Quest® QoreStor™ 5.1.0

User Guide

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.**

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

QoreStor User Guide
Updated - March 2019
Version - 5.1.0

Contents

Introducing the Quest® QoreStor™ documentation 8

Understanding the QoreStor documentation 8

Other information you may need 8

Information on compatible products 9

Source code availability 10

Introducing Quest® QoreStor™ 11

QoreStor data storage concepts 12

Data deduplication and compression 12

Encryption at rest 12

Streams and connections 12

Secure connect 13

Replication 13

Reverse replication 14

Reverse replication: alternate method 15

Supported file system protocols 15

CIFS 16

CIFS ACL support 16

NFS 17

Rapid NFS and Rapid CIFS benefits 17

Rapid NFS and Rapid CIFS 17

RDA with Quest's Netvault Backup and vRanger 18

RDA with OST for QoreStor 18

Software components and operational guidelines 19

NDMP 20

iSCSI 20

Fibre channel 21

QoreStor processes 21

Accessing QoreStor 23

Networking prerequisites for QoreStor 23

Configurations required when using proxy servers 24

Logging onto the system GUI for the first time 24

Enabling active scripting in IE 24

Disabling the Compatibility View settings for IE 25

Configuring QoreStor with the Configuration Menu 25

Initial login and changing your password 26

Initial network configuration 26

Using the QoreStor Menu 26

QoreStor Administration 28
QoreStor Maintenance 29
QoreStor Statistics 30
Using the QoreStor command line 30

Configuring QoreStor settings 32
Licensing QoreStor 32
Evaluating QoreStor 32
Viewing your license configuration 33
Installing a license 33
Configuring an SSL certificate for your QoreStor system 34
Installing an SSL certificate 34
Restoring the default certificate 34
Understanding system operation scheduling 34
Configuring cleaner schedules 35
Viewing cleaner status 36
Viewing cleaner statistics 37
Configuring replication schedules 38
Configuring Secure Connect 38
Enabling Secure Connect 38
Configuring Secure Connect properties 39
Managing Secure Connect with plug-in 4.1.0.265 40
Checking Secure Connect status 41
Disabling Secure Connect 41
Enabling Secure Connect 41
Adding certificates for Secure Connect 42
Adding a Secure Connect certificate - Windows Client 42
Adding a Secure Connect certificate - Linux Client and QoreStor server 43
Configuring email alert settings 44

Managing storage groups 46
Viewing storage group information 46
Adding a storage group 47
Adding a storage group through the GUI 48
Adding a storage group through the command line 49
Modifying a storage group 49
Deleting a storage group 50
Deleting a storage group from the GUI 51
Configuring additional storage 51
Guidelines for configuring additional storage 51
Adding additional storage 51

Managing containers 53
Viewing containers 53

Viewing containers in the GUI 53
Viewing containers via the CLI 54
Viewing container statistics 54
Displaying container statistics by using the CLI 55
Creating a container 55
Creating an OST or RDS connection type container 56
Creating an NFS or CIFS connection type container 57
Creating a VTL type container 59
Viewing VTL tape information 63
Deleting a container 64
Deleting a container through the GUI 64
Deleting a container through the command line 64

Managing replications 65
Guidelines and prerequisites for replication 65
Replication seeding 66
Viewing replication information 66
Adding replication relationships 67
Modifying replication relationships 68
Deleting replication relationships 69
Starting and stopping replication 69

Managing users 70
Viewing users 70
Viewing users through the GUI 70
Viewing users through the command line 71
Adding a user 71
Adding a user through the GUI 71
Adding a user through the command line 72
Modifying user roles 72
Modifying a user through the GUI 72
Modifying a user through the command line 73
Changing a user password 73
Deleting a user 73
Deleting a user account through the GUI 74
Deleting a user account through the command line 74

Managing QoreStor Remotely 75
Getting Started With the Global View Cloud Portal 75
Registering QoreStor with the Quest Global View Cloud 75
Enabling Remote Management 76
Viewing and using the GlobalView Cloud Portal 76

Monitoring QoreStor 78
Using the Dashboard page 78
Viewing QoreStor statistics by using the CLI 79
Monitoring system alerts 80
Monitoring clients 80
Monitoring clients through the QoreStor GUI 80
Monitoring clients through the QoreStor CLI 80

Configuring and using Rapid NFS and Rapid CIFS 81
Rapid NFS and Rapid CIFS benefits 81
Best practices: Rapid NFS 81
Best practices: Rapid CIFS 83
Installing the Rapid NFS plug-in 84
Installing the Rapid CIFS plug-in 85
Monitoring performance 86
Uninstalling the Rapid NFS plug-in 86
Uninstalling the Rapid CIFS plug-in 87

Configuring and using VTL 88
Understanding VTL 88
Terminology 88
Supported virtual tape library access protocols 88
NDMP 89
iSCSI 89
Fibre channel 89
VTL and QoreStor specifications 89
Guidelines for configuring VTL 91
Plan your Environment 91
Create Containers of Type VTL 91
Authentication/User Management Considerations 92
Verify the Tape Library Creation 92
Configure the Library in the DMA 92

Configuring and Using Encryption at Rest 93
Understanding Encryption at Rest 93
Encryption at Rest Terminology 93
Encryption at Rest and QoreStor Considerations 94
Understanding the encryption process 95

Support, maintenance, and troubleshooting 97
Using QoreStor Diagnostics 97
Viewing system diagnostic log files 97

Understanding diagnostics collection 98
Generating a diagnostics log file 98
Downloading diagnostics log files 99
Deleting a Diagnostics Log File 99
Troubleshooting error conditions 99
About us 101
Technical support resources 101

1

Introducing the Quest® QoreStor™ documentation

The Quest® QoreStor™ documentation contains topics that describe how to perform data storage operations and to manage storage containers.

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.

> **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	Decribes 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.

> **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.

> **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.

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.

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.

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.

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.

> **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 protocols and is fully handled by QoreStor.

For VTL type containers, replication is done at the cartridge level, and the system replicates the media/tape cartridges from a source QoreStor or DR Series system to a target QoreStor . The media is replicated to the target with the same markers. This condition restores successfully for a multi-domain environment; however, if the source and target are in the same domain, the media must be re-serialized on the target side once replication completes to successfully restore. This requires you to activate the VTL container, and change the bar codes of the tapes on the target DMA.

While replication of NFS, CIFS, Rapid NFS or Rapid CIFS containers is managed by QoreStor, RDA with OST, RDA with NetVault Backup, and RDA with vRanger container replication is handled by the media servers of the respective Data Management Applications (DMAs).

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.

> **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 forQoreStor 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.

> **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.

> **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.

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)
  - Fibre Channel (FC)

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.

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

> **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.

> **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.

> **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.

> **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`

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 Installation 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

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 .

Fibre channel

Fibre Channel (FC) is a high-speed network technology primarily used to connect computer data storage to servers in storage area networks (SAN) in enterprise storage. Fibre Channel networks are known as a Fabric because they operate in unison as one big switch. Fibre Channel mainly runs on optical fiber cables within and between data centers. Virtual tape libraries (VTLs) can ingest data over a Fibre Channel interface, which enables seamless integration with many existing backup infrastructures and processes.

The QoreStor VTL container type is designed to work seamlessly with the FC interface. With FC, QoreStor can direct attach to NAS filers or Fibre Channel switches and supports SAN devices.

A FC VTL container on a QoreStor system supports multiple initiators, making it possible for the VTL to be shared across multiple clients of a Data Management Application (DMA).

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.
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.
sc_server	A Secure Connect server that handles secure connects from OST and RDA plug-ins
oca_idm_eda	An event and data aggregator service for events and alerts.
ocardslogwriter	Process captures logging from all the processes, writes the data to the corresponding logs, and rotates the logs.
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.
ocamonitor	QoreStor process for periodically collecting stats from ocafsd, ocaconfigsvc and Linux system monitoring tools and populating an internal (r3) database.

ocahttp	QoreStor HTTP server to service requests for QoreStor web UI and REST API methods. Uses ocafsd, ocaconfigsvc and r3 database (graphs).
ocaagent_charts	Periodically (every hour) sends QoreStor chart related data to the Global View Cloud.
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.
ocaagent_diagnostics	Periodically queries database for keep-alive commands. Responsible only for handling diagnostic upload command.
ocaagent_keepalive	Queries the Global View Cloud for keep-alive commands (diagnostic upload and portal unregistration) and executes them. This query occurs once a minute.

3

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"
```

> **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

     > **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*.

     > **NOTE:** For best results when using IE web browsers in combination with supported Windows-based servers, ensure that Active Scripting (JavaScript) is enabled on the Windows client. This setting is often disabled by default on Windows-based servers. For more information on enabling Active Scripting, see the topic Enabling Active Scripting in Windows IE Browsers.
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.

Enabling active scripting in IE

To enable Active Scripting (JavaScript) in Microsoft Windows Internet Explorer (IE) web browsers, complete the following steps:

ℹ NOTE: This procedure describes how to configure your Windows IE web browser to enable Active Scripting (JavaScript). This setting is often disabled by default on Windows-based servers.

1. Launch the IE web browser, and click **Tools** → **Internet Options**.
2. Click the **Security** tab, and click **Custom level…**.
3. Using the right scroll bar, scroll down the **Settings** choices until you reach **Scripting**.
4. In **Active scripting**, click **Enable**.
5. Click **OK** to enable JavaScript and the **Active Scripting** feature for your web browser.
6. Click **OK**.

Disabling the Compatibility View settings for IE

To disable the Compatibility View settings of the IE web browser, complete the following steps:

ℹ NOTE: This procedure describes how to disable the Compatibility View settings to ensure there is no conflict between different versions of the Microsoft Internet Explorer (IE) web browser you use to access the QoreStor GUI. Disabling the compatibility view settings requires that the **Display all websites in Compatibility View**check box option in the **Compatibility View Settings** page is cleared, and that there are no QoreStor instances or domains associated with these systems listed in the Compatibility View list on this page.

1. Launch the IE web browser, and click **Tools**→ **Compatibility View settings**.
2. If selected, clear the **Display all websites in Compatibility View** check box option.
3. If any QoreStor systems are listed in the **Compatibility View** list, select the entry and click **Remove**.
4. Click **Close**.

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 Installation 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. Using the terminal emulation application of your choice, log on to the QoreStor server 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). (missing or bad snippet).

   > **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-menues, 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	• 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	Displays the current storage configuration for each filesystem, including: • size • used space • available space • used percentage • mount path
Storage Layout	Displays the layout per storage device, including: • Device name • Filesystem type • Mountpoint • UUID • Schedule • Model
Administration	Provides options to configure networking, storage, application and operating system configurations. Refer to the section QoreStor Administration
System Info	Displays information about the QoreStor system, including: • output of the QoreStor system --show command • Management user interface information and credentials • license information
QoreStor	Provides access to QoreStor filesystem maintenance utilities and diagnostic management.

Maintenance	Refer to QoreStor Maintenance for more information.
QoreStor Stats	Provides access to QoreStor system statistics. Refer to QoreStor Statistics for more information.
QoreStor CLI	Allows access to the QoreStor CLI commands using the **qsadmin** account. Refer to the *QoreStor Command Line Reference Guide* for more information. To return to the QoreStor Menu from the CLI, type **exit** at the prompt. IMPORTANT: You must be logged in as the **qsadmin** account when executing QoreStor commands.
Service Shell	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. 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 `#sudo su - qsadmin` or **exit** to the QoreStor menu and select **QoreStor CLI**.

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 download the Qorestor update package, and update QoreStor if the package is valid.
QoreStor Features	Provides options to tune system performance: • **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.
Operating System	Provides options to **update**, **restart**, and **shutdown** the operating system.).
Troubleshooting tools	Provides tools to troubleshoot your QoreStor machine. Consult the documentation for each utility for more information. • **EPEL Repositor**y - 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. • **iotop** - 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. NOTE: To return to the Troubleshooting tools menu from the selected monitoring tool, press **q** to quit**.**
Color theme	Provides options to change the color theme settings.

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	• Diagnostics Show • Diagnostics Collect • Diagnostics Delete • Diagnostics Delete All

Maintenance Filesystem	- 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

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.

To access the command line interface for QoreStor:

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

4

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.
- > **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.

> **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*.

> 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 Configuration**
2. Scroll to the **License Information** section at the bottom of the page to view detailed information about your configured license.

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 Configuration**
2. Scroll to the **License Information** section at the bottom of the page.
3. Click **Upload License**.
4. Click **Choose File** and select the license file. Click **Open**.
5. Click **Apply**.

> 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.

Installing an SSL certificate

To install an SSL certificate, complete the following steps:

1. In the navigation menu, click **System Configuration**. Click **Upload Certificate**.
2. Click **Choose cert file** and select the SSL certificate on your system that you want to install.
3. Click **Choose key file** and select your private key.
4. Click **Apply**.
5. Click either the page reload icon or the back-arrow on the browser to restore the page.

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**.

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)

  > 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.

> 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 on the System Configuration page of the QoreStor GUI, or via the QoreStor command line interface, using the **schedule** command:

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

The **Replication** schedule can be viewed 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

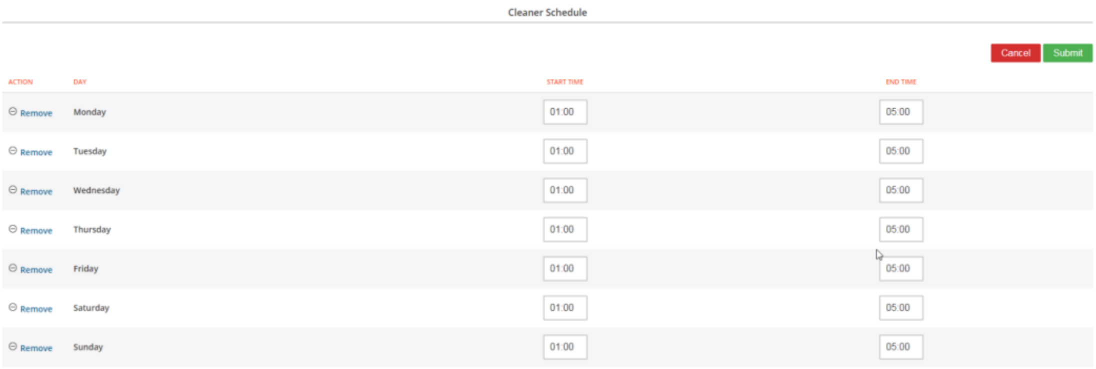
Performing scheduled disk space reclamation operations are recommended as a method for recovering disk space from the system. The recommended method is to schedule a time when you can run the Cleaner on your QoreStor system with no other planned processes running.

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 **System Configuration** . In the Cleaner Schedule pane, click **Edit Schedule**.
   The schedule lists a **Start Time** and **End Time** for each day of the week.



ACTION	DAY	START TIME	END TIME
⊖ Remove	Monday	01:00	05:00
⊖ Remove	Tuesday	01:00	05:00
⊖ Remove	Wednesday	01:00	05:00
⊖ Remove	Thursday	01:00	05:00
⊖ Remove	Friday	01:00	05:00
⊖ Remove	Saturday	01:00	05:00
⊖ Remove	Sunday	01:00	05:00

2. For any day on which you do not want the Cleaner to run, click **Remove** in the **Action** colum.
3. For remaining days, edit the **Start Time** and **End Time** to set the Cleaner window.
4. 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:

> 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.
>
> 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

The current Cleaner Status is shown in the status pane at the top of the QoreStor UI as one of the three following states:

- **Pending**—displays any scheduled window for the Cleaner operation.
- **Running**—displays when the Cleaner operation is running.

- **Done**—displayed only if there is no Cleaner operation required.

On the **System Configuration** 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 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, 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.

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 plug-in version 4.1.0.265
  - Managing Secure Connect with plug-in 4.1.0.265
- For plug-in versions prior to 4.1.0.265
  - Enabling Secure Connect
  - Configuring Secure Connect properties
- Adding certificates for Secure Connect

Enabling Secure Connect

> i **IMPORTANT:** The procedure below is for plug-in verisons 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 plug-in 4.1.0.265.

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 failback 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.

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 failback 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.

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:

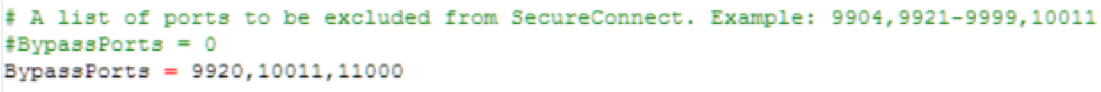
- 9443 - this is the listening port. The Secure Connect server listens for connection requests on this port.
- 10011, 11000 and 9920 - These are the standard Secure Connect communication ports.

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 plug-in 4.1.0.265

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.propertie**s file. By default this is:

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

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
   ```

Enabling Secure Connect

To enable Secure Connect

1. Execute the sc_manager disable 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
   ```

Adding certificates for Secure Connect

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

> **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.

> **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.

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

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, peform 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**.

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

5

Managing storage groups

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 **Storage Groups** in the QoreStor navigation bar.

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 **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. To view a chart of throughput activity and detailed storage group statistics, select a storage group, and, in the Actions column, click the Chart icon. A page for the selected storage group is displayed, showing the following:
   - 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)
   - Statistics—Lists the following statistics for the storage group.
     - Capacity Used
     - Capacity Used in GB
     - Current Files
     - Post Dedupe Bytes
     - Post Encryption Bytes
     - Bytes Decrypted
     - Compression Status
     - Dedupe Savings
     - Total Inodes
     - Capacity Free
     - Capacity Free in GB
     - Current Bytes
     - Post Compression Bytes
     - Post Encryption Bytes in GiB
     - Cleaner Status
     - Encryption Status
     - Compression Savings
     - Total Savings

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 **Storage Groups**.
2. On the right side of the page, 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. For Storage Optimization, 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. 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.

     > 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.

   > NOTE: Refer to Configuring and Using Encryption at Rest for more information about encryption.

   > 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

   > 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.**

6. 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>]
   ```

   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*.

   > **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

   > **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.

   > **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 **Storage Groups**.
2. In the **Storage Group** list, select a storage group, and, in the **Actions** column, click **Edit**.
3. For Storage Optimization, select a **Compression Level** 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.
4. Click **Next**.

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 **Next**.
7. Review the Storage Group summary, and then click **Save**.

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>]
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 **Storage Groups**.
2. In the list of storage groups, select a storage group, and, in the **Actions** column, click **Remove**.

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

3. When prompted to confirm, click **Remove.**

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 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.

- QoreStor supports a maximum of 5 enclosures (1 internal plus 4 expansion)
- 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. On the navigation menu, click **System Configuration**. Scroll to the **Storage Enclosure** section.
2. Click **Add Path.**
3. Enter the mount path for the additional storage. Click **Add**.

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 **Storage Groups**, and then select the storage group that has the containers you want to view. (If you only have the DefaultGroup storage group, you will not need to select a group.) The Containers page is displayed.

2. You can view the following columns of information about the containers.
   - **Storage Group**—The storage group to which the container belongs.
   - **Container**—The name of the container.
   - **Marker Type**—The marker type that supports your Data Management Application (DMA).
   - **Access Protocol**—the connection type/access protocol for the container:
     - NFS
     - CIFS
     - RDA
     - OST

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. On the navigation menu, click **Storage Groups**, and then select the storage group that contains the container you want to view. (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 for which you want to view statistics, and then click **Container details**.
3. The **Container details** page contains the following sections:
   - In the **Active** and **Throughput** charts, you can view current statistics for the container. The **Active** chart displays the number of active files ingested based on time (in minutes), and 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).

     NOTE: The values in the Active 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
  - Quota
  - Used Capacity
- In the **Quota and duplication** pane, you can view detailed information on the capacity, inbound throughput, and outbound throughput.
- The **Client statistics** 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 storage groups

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

Containers can be accessed using the following connection types:

- **NFS**
- **CIFS**

- **RDA** (Rapid Data Access)
    - **OST** (OpenStorage Technology)
    - **RDS** (Rapid Data Storage)

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 OST or RDS connection type container

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

1. On the navigation menu, click **Storage Groups**, and then select the storage group for which you want to create a container. (If you are only using the DefaultGroup storage group on your QoreStor system, you do not need to select a group.)
2. In the storage group list, click the storage group to which you want to add a container. 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. For **Protocol**, select **Rapid Data Storage (RDS)** or **OpenStorage (OST)** as appropriate.
5. Click **Next**.
6. If you selected **RDS**, **LSU Capacity** is set to **Unlimited** by default. If you selected Symantec 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.
7. Click **Finish**.

> 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.

Creating an NFS or CIFS connection type container

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

1. On the navigation menu, click **Storage Groups**, and then select the storage group for which you want to create a container. (If you are only using the DefaultGroup storage group on your QoreStor system, you do not need to select a group.)
2. In the storage group list, click the storage group to which you want to add a container. 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. For Access Protocol, select **NAS**.
5. Click **Next**.
6. 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.

   > **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.

7. 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.)
8. Click **Next**.
9. If you selected NFS as the connection type, configure NFS access as follows.
   - **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.
   - **Map Root To** — Select one of the following options from the drop-down list to define the user level you want mapped to this container.
     - **Nobody** — to specify a user on the system without root access permissions.
     - **Root** — to specify a remote user with root access to read, write, and access files on the system.
     - **Administrator** — to specify the system administrator.
   - **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.)
10. 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.)

    > **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.*
11. Click **Next**.
    A Configuration Summary of the options you selected for creating the container appears.
12. Click **Finish**.

Creating a VTL type container

> 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.

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

1. On the navigation menu, click Storage Groups, and then select the storage group for which you want to create a container. (If you are only using the DefaultGroup storage group on your system, you do not need to select a group.)
2. In the Action menu in the upper right corner of the page, click **Add Container**.
3. For **Name**, type the name of the container.

   > 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

   > 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 **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.

   > NOTE: The Quest version of the VTL issupported 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

   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 **VTL 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:

    > 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.

- **FC**
  - 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.
  - Enter the **targetWWN** and **initiatorWWN**.
- **No Access.**

> **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. On the **Storage Groups** page in the list of containers, expand the Storage Group that contains VTL container for which you want to view detailed information.
2. In the list of containers in the selected storage group, find the desired VTL container and click **Container Details**.

3. 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

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. Access the QoreStor CLI. Refer to Using the QoreStor command line for more information.
2. Delete a container with the command

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

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

7

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.

> 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.

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 **Replication.** The list of configured replications is displayed, including the following information:
   - **Source**—The name of the source container (with IP address or hostname)
   - **Status**—The status of the source container.
   - **Replica**—The name of the target container in the replication process (with IP address or hostname)
   - **State—**The state of the replica container.
   - **Average Throughput**— the average replication throughput in KiB/s

- **Dedupe Network Savings**— the estimate reduction in data replicated achieved through QoreStor deduplication.

2. To view the following detailed replication information about the source and target, click a selected replication in the list to expand it. The information below is displayed:
   - Role— Whether the current QoreStor serves as the source or target for the replication.
   - Replication Source Container
   - Replication Target Container
   - Replication Target System
   - Peer Status—Displayed as Online, Offline, Paused, or Disconnected. When replication is started, the Peer Status displays the status as Online for the selected container. When stopped, the Peer Status initially displays the status as Paused, and then changes to Offline.
   - Replication State—The current peer status as In sync, Paused, or Replicating.
   - Schedule Status
   - Replication Average Throughput
   - Replication Maximum Throughput
   - Network Average Throughput
   - Network Maximum Throughput
   - Network Bytes Sent
   - Pending Bytes
   - Dedupe Network Savings
   - Compression Network Savings
   - Last INSYNC Time—The last time the system synchronization occurred.
   - Estimated Time to Sync

   NOTE: These statistics refresh every 30 seconds.

Adding replication relationships

To add a new replication relationship, complete the following steps.

1. In the navigation menu, click **Replication.**
2. In the upper right corner of the page, 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 System**—enter the domain name of the remote system.
     - Click **Retrieve Remote 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: **Not Enabled**, **AES 128–bit**, or **AES 256–bit**.
5. Under **Replica Container**, define the target replica container by configuring the following settings.
   - **Username**—enter the username for the remote system.

     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 **Remote Container**—Select the remote container from the drop-down list.
6. Click Next.
7. Review the summary and click **Finish**.

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.

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.

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.**

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. From the list, select the replication relationship that you want to modify, and click to expand the details.

3. Click the **Edit** icon and then, in the **Edit Replication** pane, modify the settings/values for the **Source**, or **Replica** 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**.

    > **NOTE:** Replication needs to be stopped before the encryption settings can be modified.

4. Click **Save**.

Deleting replication relationships

To delete an existing replication relationship, complete the following steps:

1. In the navigation menu, click **Replications**.
2. From the list, select the replication relationship that you want to delete, and click to expand the details.
3. Click the **Delete** icon and then, 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. From the list, select the replication relationship that you want to start or stop, and click to expand the details.
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.

8

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, 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**.

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. Access the QoreStor CLI. Refer to Using the QoreStor command line for more information.
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.
   - **User Type**— Select either **User** or **Monitor**. The Monitor user type is for a monitor role that can only access the UI in read-only mode. For users that need protocol access, select **User**.
   - **Username**—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.

4. For **Roles**, select from the following options.

   > **NOTE:** You can select more than one role for a user.

   - **Monitor**—Limits the user to read-only access in the QoreStor GUI.
   - **CIFS**—Designates the user as a CIFS protocol user.
   - **RDA—**Designates the user as an RDA protocol user.
   - **OST—**Designates the user as an OST protocol user.
   - **NDMP—**Designates the user as an NDMP protocol user.
   - **iSCSI**—Designates the user as an iSCSI protocol user.
   - **Secure connect** - Designates the user as a Secure Connect user.

5. Click **Create**.

Adding a user through the command line

To add a user through the command line, complete the following steps:

1. Access the QoreStor CLI. Refer to Using the QoreStor command line for more information.
2. Add a new user account with the command

   ```
   user --add --name <user name>
   ```

3. To define roles for the new user, use the command

   ```
   user --update --name <user name> [--add_roles <cifs|ost|rda|monitor|secure_
   connect>]
   ```

   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, select the user you want to modify, and, in the **Actions** column, click the **Edit** icon. 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.

   - **Monitor**—Limits the user to read-only access in the QoreStor GUI.
   - **CIFS**—Designates the user as a CIFS protocol user.
   - **RDA—**Designates the user as an RDA protocol user.
   - **OST—**Designates the user as an OST protocol user.
   - **NDMP—**Designates the user as an NDMP protocol user.
   - **iSCSI**—Designates the user as an iSCSI protocol user.
   - **Secure connect** - Designates the user as a Secure Connect user.
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. Access the QoreStor CLI. Refer to Using the QoreStor command line for more information.
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, select the user you want to modify, and, in the **Actions** column, click the Change Password icon (which looks like a key). The **Edit User** pane is displayed.
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.

> 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, select the user you want to delete, and, in the **Actions** column, click the **Delete** icon.
3. When prompted to confirm, click **Remove**.

Deleting a user account through the command line

To delete a user, complete the following steps:

1. Access the QoreStor CLI. Refer to Using the QoreStor command line for more information.
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 a 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	Lists the model of the asset.

Column	Description
model	
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.

3. 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.

4. 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.

9

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:
   - **Physical Capacity**—displays total used space, free space, and used and encrypted space in GBs and TBs.
   - **Storage Savings**—displays a total savings in percentage (combining both deduplication and compression) over a time period (for example, every hour, which is the default).
   - **Throughput**—displays the throughput volume (reads and writes) in Mebibytes/second (MiB/s) based on time (for example, every hour, which is the default).
   - **System Usage**—displays information about memory and CPU usage.
   - **Network Interfaces**—displays performance information for the configured NICs
   - **Number of RDA Connections**—displays information about the number of RDA connections made to the QoreStor server.

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**

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 (system capacity used in Gibibytes or GiBs)
- Capacity Free (system capacity free in GiBs)
- Read Throughput (read throughput rate in Mebibytes or MiB/s)
- Write Throughput (write throughput rate in MiB/s)
- Current Files (current number of files in system)
- Current Bytes (current number of ingested bytes in system)
- Post Dedupe Bytes (number of bytes after deduplication)
- Post Compression Bytes (number of bytes after compression)
- Post Encryption Bytes
- Post Encryption Bytes in GiB
- Cleaner Status (current space reclamation process status)
- Compression Status (current compression status)
- Total Inodes (total number of data structures)
- Bytes decrypted
- Dedupe Savings (deduplication storage savings by percentage)
- Compression Savings (compression storage savings by percentage)
- Total Savings (total storage savings by percentage)

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 monitor system alerts, on the navigation menu, click **Alerts**.
  The Alerts page displays a summary table of alerts listed by index number, timestamp of the system alert, and a brief message describing the alert.

  > 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. Access the QoreStor CLI. Refer to Using the QoreStor command line for more information.
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.

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 (such as Veritas products), 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, hpdp, 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

> **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/openv/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
```

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.

After it is downloaded, follow the steps that follow to run the Plug-In Installer to install the plug-in on your designated Linux-based media server.

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

1. Download `QuestRapidNFS-xxxxx-xxxxx-x86_64.bin.gz` from the website, as detailed previously.
2. Unzip the package.

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

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

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

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

   ```
   QuestRapidNFS-xxxxx-xxxxx-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 10.222.322.190:/containers/backup/mnt/backup
   ```

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

   > **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.

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.

> **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-xxxxx.msi.`
5. Follow the installation prompts.

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\rdcifsctl.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.

> 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
   ```

   > **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 Statisticspage.

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*.

```
rdcifsctl.exe driver -d
```

> **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)
- Fibre Channel (FC)

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 .

Fibre channel

Fibre Channel (FC) is a high-speed network technology primarily used to connect computer data storage to servers in storage area networks (SAN) in enterprise storage. Fibre Channel networks are known as a Fabric because they operate in unison as one big switch. Fibre Channel mainly runs on optical fiber cables within and between data centers. Virtual tape libraries (VTLs) can ingest data over a Fibre Channel interface, which enables seamless integration with many existing backup infrastructures and processes.

The QoreStor VTL container type is designed to work seamlessly with the FC interface. With FC, QoreStor can direct attach to NAS filers or Fibre Channel switches and supports SAN devices.

A FC VTL container on a QoreStor system supports multiple initiators, making it possible for the VTL to be shared across multiple clients of a Data Management Application (DMA).

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

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

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>
```

  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.

  > **NOTE:** A Fibre Channel (FC) VTL container on a QoreStor system supports multiple initiators, making it possible for the VTL to be shared across multiple clients of a DMA.

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.
- For the FC protocol, determine the initiator WWPN, and create the FC switch zone and enable it. (Refer to the administrator documentation for your switch for more information.) FC zoning is required to be "single target single initiator" zoned.

  > **NOTE:** Point to point cabling is not supported (directly attaching the QoreStor system to another system rather than using a switch), and multi-pathing is not currently supported.

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

  > **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, iSCSI, or FC) 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, iSCSI, or FC. You need to provide either the DMA IP/hostname for NDMP, the IP/hostname or IQN for an iSCSI connection type, or the initiator WWPN for FC.
  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.

10

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.

> **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.
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.

   > **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 theQoreStor *Command Line Interface Reference Guide* for information about the CLI commands used for encryption.

11

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 .lzip 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. TheQoreStor 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

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

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