions from overwriting or deleting an object version or altering its lock settings. With governance mode, you protect objects against being deleted by most users, but you can still grant some users permission to alter the retention settings or delete the object if necessary. You can also use governance mode to test retention-period settings before creating a compliance-mode retention period.
 - **None** - provides no object locking.
5. In the **Locking Duration** field, select the number and format (days or years) to specify the time that the object lock will be active.
6. Click **Update**.

Deleting a bucket

Before deleting a bucket review the details below:

- Deleting a bucket is permanent. Make sure that objects within the bucket can be removed.
- To avoid unnecessary charges, confirm the bucket deletion on your cloud provider portal.

To delete a bucket

1. In the navigation menu, click **Containers**.
2. On the **Containers** pane, find the object storage container **ObjectContainer**. Click the ellipses icon, and click **Edit**.
3. On the list of buckets, click the ellipses icon and click **Delete**.
4. Click **Remove**.

Setting user policy

This dialog allows you to set more detailed permissions for the object tier. Only users with the **Object** role are displayed for policy configuration. See [Managing users](#) for information about adding and modifying user accounts.

i | **NOTE:** Manually created user accounts default to **no Access** to the object container.

To set a user policy

1. In the navigation menu, click **Containers**.
2. On the **Containers** pane, find the object storage container **ObjectContainer**. Click the ellipses icon, and click **Edit**.
3. Click **Set user policy**.
4. In the dialog, users with the **Object** role are displayed. For each user, select the appropriate permission from the drop-down menu. The available options are:
 - **No Access**
 - **Read Only**
 - **Read Write**
5. Click **Save**.

i | **NOTE:** You may also configure object container user policies using the QoreStor CLI, Refer to the QoreStor Command Line Reference Guide for usage details on the **object_container --policy** command option.

Configuring additional storage

QoreStor allows for the configuration of additional storage enclosures in order to increase capacity.

Guidelines for configuring additional storage

Refer to the following important notes and guidelines for understanding storage expansion in QoreStor.

- For Standard and Cloud-Optimizeed installation modes, QoreStor supports a maximum of 5 locations (1 internal plus 4 expansion). When installed in Large mode, QoreStor supports a maximum of 7 locations.
- QoreStor can only add a mounted filesystem path. QoreStor will not create a filesystem if one is not present.
 - The mounted filesystem should be XFS type.
 - Mount path cannot be read-only.
 - The mount path should not be already configured enclosure path.
- When adding storage, the filesystem service will be restarted.
- Storage can be added without being licensed, but an appropriately sized license is required to make the storage usable by QoreStor.
 - Licenses can be added in multiples of Terabytes from 1 TB to the maximum capacity for your QoreStor installation mode.

Adding additional storage

Additional storage can be added through the QoreStor UI or via the **system --storage** command in the QoreStor CLI. Refer to the *QoreStor Command Line Reference Guide* for more information on the **system --storage** command.

i | **IMPORTANT:** Adding storage requires QoreStor services to be restarted. This will take the QoreStor server offline for several minutes.

To add storage

Before adding storage, ensure that the storage is mounted to the QoreStor server as an XFS filesystem. Refer to [Guidelines for configuring additional storage](#) for additional guidelines and requirements.

1. In the navigation menu, click **Local Storage** to expand the menu, then click **Storage Groups**.
2. Click **Add Storage Location**.
3. Enter the mount path for the additional storage. Click **Save**.
4. A warning will be displayed notifying you that a service restart may be required. Click **Confirm** to continue.

Managing cloud storage

QoreStor enables multiple options for extending your on-prem environment to the cloud. Please refer to the sections below for additional information.

- [Adding a Cloud Tier](#)
- [Adding an archive tier](#)

Adding a Cloud Tier

You can add a cloud tier to QoreStor through either the QoreStor GUI or the command line interface. For more information on Cloud Storage Groups and cloud replication, refer to the topics below:

- [Cloud Tier](#)
- [Adding a Cloud Tiering policy](#)
- [Editing a cloud tiering policy](#)
- [Deleting a cloud tier](#)

Adding a cloud tier through the GUI

i | **IMPORTANT:** Your cloud storage must be configured prior to completing this procedure.

The procedures for adding a cloud tier differ slightly based on the cloud storage provider. Review the procedure for your cloud storage provider:

- [Adding a Microsoft Azure cloud tier](#)
- [Adding an Amazon S3 cloud tier](#)
- [Adding a Wasabi S3 cloud tier](#)
- [Adding a Google S3 cloud tier](#)
- [Adding an S3 Compatible cloud tier](#)

Adding a Microsoft Azure cloud tier

To add a Microsoft Azure cloud storage group, complete the following steps:

1. In the navigation menu, click **Cloud Storage** to expand the menu, then click **Cloud Tier**.
2. Click **Configure**.
3. In the **Cloud Provider** drop-down, select **Azure Blob**.
4. Provide a container name. This is the name of your existing Azure container.

5. Enter your **Cloud Connection String**.

i | **NOTE:** The Connection String can be found in your **Azure** portal under **Storage Accounts >Access keys > Connection string**.

6. To apply encryption, in the **Cloud Tier Encryption** section enter the following:

- **Passphrase** — the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.

i | **IMPORTANT:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable. If this passphrase is lost or forgotten, data in the cloud will be unrecoverable.

- **Confirm Passphrase** — re-enter the passphrase used above.

7. Click **Configure**. A Cloud Storage Group will be created.

8. To enable replication to the cloud, you must link a local container to the cloud using the procedures in [Adding a Cloud Tiering policy](#).

Adding an Amazon S3 cloud tier

To add a cloud storage group, complete the following steps:

1. In the navigation menu, click **Cloud Storage** to expand the menu, then click **Cloud Tier**.
2. Click **Configure**.
3. In the navigation menu, click **Cloud Tier**.
4. In the Cloud pane, click **Configure** to add a cloud tier.
5. In the **Cloud Provider** drop-down, select **AWS S3**.
6. Provide the name for your S3 bucket.

7. Enter your **Connection String** using one of the two methods below:

- **Default** - this option will compile your connection string into the correct format using the inputs below.
 - **Access key** - The access key is typically 20 upper-case English characters
 - **Secret key** - The secret key is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
 - **Region** - The region specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region
- **Custom** - this option allows you to enter your connection string with additional parameters.
- Your connection string uses the following syntax:

```
"accesskey=<ABDCEWERS>;secretkey=< >; loglevel=warn; region=<aws-region>;"
```

Please note the following:

- a. The **access key** is typically 20 upper-case English characters
- b. The **secret key** is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
- c. The **region** specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region

An example of a connection string with this syntax follows. Logically, each connection string is unique.

```
accesskey=AKIARERFUCFODHFJUCWK;secretkey=p+8/T+o5WeZkX11QbuPazHX1IdWbwgFplxuVl08J;loglevel=warn;region=eu-central-1;
```

8. To apply encryption, in the **Cloud TierEncryption** section enter the following:

- **Passphrase** — the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.

i **IMPORTANT:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable. If this passphrase is lost or forgotten, data in the cloud will be unrecoverable.

- **Confirm Passphrase** — re-enter the passphrase used above.

9. Click **Configure**. A Cloud Storage Group will be created.

10. To enable replication to the cloud, you must link a local container to the cloud using the procedures in [Adding a Cloud Tiering policy](#).

Adding a Wasabi S3 cloud tier

To add a cloud storage group, complete the following steps:

1. In the navigation menu, click **Cloud Storage** to expand the menu, then click **Cloud Tier**.
2. In the Cloud pane, click **Configure** to add a cloud tier.
3. In the **Cloud Provider** drop-down, select **Wasabi S3**.
4. Provide a container name. This is the existing name of your container in your cloud platform.
5. Enter your **Connection String** using one of the two methods below:
 - **Default** - this option will compile your connection string into the correct format using the inputs below.
 - **Access key** - The access key is typically 20 upper-case English characters
 - **Secret key** - The secret key is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
 - **Region** - The region specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region
 - **Endpoint** - If you are using VPC endpoints, enter the correct endpoint information.
 - **Custom** - this option allows you to enter your connection string with additional parameters.
 - Your connection string uses the following syntax:

```
"accesskey=<ABDCEWERS>;secretkey=< >; loglevel=warn; region=<aws-region>;"
```

Please note the following:

- a. The **access key** is typically 20 upper-case English characters
- b. The **secret key** is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
- c. The **region** specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region

An example of a connection string with this syntax follows. Logically, each connection string is unique.

```
accesskey=AKIARERFUCFODHFJUCWK;secretkey=p+8/T+o5WeZkX11QbuPazHX1IdWbwgFplxuVl08J;loglevel=warn;region=eu-central-1;
```

6. To apply encryption, select **Encryption** and enter the following:
 - **Passphrase** — the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.

i **IMPORTANT:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable. If this passphrase is lost or forgotten, data in the cloud will be unrecoverable.
 - **Confirm Passphrase** — re-enter the passphrase used above.
7. Click **Configure**. A Cloud Storage Group will be created.
8. To enable replication to the cloud, you must link a local container to the cloud using the procedures in [Adding a Cloud Tiering policy](#).

Adding a Google S3 cloud tier

To add a cloud storage group, complete the following steps:

1. In the navigation menu, click **Cloud Storage** to expand the menu, then click **Cloud Tier**.
2. In the Cloud pane, click **Configure** to add a cloud tier.
3. In the **Cloud Provider** drop-down, select **Google S3**.
4. Provide a container name. This is the existing name of your container in your cloud platform.

5. Enter your **Connection String** using one of the two methods below:

- **Default** - this option will compile your connection string into the correct format using the inputs below.
 - **Access key** - The access key is typically 20 upper-case English characters
 - **Secret key** - The secret key is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
 - **Region** - The region specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region
 - **Endpoint** - If you are using VPC endpoints, enter the correct endpoint information.
- **Custom** - this option allows you to enter your connection string with additional parameters.

- Your connection string uses the following syntax:

```
"accesskey=<ABDCEWERS>;secretkey=< >; loglevel=warn; region=<aws-region>;"
```

Please note the following:

- a. The **access key** is typically 20 upper-case English characters
- b. The **secret key** is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
- c. The **region** specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region

An example of a connection string with this syntax follows. Logically, each connection string is unique.

```
accesskey=AKIARERFUCFODHFJUCWK;secretkey=p+8/T+o5WeZkX11QbuPazHX1IdWbwgFplxuV108J;loglevel=warn;region=eu-central-1;
```

6. To apply encryption, select **Encryption** and enter the following:

- **Passphrase** — the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.

i **IMPORTANT:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable. If this passphrase is lost or forgotten, data in the cloud will be unrecoverable.

- **Confirm Passphrase** — re-enter the passphrase used above.

7. Click **Configure**. A Cloud Storage Group will be created.

8. To enable replication to the cloud, you must link a local container to the cloud using the procedures in [Adding a Cloud Tiering policy](#).

Adding an S3 Compatible cloud tier

To add a cloud storage group, complete the following steps:

1. In the navigation menu, click **Cloud Storage** to expand the menu, then click **Cloud Tier**.
2. In the Cloud pane, click **Configure** to add a cloud tier.
3. In the **Cloud Provider** drop-down, select **S3 Compatible**.
4. Provide a container name. This is the existing name of your container in your cloud platform.
5. Enter your **Connection String** using one of the two methods below:
 - **Default** - this option will compile your connection string into the correct format using the inputs below.
 - **Access key** - The access key is typically 20 upper-case English characters
 - **Secret key** - The secret key is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
 - **Region** - The region specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region
 - **Endpoint** - If you are using VPC endpoints, enter the correct endpoint information.
 - **Custom** - this option allows you to enter your connection string with additional parameters.
 - Your connection string uses the following syntax:

```
"accesskey=<ABDCEWERS>;secretkey=< >; loglevel=warn; region=<aws-region>;"
```

Please note the following:

- a. The **access key** is typically 20 upper-case English characters
- b. The **secret key** is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
- c. The **region** specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region

An example of a connection string with this syntax follows. Logically, each connection string is unique.

```
accesskey=AKIARERFUCFODHFJUCWK;secretkey=p+8/T+o5WeZkX11QbuPazHX1IdWbwgFplxuVl08J;loglevel=warn;region=eu-central-1;
```

6. To apply encryption, select **Encryption** and enter the following:
 - **Passphrase** — the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.

i | **IMPORTANT:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable. If this passphrase is lost or forgotten, data in the cloud will be unrecoverable.
 - **Confirm Passphrase** — re-enter the passphrase used above.
7. Click **Configure**. A Cloud Storage Group will be created.
8. To enable replication to the cloud, you must link a local container to the cloud using the procedures in [Adding a Cloud Tiering policy](#).

Adding a cloud tier through the command line

To add a cloud tier, complete the following steps.

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Add a new cloud tier using the command

```
cloud_tier --add --cloud_container <name> --cloud_provider <AWS-S3|AZURE|Wasabi-S3|Google-S3|S3-Compatible>
```

i | **NOTE:** You will be prompted to enter your Azure connection string or AWS access string after executing the command.

Refer to the *QoreStor Command Line Reference Guide* for more information on the **cloud_tier** command and available options.

Deleting a cloud tier

Before deleting a cloud tier, review the details below:

- The metadata for the files replicated to cloud will be removed locally. This makes those cloud-replicated files unrecoverable.
- Data in the cloud bucket has to be deleted manually.
- Cloud policy settings on the source containers are unaffected.

Deleting a cloud tier from the GUI

To delete a cloud tier, complete the following steps.

1. In the navigation menu, click **Cloud Storage** to expand the menu, then click **Cloud Tier**.
2. Click **Delete**.

3. When prompted to confirm, click **Delete**.
4. In the **Passphrase** field, enter the passphrase used for Cloud Tier encryption. This provides validation that the person deleting the cloud tier has the appropriate authorization.
5. Review the containers linked to the cloud tier and confirm that data in these containers can be deleted. Any containers with managed replication configured must be deleted manually before the cloud tier can be deleted.
6. Click **Delete**.

Deleting a cloud tier from the CLI

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Delete your cloud tier using the command below. Refer to the *QoreStor Command Line Reference Guide* for more information.

```
cloud_tier --delete
```

3. At the prompt, enter **y** for yes and press **[Enter]**.

Configuring an Archive Tier

Archive tiers can be configured via the UI or via the **cloud_tier** command in the QoreStor CLI. Before configuring an archive tier, ensure the following requirements are met:

- Your cloud storage must be configured prior to configuring an archive tier.
- Archive tier is not supported when QoreStor is installed in Cloud Optimized mode, Object Direct Small mode, or Demo mode.
- Permissions for your cloud storage must be correctly configured. Refer to [Required permissions to restore from Archive Tier](#) for more information.
- Only RDA, VTL, and Object containers can be configured to tier data to Archive Tier.

i **NOTE:** QoreStor's archive tier functionality relies on Amazon S3 Glacier and/or Amazon S3 Glacier Deep Archive storage. Before configuring an archive tier, your cloud archive storage must be properly configured. Please refer to the Amazon S3 documents below for more information:

- [Getting Started with Amazon Simple Storage Service](#)
- [Amazon S3 Console User Guide](#)
- [S3 Batch Operations](#)

Required permissions to restore from Archive Tier

In order for Qorestor to be able to perform batch operations for restoring objects to Amazon S3 storage from Amazon S3 Glacier or Amazon S3 Glacier Deep Archive storage , you must configure an AWS IAM policy with the required permissions listed below and attach the policy to your AWS account used to access the for accessing AWS S3 storage.

In order for QoreStor to be able to perform batch operations on your S3 storage, you must configure an S3 IAM role with the required permissions and batch operation policy and use that role when creating your archive tier. The permissions required are:

- Create Job
- Pass Role
- The permissions defined in the "Initiate S3 Glacier restore" policy described in the Amazon S3 document [Granting permissions for Amazon S3 Batch Operations](#)
 - s3:RestoreObject
 - s3:GetObject
 - s3:GetObjectVersion
 - s3:GetBucketLocation
 - s3:PutObject
 - s3:GetBucketLocation

i | **NOTE:** Permission verification is done when restoring an object from S3.

Adding an archive tier

To add an archive tier

1. In the navigation menu, click **Cloud Storage** to expand the menu, then click **Archive Tier**.
2. In the Archive Tier pane, click **Configure** to add a cloud tier.
3. In the **archive provider** drop-down, select **AWS S3**.
4. Provide the name for your S3 bucket.

5. Enter your **Connection String** using one of the two methods below:

- **Default** - this option will compile your connection string into the correct format using the inputs below.
 - **Access key** - The access key is typically 20 upper-case English characters
 - **Secret key** - The secret key is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
 - **Region** - The region specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region
- **Custom** - this option allows you to enter your connection string with additional parameters.
- Your connection string uses the following syntax:

```
"accesskey=<ABDCEWERS>;secretkey=< >; loglevel=warn; region=<aws-region>;"
```

Please note the following:

- a. The **access key** is typically 20 upper-case English characters
- b. The **secret key** is generated automatically by AWS. It is typically 40 characters, including mixed upper and lower-case and special symbols.
- c. The **region** specifies the Amazon-specific region in which you want to deploy your backup solution. Your region name can be obtained from https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region

An example of a connection string with this syntax follows. Logically, each connection string is unique.

```
accesskey=AKIARERFUCFODHFJUCWK;secretkey=p+8/T+o5WeZkX11QbuPazHX1IdWbwgFplxuVl08J;loglevel=warn;region=eu-central-1;
```

6. To apply encryption, in the **Archive Tier Encryption** section enter the following:

- **Passphrase** — the passphrase is user-defined and is used to generate a passphrase key that encrypts the file in which the content encryption keys are kept. The passphrase is a human readable key, which can be up to 255 bytes in length. It is mandatory to define a passphrase to enable encryption.

i **IMPORTANT:** It is mandatory to define a passphrase to enable encryption. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable. If this passphrase is lost or forgotten, data in the cloud will be unrecoverable.

- **Confirm Passphrase** — re-enter the passphrase used above.

7. In the **Archive Tier Options** section, enter the following:
 - **Archive Retention in Warm Cloud** - When restore operation succeeds, a temporary copy of the Glacier object is created in standard S3 storage. This setting specifies the number of days this temporary copy is held in S3 before it is deleted. Valid values are any integral values from 1 through 365.
 - **Archive Role ARN** - S3 must have permissions to perform batch operations on behalf of the user. An IAM role must be created that has "Create Job", "Pass Role" and other permissions to access the buckets as well as perform the batch operations. The account admin is expected to create such roles.
 - **NOTE:** For more information on required permissions and S3 batch operations, refer to [Required permissions to restore from Archive Tier](#) and the AWS documents [Granting permissions for Amazon S3 Batch Operations](#) and [The basics: S3 Batch Operations](#).
 - **Archive Service Name**- Select between **S3-Glacier** or **S3 Deep Archive**.
8. Click **Configure**. A Cloud Storage Group will be created.
9. To enable replication to the cloud, you must link a local container to the cloud using the procedures in [Adding a Cloud Tiering policy](#).

Deleting an archive tier

Before deleting a archive tier, review the details below:

- The metadata for the files archived to the cloud will be removed locally. This makes those files unrecoverable.
- Data in the cloud bucket has to be deleted manually.
- Archive policy settings on the source containers are unaffected.

Deleting a cloud tier from the GUI

To delete an archive tier, complete the following steps.

1. In the navigation menu, click **Cloud Storage** to expand the menu, then click **Archive Tier**.
2. Click **Delete**.
3. When prompted to confirm, click **Delete**.
4. In the **Passphrase** field, enter the passphrase used for Archive Tier encryption. This provides validation that the person deleting the archive tier has the appropriate authorization.
5. Review the containers linked to the archive tier and confirm that data in these containers can be deleted.
6. Click **Delete**.

Deleting an archive tier from the CLI

1. Access the QoreStor CLI. Refer to [Using the QoreStor command line](#) for more information.
2. Delete your archive tier using the command below. Refer to the *QoreStor Command Line Reference Guide* for more information.

```
cloud_tier --delete --cloud_archive
```

3. At the prompt, enter **y** for yes and press **[Enter]**.

Restoring from archive tier

Depending on the container type, data is sent to the archive tier by different methods. For RDA and Object containers, data is archived based on the Archive Tiering Policy. For VTL containers, exporting the cartridge from the backup application will trigger the movement of cart data to cloud. Restoring data from an archive tier differs in some ways from a standard restore process. When restoring from an archive tier, no files are saved to on-prem storage. Instead, files are copied from the archive storage (Glacier or Amazon S3 Glacier Deep Archive) to warm AWS S3 storage for a period of time specified by the **Archive Retention in Warm Cloud** setting. When restoring from an archive tier, consider the following:

- Restoring from archive storage is a two-step operation. First, archive data is restored to standard AWS S3 storage, then the objects are read from there.
- Restored objects will be ready for readback after 4-6 hours for Amazon S3 Glacier (10-12 hours for Amazon S3 Glacier Deep Archive). No notification is issued when restored objects are available. You may view the status of restore operations in the AWS Console. Refer to the Amazon S3 document [Checking Archive Restore Status and Expiration Date](#) for more information. To perform a batch restore for disaster recovery purposes, refer to [Manually restoring datastores from Amazon S3 Glacier](#).
- When restoring objects from archive, you are charged for both the archive copy and the restore copy in warm storage. Use the **Archive Retention in Warm Cloud** value to minimize the duration objects are kept in warm storage.
- For restoring VTL cartridge data, the **command vtl --import** must be run on the QoreStor server.

Manually restoring datastores from Amazon S3 Glacier

To perform a disaster recover from an archive tier, you must first restore all datastores to standard Amazon S3 storage. The procedure below will guide you in performing this action in the AWS Console.

1. Using the **ls** command, recursively get the contents of the cds folder in the cloud bucket you wish to restore.

i | **NOTE:** Note that **bucket_name** is a placeholder for the bucket name. Replace this with your actual bucket name.

```
# aws s3 ls s3://bucket_name/cds --recursive | awk '{print "bucket_name,"$NF}'  
> manifest.csv
```

This command will create a *manifest.csv* file. A sample version of a *manifest.csv* file is shown below:

```
# head manifest.csv  
bucket_name,cds/0000/0000/0000/0001/158/158.imap
```

```

bucket_name,cds/0000/0000/0000/0001/158/158_0
bucket_name,cds/0000/0000/0000/0003/357/357.imap
bucket_name,cds/0000/0000/0000/0003/357/357_0
bucket_name,cds/0000/0000/0000/0004/439/439.imap
bucket_name,cds/0000/0000/0000/0004/439/439_0
bucket_name,cds/0000/0000/0000/0008/869/869.imap
bucket_name,cds/0000/0000/0000/0008/869/869_0
bucket_name,cds/0000/0000/0000/0010/1035/1035.imap
bucket_name,cds/0000/0000/0000/0010/1035/1035_0

```

2. To ensure the manifest file can be uploaded successfully, add an MD5 hash.

```

# openssl md5 -binary manifest.csv | base64
BBpU3xTS3/XKnmDm+uqdnng==

```

3. Paste the MD5 in the **put-object** command. The resulting ETAG can be used for initiating the restore job.

i | **NOTE:** `--key <path>` can be used for uploading manifest into any prefixed location in that bucket.

```

# aws s3api put-object --bucket bucket_name --key manifest.csv --body
manifest.csv --content-md5 BBpU3xTS3/XKnmDm+uqdnng==
{
  "ETag": "\"041a54df14d2dff5ca9e60e6faea9d9e\""
}

```

4. The uploaded manifest, its location and ETAG can be used for initiating a batch operation restore job through the AWS console. Alternatively, you may use the **create-job** API as follows:

```

# aws s3control create-job --no-confirmation-required --account-id
177436582181 \
  --operation '{"S3InitiateRestoreObject" : { "ExpirationInDays" : 7,
"GlacierJobTier" : "STANDARD" }}' \
  --report '{ "Bucket":"arn:aws:s3:::bucket_name", \
    "Prefix":"batch", \
    "Format":"Report_CSV_20180820", \
    "Enabled":true, \
    "ReportScope":"AllTasks" }' \
  --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_
20180820","Fields":["Bucket","Key"]}, \
    "Location":{"ObjectArn":"arn:aws:s3:::bucket_
name/manifest.csv","ETag":"\"041a54df14d2dff5ca9e60e6faea9d9e\""}}' \
  --role-arn arn:aws:iam::177436582181:role/BatchOperationUser \
  --priority 10
{
  "JobId": "ea4915fc-2cbb-4d00-895e-a363743b9c8c"
}

```

5. Restored objects will be ready for readback after 4-6 hours for Amazon S3 Glacier (10-12 hours for Amazon S3 Glacier Deep Archive). You can click on an individual CDS object to make sure it is ready for readback (ongoing-request = false, expiry-date = <some future date>) before attempting to restore from QoreStor. Optionally, you can perform a head-object inquiry on any one of the CDS entries from the uploaded manifest file:

```
# aws s3api head-object --bucket bucket_name --key
cds/0000/0000/0000/0001/158/158_0
{
  "AcceptRanges": "bytes",
  "Restore": "ongoing-request=\"false\", expiry-date=\"Sat, 05 Sep
2020 00:00:00 GMT\"",
  "LastModified": "2020-09-03T08:20:42+00:00",
  "ContentLength": 4245203,
  "ETag": "\"98b38ff76a2dc04f423ba954af44c052\"",
  "ContentType": "binary/octet-stream",
  "Metadata": {},
  "StorageClass": "GLACIER"
}
```

i **NOTE:** Note that the time required to run the **ls** command can be quite long for a high number of objects. In the example below, the **ls** operation on a 1 TB file took approximately 43 minutes. If the command fails due network or connection issues, please restart.

```
# time aws s3 ls s3://st-6300-19-archive/cds --recursive | awk '{print "st-
6300-19-archive,"$NF}' > st-6300-19-archive_manifest.csv
real    43m24.906s
user    39m1.575ssys    1m11.745s

# ls -al st-6300-19-archive_manifest.csv
-rw-rw-r-- 1 quser quser 163138124 Sep  3 05:15 st-6300-19-archive_
manifest.csv

# wc -l st-6300-19-archive_manifest.csv
2680848 st-6300-19-archive_manifest.csv

# time aws s3api put-object --bucket bucket_name --key st_manifest.csv --body
./st-6300-19-archive_manifest.csv --content-md5 ni/tJMLCpB019A1m3Te3sg==
{
  "ETag": "\"9e2fed24c2c2a41d25f40d66dd37b7b2\""
}

real    0m5.281s
user    0m1.930s
sys     0m0.560s
```

Performing a recovery from the cloud

To recover your QoreStor configuration and cloud-replicated data from the cloud, perform the steps below. Before performing these steps, make sure you have the following:

- A functional, properly licensed QoreStor server.
- The connection string for your cloud storage account. This is different depending on your cloud provider. Refer to the appropriate section below for more information.
 - [Adding a Microsoft Azure cloud tier](#)
 - [Adding an Amazon S3 cloud tier](#)
 - [Adding a Wasabi S3 cloud tier](#)
 - [Adding an S3 Compatible cloud tier](#)

To perform a disaster recovery

1. On your QoreStor server, execute the recovery command

```
maintenance --disaster_recovery --cloud_string <name> --container_name <name>
--cloud_provider_type <name> --passphrase <name> [--logfile <name>]
```

where

```
--cloud_string          cloud connection string.
--container_name        cloud container name.
--cloud_provider_type   cloud provider type.
--passphrase            passphrase.
--logfile               log file path.
```

This will regenerate configuration data, initialize the QoreStor dictionary, and configure container namespace and blockmaps. When completed, you will see the message

```
Processing Datastores: Done
```

2. After the data recovery process is complete, perform a filesystem repair with the command

```
maintenance --filesystem --repair_now
```

When the file system repair is finished, the process is complete.

Next steps

Depending on your configuration, there may be several steps required after recovering your QoreStor server. Some actions to consider are:

- If you are using QoreStor with NetVault Backup, you will need to add the new QoreStor as target device and add the container.
- Depending on your DMA, you may need to reconfigure DMA or client connections to reference the new QoreStor server.
- Once a disaster recovery completes, the recovered source containers will be unencrypted. Before ingesting new data into the recovered containers, you must enable encryption on the recovered storage groups.

i | **NOTE:** The recovered containers contain only stub files. The data remains encrypted in the cloud tier.

Managing replications

In the QoreStor GUI, you can set up and manage data replication operations. Such replication operations include, creating new replication relationships, managing or deleting existing replication relationships, starting and stopping replication, and displaying current replication statistics.

Guidelines and prerequisites for replication

Refer to the following important notes and guidelines for understanding and using replication in QoreStor.

- **TCP Port Configuration**—If you plan to perform replication operations across a firewall, the replication service requires that the following fixed TCP ports be configured to support replication operations:
 - port 9904
 - port 9911
 - port 9915
 - port 9916
- **DMAs and Domain Relationships** — To allow replication storage information to be viewed by a corresponding data management application (DMA), the target QoreStor system must reside in the same domain as the source QoreStor system in the replication relationship.
- **Replication Limits** — Refer to the *QoreStor Interoperability Guide* for details about the supported system limits for replication. For a definition of connections and streams, see [Streams_vs_Connections](#).
- **Version Checking** — The QoreStor software includes version checking that limits replication only between other QoreStor systems that run the same system software version. If versions are incompatible, the administrator will be notified by an event, and replication will not continue.
- **Storage Capacity and Number of Source Systems** — Be aware that the storage capacity of the target QoreStor system is directly affected by the number of source systems writing to its containers, and also by the amount being written by each of these source systems.

- **Bandwidth limiting** — Refer to the **replication** command in the QoreStor Command Line Reference Guide for information regarding limiting bandwidth consumption for replication.
- **MTU Setting** — Primary and secondary replication targets should have the same network maximum transmission unit (MTU) setting.

Replication seeding

QoreStor supports replication seeding, which provides the ability to create a local seed and place it in a remote system. The seed backup is a process on the source QoreStor system, which collects all of the unique data chunks from the containers and stores them on the target device. This is helpful if you have a new replication target to set up, the amount of data to be replicated is very large, and the network bandwidth is low.

You can seed the target replica with the source data saved on a third party device, for example, a CIFS-mounted share, attach it to the target QoreStor and then get the data into the target QoreStor. Once the seeding is complete, replication is enabled between source and target and replication re-synchronization is done to complete any pending data transfers. Thereby, continuous replication can be done, which reduces network traffic significantly, and data can be replicated and synced with the target in a short amount of time.

i **NOTE:** The following scenarios are not supported for seeding:

- Import AND export from one share/device cannot occur at the same time.
- Import from one share/device cannot be completed from multiple locations at the same time.
- Export to a mount point can be completed only from one seed job. Multiple seed export jobs cannot send data to a single mount point.

You can initiate seeding using the QoreStor command line interface (CLI), and the data to be seeded is gathered in an organized manner and stored in the target devices. Refer to the QoreStor *Command Line Reference Guide* for more information about replication seeding support.

Adding replication relationships

When configuring replication for object containers, replication must be added from the source system. Also once replication is added for Object container, the replica container is not accessible. Once replication is deleted then the replica becomes accessible over S3 to the clients.

To add a new replication relationship, complete the following steps.

1. In the navigation menu, click **Replications**.
2. Click **Add Replication**.

3. To define the **Source Container**, select the **Local** or **Remote** option.
 - If you select **Local**, select the local container from the drop-down list.
 - If you select **Remote**, configure the following settings:
 - **Username**—enter the username for the remote system.
 - **Password**—enter the password for the remote system.
 - **Remote Machine**—enter the domain name of the remote system.
 - Click **Retrieve Containers**.
 - **Select Remote Container**—Select the remote container from the drop-down list.
4. For **Encryption**, select one of the following encryption options to encrypt the data as it is replicated: **None**, **AES 128-bit**, or **AES 256-bit**.
5. Under **Target Container**, define the target replica container by configuring the following settings.
 - **Username**—enter the username for the remote system.
 - i** **NOTE:** The credentials used need to be either the admin or administrator account.
 - **Password**—enter the password for the remote system.
 - **Remote Machine**—enter the domain name of the remote system.
 - Click **Retrieve Remote Containers**.
 - Select the remote container from the drop-down list.
6. Click **Next**.
7. Review the summary and click **Finish**.

i **NOTE:** For information about starting and stopping replication, see the topic, [Starting and stopping replication](#). For information about scheduling system operations such as replication, see [Understanding system operation scheduling](#).

Configuring replication schedules

By default, replication of any newly written files in the replicated container will occur when QoreStor detects three (3) minutes of idle time. If you wish to constrain replication activities to a specific schedule, you can configure replication schedules on a weekly basis for individual replication-enabled source containers.

i **NOTE:** It is recommended that you do not schedule the running of any Replication operations during the same time period when Cleaner or data ingest operations will be running. If you do not follow this recommendation, the time required to complete the system operations or system performance might be affected.

To configure replication schedules using the UI:

1. On the left navigation menu, click **Replications**.
The Replications page is displayed, listing all configured replication relationships.
2. The configured replications are displayed.
3. To configure or edit the replication schedule, click **Details**.

4. Click **Edit Schedule**.
5. For each day of the week, click the time selector field. Select the **From** and **To** times to configure a window during which replication can run. Click **Set**.
6. Click **Save Schedule**.

To configure replication schedules, complete the following steps.

1. Access the QoreStor command line interface.
2. Use the QoreStor command line interface (CLI) to create and delete the replication schedule. The available commands are:

```
schedule --add --day <Day of the Week> --start_time <HH:MM> --stop_time
<HH:MM> --name --replication
schedule --delete --day <Day of the Week> --name --replication
```

For full details on running the cleaner schedule commands, help is available by entering:




```
schedule --help
```

You can view replication details and status on the **Replications** page in the QoreStor GUI by selecting a replication and clicking to expand and view details.

Viewing replication information

In the QoreStor GUI, the Replication page displays current information about replication relationships for data containers in your QoreStor system.

To view replication information

1. In the navigation menu, click **Replications**.
2. The configured replications are displayed.
Using the  or  toggle in the upper-right corner of the Replications pane, you may switch between tile and grid views.
3. To view more detailed information and additional options, click the ellipsis icon  and click **Details**.
 - **Tile view** - the ellipsis icon is to the right of the source container. You may also click the **Details** button to the right of the configured replication.
 - **Grid View** - the ellipsis icon is in the Actions column.

The information below is displayed:

- Replication Source and Target Containers
- Replication Source and Target Systems
- Replication Schedule

- A Summary showing:
 - Cloud Enabled status
 - Cloud Storage Group
 - Peer Status
 - Estimated time to sync
 - Last sync time
 - Schedule status.
- Network Savings
- Replication Throughput
- Transfer
- Network Throughput




i | **NOTE:** These statistics refresh every 30 seconds.

Modifying replication relationships

You can modify the following replication settings: encryption and remote container's IP address/host name settings. To modify settings for an existing replication relationship, complete the following steps.

i | **CAUTION:** You should exercise caution when configuring the direction of replication for source and target containers. For example, target containers can have their contents deleted if they contain existing data.

i | **NOTE:** Because you cannot modify an existing defined role (source or target replica) for a replication relationship, if necessary, you must delete the existing replication relationship, and then recreate a new relationship with the specific source and target roles that you want.

1. In the navigation menu, click **Replications**.
2. The configured replications are displayed.
Using the  or  toggle in the upper-right corner of the Replications pane, you may switch between tile and grid views.
3. To edit the replication, click the ellipsis icon  and click **Edit**.
 - **Tile view** - the ellipsis icon is to the right of the source container.
 - **Grid View** - the ellipsis icon is in the Actions column.
4. Modify the settings/values for the **Source**, or **Target** containers as needed.
 - a. **For Remote System**, modify the IP address/host name and user logon credentials of the source remote system as needed.
 - b. Review the replication details, and then click **Save**.



i | **NOTE:** Replication needs to be stopped before the encryption settings can be modified.


5. Click **Save**.

Deleting replication relationships

To delete an existing replication relationship, complete the following steps:

1. In the navigation menu, click **Replications**.
2. The configured replications are displayed.

Using the  or  toggle in the upper-right corner of the Replications pane, you may switch between tile and grid views.

To view more detailed information and additional options, click the ellipsis icon  and click **Delete**.

- **Tile view** - the ellipsis icon is to the right of the source container.
- **Grid View** - the ellipsis icon is in the Actions column.



3. In the confirmation dialog box, click **Delete**.


 **NOTE:** If the deletion fails, you can click **Force Delete** to force removal of the relationship.

Starting and stopping replication

To start or stop replication in an existing replication relationship, complete the following steps.


1. In the navigation menu, click **Replications**.
2. The configured replications are displayed.

Using the  or  toggle in the upper-right corner of the Replications pane, you may switch between tile and grid views.

To view more detailed information and additional options, click the ellipsis icon .

- **Tile view** - the ellipsis icon is to the right of the source container.
- **Grid View** - the ellipsis icon is in the Actions column.

3. To stop the replication process, click the **Stop** icon, and, in the confirmation dialog box, click **Yes** to stop replication.
4. To start the replication process, click the **Start** icon, and, in the confirmation dialog box, click **Yes** to start replication.

 **NOTE:** You can also set up replication schedules as needed. For more information see the topic, [Configuring replication schedules](#).

Managing users

QoreStor gives you the ability to define user roles and assign users to those roles. A user can have more than one role. There are default user roles for the system as well.

QoreStor has the following types of user roles: CIFS, OST, RDA, Secure Connect, Object, and Monitor. For the protocol specific user roles, the user is validated with the protocol credentials when the clients connect.

Refer to these important notes about user management in QoreStor.

- Excluding the admin, users can have multiple roles.
- However, OST users are exclusive user roles that can only be assigned to one user at a time.
- The **admin** user is a special default user; it cannot be deleted and no new administrator roles can be created.
- The maximum number of users that can be created for the system is 64.

To view the Users page, on the left navigation menu, click **Users**.

Managing the default QoreStor user accounts

During the installation process, QoreStor creates two user accounts that simplify permissions and access to QoreStor configurations outside of the UI. Logging in with the **qsadmin** account provides direct access to the QoreStor command line, while the **qsservice** account provides direct access to the QoreStor Menu.

If these accounts are not needed, or if security protocols prohibit non-essential accounts, you may remove these accounts using the QoreStor Menu. To manage these accounts, navigate to the Remove QoreStor Account menu found at **QoreStor Menu > Administration > Operating System > QoreStor User Management**. Refer to [Configuring QoreStor with the Configuration Menu](#) for more information.

Viewing users

You can view user accounts and settings through either the QoreStor GUI or the command line interface.

Viewing users through the GUI

To view users in the GUI, complete the following steps.

1. In the navigation menu, click **Users**.
2. On the **Users** page you can view the following columns of information about users of your system.
 - **Name**—Displays the name of the user.
 - **Role**—Displays the role(s) assigned to this user.
3. For each user, you have the available actions:
 - **Edit Roles** - Displays the roles currently assigned to user and allows you to change assigned roles.
 - **Change password** - Allows you to change the password for a user account.
 - **Remove** - Removes the user account

Viewing users through the command line

To view users using the command line:

1. (missing or bad snippet)
2. View current user accounts with the command:

```
user --show [--users] [--logins] [--verbose] [--name <username>] [--roles  
<cifs|ost|rda|monitor|secureconnect>
```

Refer to the QoreStor Command Line Reference Guide for more information.

Adding a user

You can easily add users and assign them specific system roles by using either the QoreStor GUI or the command line interface. The system supports up to 64 users. Only one administrator account is supported.

Adding a user through the GUI

To add a user through the GUI, complete the following steps.

1. In the left navigation menu, click **Users**.
2. On the right side of the page, click **Add User**. The **Add** pane is displayed.

3. Enter the following information.
 - **Name**—Enter a username between 1 and 32 characters. This setting is required.
 - **Password**—Enter a password between 8 and 16 characters. This setting is required.
 - **Confirm Password**—Re-enter the password. This setting is required.
 - **Roles** —Select from the following options:
 - **RDA**—Designates the user as an RDA protocol user.
 - **Secure connect** - Designates the user as a Secure Connect user.
 - **CIFS** - Designates the user as a CIFS protocol user
 - **Monitor**—Limits the user to read-only access in the QoreStor GUI.
 - **NDMP** - Designates the user as an NDMP protocol user
 - **Object** - Designates the user as an object protocol user
 - **Full Name**—Enter a name for the user.
 - **Email Address**—Enter an email address for the user.
 - **Phone**—Enter a phone number for the user.
 - **Description**—Enter a description for the user.
4. Click **Save**.

Adding a user through the command line

To add a user through the command line, complete the following steps:

1. (missing or bad snippet)
2. Add a new user account with the command
3. To define roles for the new user, use the command

```
user --add --name <user name>
```

```
user --update --name <user name> [--add_roles  
<cifs|ost|rda|ndmp|iscsi|monitor|administrator|secure_connect|object>]
```


Refer to the *QoreStor Command Line Reference Guide* for more information.


Modifying user roles

You can easily change the roles assigned to a user through both the QoreStor GUI and the command line interface.

Modifying a user through the GUI

To modify user roles through the GUI, complete the following steps.

1. In the left navigation menu, click **Users**.
2. In the list of users, find the user you want to modify. In the **Actions** column, click the ellipsis icon , then click **Edit**. The **Edit User** pane is displayed.
3. Edit the user's **Roles** as required, select from the following options.

 **NOTE:** You can select more than one role for a user.

- **OST**—Designates the user as an OST protocol user.
- **RDA**—Designates the user as an RDA protocol user.
- **Secure connect** - Designates the user as a Secure Connect user.
- **Monitor**—Limits the user to read-only access in the QoreStor GUI.

4. Click **Save**.

Modifying a user through the command line

To modify a user's roles through the command line, complete the following steps:


1. (missing or bad snippet)
2. Modify a user account with the command

```
user --update --name <user name> [--add_roles <cifs|ost|rda|monitor|secure_
connect>] [--remove_roles <cifs|ost|rda|monitor|secure_connect>]
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

Changing a user password

To change a user's password for logging in to QoreStor, including the administrator if you have proper permissions, complete the following steps:

1. In the left navigation menu, click **Users**. The Users page is displayed.
2. In the list of users, find the user you want to modify. In the **Actions** column, click the ellipsis icon , then click **Change Password**.
3. In the **Old password** field, type the current password for the user.
4. In the **New password** field, type the new password.
5. In **Confirm password**, retype the new password to confirm.
6. Click **Save**.


Deleting a user

You can delete a user account from both the QoreStor GUI and the command line interface.

i | **NOTE:** You cannot delete the administrator user.

Deleting a user account through the GUI

To delete a user, complete the following steps:

1. In the navigation menu, click **Users**.
2. In the list of users, find the user you want to delete. In the **Actions** column, click the ellipsis icon , then click **Delete**.
3. When prompted to confirm, click **Remove**.

Deleting a user account through the command line

To delete a user, complete the following steps:

1. (missing or bad snippet)
2. Delete a user account with the command

```
user --delete --name <user name>
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

Managing QoreStor Remotely

QoreStor leverages the Quest Global View Cloud to provide a detailed dashboard of all of the QoreStor and DR Series systems in your organization. With this dashboard, you can easily monitor and manage all of the QoreStor and DR Series systems in your enterprise through one view.

To view QoreStor and DR Series systems on the Global View Cloud, you must register the system with the portal and enable remote management. See the topics below for more information:

- [Registering QoreStor with the Quest Global View Cloud](#)

Getting Started With the Global View Cloud Portal

Before registering your QoreStor system(s) with the Global View Cloud Portal, you must have at least one user account and one organization. Follow the steps below to complete the initial configuration:

1. Access the Global View Cloud Portal at <https://QuestQoreStor.com>.
2. If you have a Quest Support login, enter your user name and password. Otherwise, click **Sign up for a new account** and complete the dialog.
3. On the Global View Portal portal, under **Organizations**, click **Add**.
4. Enter a name for the Organization.
5. Click **Add**.

Registering QoreStor with the Quest Global View Cloud

In order to register your QoreStor or DR Series system with the Global View Cloud Portal, you must have an account on the portal and at least one Organization configured.

To register QoreStor

1. On the Global View Cloud Portal, select the organization to which you want to add a QoreStor system.
2. Click **Register Asset**.
3. Click **Generate registration token**. Click the copy icon to copy the token to your clipboard or other wise record the token.
4. On your QoreStor system navigation menu, click **Management**.
5. In the **Registration** section, read the registration rules and select **I have read and accept the rules**.
6. Click **Register**.
7. Paste or enter the token generated above. Click **Register**.

Enabling Remote Management

Once a QoreStor system is registered with the Global View Portal, you have the option of enabling remote management, which allows management and configuration of a QoreStor system through the Global View Portal.

To enable remote management

1. On your QoreStor system navigation menu, click **Management**.
2. In the **Remote Management** section, click **Enable**.

Viewing and using the GlobalView Cloud Portal

The Global View Cloud Portal displays a convenient view of the operating statistics for all of the QoreStor and DR Series systems that you have added. On this page, you can monitor the status of and easily navigate to the QoreStor and DR Series systems that you have added to the Global View Cloud Portal. Using the portal makes it easy to navigate to a different system in your enterprise without having to log out and log on by using new browser sessions.

To view and use the Global View Cloud Portal, follow these steps.

1. To view the **GlobalView Cloud Portal**, enter the URL (<https://QuestQoreStor.co>) in a supported browser and log in.
2. In the **Organizations** list, click the desired organization. The GlobalView **Assets** page is displayed, showing a summary and a list of assets that have been added to GlobalView.

This list includes all of the systems in GlobalView and provides a high-level status. By default, assets are listed alphabetically by host name. You can sort the list by clicking the column header, which toggles between ascending and descending order. This sort order is retained if you leave the page and return later. The following table describes the information displayed in the asset list.

Column	Description
Asset Type	Describes the type of system (QoreStor or DR Series system) listed.
Host name	Lists the host name of the system
Service tag	For QoreStor systems, this column lists the System ID. For DR Series systems, it lists the Service Tag.
Product model	Lists the model of the asset.

Column	Description
System state	Lists the current state of the system (such as Operational Mode or Manual Intervention Required)
Alerts	Displays the alert count. You can click the number to navigate to the Alerts page.
Diags	Displays the number of generated diagnostic bundles available.

- To view more detailed information on a specific system, click **Details**. This action provides the following views:

View	Description
Dashboard	Provides a condensed view of the QoreStor dashboard containing charts for Capacities, Storage savings, Throughput, and System usage . The charts can be configured to show data for the previous three hours, the previous day, week or month, or for a custom date range.
Storage Groups	Lists the configured storage groups and containers and key data points for each.
Alerts	Lists generated alerts
Diagnostics	Provides details about generated diagnostic bundles as well as a direct download link.

- To manage a QoreStor system, find the system in Global View Cloud Portal **Assets** page. Click **Manage**. A cloud-enabled version of the QoreStor UI will be displayed, providing management and configuration options as documented in this *User Guide*.

i **NOTE:** Remote Management must be enabled on each QoreStor system before you can manage the system through the GlobalView Cloud Portal. Refer to [Enabling Remote Management](#) for information.

Monitoring QoreStor

This topic describes how you can monitor the current state of QoreStor operations on the **Dashboard** page.

Using the Dashboard page

The Dashboard page contains graphics that show key information about the current state of your QoreStor instance. This page automatically refreshes every 30 seconds.

To use the Dashboard page, follow these steps.

1. Click **Dashboard** in the navigation menu of the QoreStor GUI.
2. You can view the following graphs:
 - **Compression**—displays a total compression in percentage (combining both deduplication and compression) over a time period (for example, every hour, which is the default).
 - **Swap memory Usage**—displays the amount of swap memory used.
 - **Physical Capacity**—displays total used space, free space, and used and encrypted space in GBs and TBs.
 - **Network throughput**—displays performance information for the configured NICs.
 - **Throughput**—displays the throughput volume (reads and writes) in Mebibytes/second (MiB/s) based on time (for example, every hour, which is the default).
 - **Storage capacity**—displays the amount of used and free storage space.
 - System Information—displays information on the QoreStor system, including:
 - System State
 - Hostname
 - System ID
 - Dictionary Type
 - Number of Storage Groups
 - Number of Containers
 - Operating System
3. At the top of the Dashboard page, you can also view the System Summary section, which lists key information about the current QoreStor system, including:
 - **Cleaner status**—The current cleaner status as one of the following states:
 - **Pending**—displayed when there is any scheduled window set and the current time is outside the scheduled window for the Cleaner operation.
 - **Running**—displayed when the Cleaner operation is running during a scheduled window.
 - **Idle**—displayed only if there is no Cleaner operation running during a scheduled window.
 - **Total number of files in all containers**
 - **Current savings**
 - **Number of containers**
 - **Capacity used**
 - **Number of Storage Groups**
 - **Physical Capacity**
4. To change the time display in the graphs, click **History** within the graph you want to view, and then select the time increment to view.

Viewing QoreStor statistics by using the CLI

An alternate method for viewing the current QoreStor statistics is by using the QoreStor CLI command: `stats --system`. This command shows the following categories of system statistics:


- Capacity Used
- Capacity Used in GB
- Capacity Free
- Capacity Free in GB
- Cloud Capacity Used
- Cloud Capacity Used in GB
- ObjectDirect Capacity Used
- ObjectDirect Capacity Used in GB
- Archive Capacity Used
- Archive Capacity Used in GB
- Metadata Used
- Metadata Used in GB
- Reserve Space
- Reserve Space in GB
- Total Capacity
- Total Capacity in GB
- Licensed Capacity
- Licensed Capacity in GB
- Read Throughput
- Write Throughput
- Current Files
- Current Files Stubbed
- Modified Files Uploaded to Cloud
- Modified Files Uploaded to Archive
- Current Bytes
- Current Stubbed Bytes
- Current Local Bytes
- Post Dedupe Bytes
- Post Compression Bytes
- Post Encryption Bytes
- Post Encryption Bytes in GiB

- Cleaner Status
- Compression Status
- Total Inodes
- Bytes decrypted
- Dedupe Savings
- Compression Savings
- Total Savings
- Local Dedupe Savings
- Local Compression Savings
- Local Total Savings

For more information on QoreStor CLI commands, see the *QoreStor Command Line Reference Guide*.

Monitoring system alerts

You can easily view current system alerts and events in the QoreStor GUI.

- To view system alerts, click the **Alerts** icon  in the header pane. The Alerts drawer displays the active alerts.

i | **NOTE:** For a detailed list of possibly occurring alerts, see the topic, “QoreStor system alert and event messages,” in the “Support, maintenance, and troubleshooting” chapter of this guide.

Monitoring clients

You can easily view the current clients that are connected to the QoreStor system. Client information can be viewed through the System Configuration page in the QoreStor GUI, or using the QoreStor CLI. .

Monitoring clients through the QoreStor GUI

1. To view client information for QoreStor, on the navigation menu, click **System Configuration**. The total number of currently active clients for a particular type is displayed at the bottom of the page.
2. Client information is grouped by client type (RDA/OST, NFS/CIFS, NDMP, iSCSI, or FC). To view client information, click the appropriate pane to view information for that client type.

Monitoring clients through the QoreStor CLI

You can monitor client status through the CLI by using either the **rda** or **ost** commands.

To monitor clients, complete the following steps:

1. (missing or bad snippet)
2. View client information with the appropriate client command

```
stats -clients[--type <NFS|CIFS|OST|RDS|NDMP|ISCSI|FC>]
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

Monitoring system events

You can easily view and filter current system events in the QoreStor GUI. To monitor QoreStor events, follow these steps:

1. In the navigation menu, click **Events**.
The Events page displays a summary table of events listed by index number, severity (Informational, Warning, or Critical), timestamp of the event, and brief message describing the event.
2. To filter the list of events, do any of the following:
 - In the **Date Range** field, click to select a range of dates.
 - In the **Message** field, enter a word or string of words for which to search in Event messages. (The system is not case-sensitive)
 - In the Filter Events field, select the severity level for which to search as **Info**, **Warning**, or **Critical**.
 - Click **Filter**. Search results appear in the Events summary table.

Support, maintenance, and troubleshooting

The QoreStor GUI provides various information and tools that can help you better understand the current state of your system and that provide basic, support, maintenance, and troubleshooting functionality.

Using QoreStor Diagnostics

In the QoreStor GUI, the **Diagnostics** page provides the ability to generate and view diagnostics bundles used by Quest Support to troubleshoot QoreStor problems.

Viewing system diagnostic log files

A QoreStor system diagnostics log file is a bundle that contains a variety of file types that record the latest system settings and saves them in a compressed .zip file format.

In the QoreStor system GUI, the **Diagnostics** page allows you to generate diagnostic logs that capture the state of your system. You can also download these log files or delete them as needed.

To view the system diagnostics page, follow these steps.

1. In the navigation menu, click **Diagnostics**.
2. You can view the following columns of information on the **Diagnostics** page for the diagnostics logs that have been generated.
 - **File name**—in this format, `<hostname>_<date>_<time>.lzip`, as in this example: **acme-sys-19_2012-10-12_13-51-40.lzip**
 - **NOTE:** Diagnostic log file names are limited to 128 characters.
 - **Size**—in Megabytes.
 - **Path**—The location to which the diagnostics bundle is saved.
 - **Download**—Use this icon to download the diagnostics bundle.

Understanding diagnostics collection

The Diagnostics function in the QoreStor system lets you collect and manage your system's diagnostic log file bundles. The Diagnostics function works by collecting all the system-related information that could help when diagnosing a problem or error condition in the system. Each diagnostic log file bundle provides:

- A current snapshot of system operations
- System-related information that assists in understanding system operations
- A record of system operations in case Technical Support needs to provide technical assistance

Diagnostics bundles are generated when a QoreStor CLI or GUI request is made by the administrator (and the default reason that is listed is admin-generated).

When the diagnostics log directory exceeds the maximum storage capacity, any log older than one hour is automatically deleted. QoreStor GUI lets you download and save diagnostics log files to other systems on your network. QoreStor also maintains a separate archive logs directory that collects other system-related information, and these archive logs are also automatically deleted when they exceed a maximum capacity. When you generate a diagnostics log file bundle, it contains all of the QoreStor information that you need when contacting Technical Support for technical assistance. . When a diagnostics log file bundle is generated, this process also collects all the previous auto-generated diagnostics and deletes them from the system.

The QoreStor GUI provides options to display existing diagnostics logs, generate new diagnostics logs, download and save copies of existing diagnostics logs, or delete existing diagnostics logs. The QoreStor CLI also provides the means for managing, generating, or downloading the diagnostics log files. For more information, see the *QoreStor Command Line Reference Guide*.

Generating a diagnostics log file

A QoreStor diagnostics log file is a bundle that contains a variety of file types that record the latest system settings, and saves them in a compressed .lzip file format. When you generate a diagnostics log file bundle, it contains all of the QoreStor information that may be needed when contacting Technical Support for technical assistance. This also includes all the previous auto-generated diagnostics log files, which are then deleted from the QoreStor system.

Generating a diagnostics file through the GUI

To generate a diagnostics log file bundle for your system, complete the following steps:

1. In the left navigation menu, click **Diagnostics**.
2. On the right side of the page, click **Generate Diagnostics**.

Once completed, the new diagnostics log file resides at the top of the **File Name** column in the table. To verify, check its timestamp (using its date and time), to ensure this is the latest diagnostics file created.

Generating a diagnostics log file through the command line

To generate a diagnostics log file bundle for your system, complete the following steps:

1. Access your system's command line interface. QoreStor commands are located in the `/opt/qorestor/bin` directory. Either change directories to the appropriate location, or add the appropriate location to your system path.

2. Generate a diagnostics log file with the command

```
maintenance --diags --collect
```

Refer to the *QoreStor Command Line Reference Guide* for more information.

Downloading diagnostics log files

To download an existing diagnostics log file, complete the following steps:

1. In the left navigation menu, click **Diagnostics**.
2. In the list, select the diagnostics log file you want to download, and click the **Download** icon.
3. Download and save the file as needed.

Deleting a Diagnostics Log File

To delete an existing diagnostics log file from the Diagnostics summary table on the Diagnostics page, complete the following:

1. Select **Diagnostics**.
2. Click **Select** to select the diagnostics file you want to delete, and click **Delete**.
3. Click **OK** to delete the selected diagnostics log file (or click **Cancel** to display the **Diagnostics** page).

Troubleshooting error conditions

To troubleshoot error conditions that disrupt your normal QoreStor operations, complete the following:

1. Generate a QoreStor diagnostics log file bundle if one has not already been automatically created. For more information, see [Generating a diagnostics log file](#) .
2. Check the system alert and system event messages to determine the current status of your QoreStor system.
3. Verify if the QoreStor system has recovered or whether it has entered into Maintenance mode.
4. If you cannot resolve the issue using the information in this QoreStor documentation, contact Quest Technical Support.

About us

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product