Quest® QoreStor™ 4.1

User Guide

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.

Contents

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.
Additional whitepapers	Instructions and best practices for configuring additional Quest and third-party applications to work with QoreStor.

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

Information on compatible products

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

Table 2: 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.

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

Table 3: vRanger documentation

Document	Description
vRanger	This document provides information on supported platforms, system requirements,

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

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

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. (For a complete list of supported backup software, see Suppored backup applications) .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.

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

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 disabled by default), 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.

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.

- Rapid Data Access (RDA)

    - RDA with OpenStorage Technology (OST)

    - RDA with NetVault Backup

    - RDA with vRanger

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. 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

Accessing QoreStor

You can interact with QoreStor using one of two supported methods: the system graphical user interface (GUI) accessed in a web browser or the command line interface (CLI).

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 (.

Logging onto the system GUI for the first time

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

1. In a supported web browser, enter:

   - https://<YourQoreStorServerName>:5233

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

     i 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 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 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. A single QoreStor server can have multiple license types. For example, one QoreStor server can support both NetVault Backup and standalone licenses.

- **Standalone license** - QoreStor is licensed by the amount of backend capacity required.

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

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

Evaluating QoreStor

QoreStor offers two methods for evaluation:

- **Default installation** - If no license is installed, QoreStor defaults to a no-cost, 1TB capacity installation supported by the QoreStor Community. This option requires no license and does not expire.
  - If a license is applied to a server running in this mode, the free 1TB is **not** added to the purchased license capacity.
  - When installed in Demo mode, the capacity is limited to 100GB.

- **Full capacity trial** - available on the Quest Software Trial site, which provides a 30-day evaluation license for up to 150TB 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 perpetual license, you can install it using the **system --license** command, as described in the *QoreStor Command Line Reference Guide*.

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

To view the current license configuration, use the command

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

To install a new license, use the command

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

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))

- System cleaner (space reclamation)

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

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

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

> **i** **NOTE:** By default, QoreStor is configured to run Cleaner operations daily between 1:00 A.M and 5:00 A.M.

Schedule operations 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
```

i 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.

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**

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

To schedule cleaner operations on your system using the CLI:

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

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

1. Access the QoreStor command line interface.

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

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

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

   ```
   schedule --help
   ```

Viewing cleaner status

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 running.

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 Secure Connect

The proper configuration of Secure Connect consists of the following:

- Enabling Secure Connect

- Configuring Secure Connect properties

i | **NOTE:** Secure Connect is only supported when running on a WAN-connected client.

Enabling Secure Connect

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 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 client 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 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.

   - **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. Encryption settings are configured in a separate step available only in the command line interface.

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:

   - **None** - Provides the fastest backup time, but with no space savings.

   - **Fast** — Results in shorter backup time, but with less space savings.

   - **Best** — Provides the highest space savings, but with a longer backup time.

5. For **Chunk Type**, select:

   - **Fixed** — fixed chunking breaks the incoming data stream into chunks of a fixed size.

   - **Variable** — variable chunking breaks the incoming data stream into chunks of different sizes based on an algorithm. Variable chunking usually provides the best storage savings and is considered the default option.

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

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

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

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

   - **Encryption Mode** — Select either **static** or **internal**.

     - **static** - A global mode of key management in which a fixed key is used to encrypt all data.

     - **internal** - A mode of key lifecycle management in which the keys are periodically generated and rotated. The minimum key rotation period before the content encryption key can be rotated and a new key is generated is 7 days. This rotation period is user-configurable and can be specified in days.

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

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

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

7. Click **Add**

Adding a storage group through the command line

To add a storage group, complete the following steps.

1. Access 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. Add a new storage group using the command

   ```
   storage_group --add --name <name> [--compression_mode <fast|best>][--chunk_type
   <fixed | variable>]
   ```

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

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

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

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

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

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

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

Modifying a storage group

Storage group settings must be modified via the command line interface.

To modify a storage group, 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. 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 <none|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**.

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

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

Deleting a storage group from the CLI

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. Delete your storage group using the command below. Refer to the *QoreStor Command Line Reference Guide* for more information.

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

Managing containers

In QoreStor, data is stored in containers, which are stored in storage groups. Some containers function like a shared file system. QoreStor containers are created using the RDA connection type, which includes both OST and RDS clients. These containers are accessed via the RDA protocol native to QoreStor.

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.

   - **Access Protocol**—the connection type/access protocol for the container:

     - RDA

     - OST

Viewing containers via the CLI

To view the list of containers, follow these 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. 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).

     i | **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 **Capacity 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:

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

You can create a container through both the QoreStor GUI and the command line interface.

Creating a container through the GUI

To create a container, complete the following steps:

1. In the navigation menu click **Storage Groups**.
2. In the storage group list, click the storage group to which you want to add a container. Click **Add Container**.
3. In the **Name** field, enter a name for the container.

4. Select the **Protocol** from the drop-down.

5. For LSU Capacity, select **Unlimited** .

6. For OST containers, optionally select **Quota** and enter a capacity in GB.

7. Click **Add**

Creating a container through the command line interface

To create a container, 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. Add a container with the command

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

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

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 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. Delete a container with the command

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

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

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: 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 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. View current user accounts with the command:

    ```
    user --show [--users] [--logins] [--verbose][--name <username>] [--roles
    <ost|rda|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.

- **Username**—Enter a username between 6 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.

    i | NOTE: You can select more than one role for a user.

    - **Monitor**—Limits the user to read-only access in the QoreStor GUI.
    - **RDA**—Designates the user as an RDA protocol user.
    - **OST**—Designates the user as an OST 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 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. 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 <ost|rda|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.

   ℹ | NOTE: You can select more than one role for a user.

     - **RDA**—Designates the user as an RDA protocol user.
     - **OST**—Designates the user as an OST 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 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. Modify a user account with the command

   ```
   user --update --name <user name> [--add_roles <ost|rda|secure_connect>] [--
   remove_roles <ost|rda|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.

ℹ | NOTE: You cannot delete the administrator user.

Deleting a user account through the GUI

To delete a user, complete the following steps:

1. In the navigation menu, click **Users**.

2. In the list of users, 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 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. Delete a user account with the command

   `user --delete --name <user name>`

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

Monitoring QoreStor

This topic describes how you can monitor the current state of QoreStor operations on the **Dashboard** page.

Using the Dashboard page

The Dashboard page contains graphics that show key information about the current state of your QoreStor instance. This page automatically refreshes every 30 seconds.

To use the Dashboard page, follow these steps.

1. Click **Dashboard** in the navigation menu of the QoreStor GUI.

2. You can view the following graphs:

   - **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 DR Series 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 DR Series system 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.

  > **i** | **NOTE:** For a detailed list of possibly occurring alerts, see the topic, "QoreStor system alert and event messages," in the "Support, maintenance, and troubleshooting" chapter of this guide.

Monitoring clients

You can easily view the current clients that are connection 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. To view RDS or OST client information, click the RDA pane to expand it to view the following details:

   - **Name** — the name of the RDS or OST client.
   - **IP Address**—the IP address of the client.
   - **Type**—the type of RDA client.
   - **Plug-in**—the plug-in type installed on the client.
   - **Backup Software**—the backup software running on the client.
   - **OS**—the operating system of the client.
   - **Idle Time**—the amount of idle time (non-activity) for the client.
   - **Connection**—the number of connections for the client.
   - **Mode**—the current mode type that is set for the client, such as:

     - **Auto:** The QoreStor server sets the deduplication as either Dedupe or Passthrough, based on the client's number of cores and whether it is 32– or 64–bit.
     - **Passthrough:** The client passes all data to the QoreStor server for deduplication processing (appliance-side deduplication).
     - **Dedupe:** The client processes hashing on data, so that deduplication processing occurs on the server side (client-side deduplication).

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 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. View client information with the appropriate client command

   ```
   stats –clients –type RDS
   ```

   ```
   stats –clients –type OST
   ```

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

Configuring and Using Encryption at Rest

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

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

Understanding Encryption at Rest

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

Term	Description
	a password in usage, but is generally longer for added security. In the DR Series system, 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.
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.

  Encryption during replication can be enabled with the **rda** command as follows:

  ```
  rda --update --opdup_encryption <none | aes128 | aes256>
  ```

  Refer to the *QoreStor CLI Reference Guide* for more information.

  > **i** | NOTE: AFter executing the above **rda** command, restart the **ocards** service to enable encryption for replication.

- **Security Considerations for Passphrase and Key Management** —

  - A passphrase is very important part of the encryption process on the QoreStor system as the passphrase is used to encrypt the content encryption key or keys. If the passphrase is compromised or lost, the administrator should change it immediately so that the content encryption keys do not become vulnerable.

  - The administrator should closely consider security requirements to drive the decision for selecting the mode of key management for the QoreStor system.

  - The Internal mode is more secure than the Static mode since the keys are periodically changed. Key rotation can be set to 7 days minimum.

  - Key modes can be changed at any time during the lifetime of the QoreStor system; however, changing the key mode is a significant operation to undertake as all encrypted data must be re-encrypted.

  - Content encryption keys are stored in their encrypted form in a primary keystore, which is maintained on the same enclosure as the data-stores. For redundancy purposes, a backup copy of the primary keystore is stored on the system in the root partition, separate from the data-store partitions.

Understanding the encryption process

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

1. **Enabling encryption.**
   Encryption is disabled by default on QoreStor. An administrator can enable encryption by using the GUI or CLI.
   Encryption is set at the storage group level.

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

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

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

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

Refer to theQoreStor *Command Line Interface Reference Guide* for information about the CLI commands used

for encryption.

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.

About the QoreStor maintenance mode

In general, QoreStor enters the **Maintenance** mode whenever the file system has encountered an issue that prevents it from operating normally.

> **i** | **NOTE:** You can use the Reason code information available in the **Maintenance** mode to contact Technical Support. All maintenance must be conducted using theQoreStor Command Line Interface.

When in its **Maintenance** mode, the filesystem is in a read-only state, and the system runs the following maintenance-based operations:

> **i** | **NOTE:** Whenever QoreStor enters or exits from the **Maintenance** mode state, all communication via protocols is lost.

- Runs an internal filesystem check.

- Generates a filesystem status report (if the filesystem check finds no issues, QoreStor switches back to **Operational** mode without user intervention).

If the filesystem check finds issues, you can choose to make repairs (using Confirm Repair Filesystem) or ignore the detected issue (using Skip Repair Filesystem), at which point the system switches back to **Operational** mode.

The **Maintenance** mode process displays a number of stages, indicated on the Maintenance Mode progress bar, which include:

- Preparing for Filesystem Check

- Scan in Progress

- Completed Generating Report

  ℹ **NOTE:** If the Filesystem Check detects any repairable files, it generates a Repair Report that identifies these reported files. The Maintenance Mode progress bar halts at the Completed Generating Repair stage, and remains in **Maintenance** mode until you click Confirm Repair Filesystem. QoreStor does not advance to the Switching to Operation Mode stage until the filesystem repair is completed.

- Switching to Operational Mode

- Operational Mode (Normal State)

After QoreStor enters **Maintenance** mode, there can only be two possible outcome states:

- **Operational** mode (Normal State): where the filesystem check was successful, and no system files need to be repaired (Filesystem Check: successful).

- **Maintenance** mode has halted: where the filesystem check detected one or more repairable files (Filesystem Check: unsuccessful).

Filesystem Check — Successful: when the **Maintenance** mode successfully completes all of its stages, the DR Series system displays its status as having entered **Operational** mode (Normal State). Only after the **Maintenance** mode has successfully completed its internal check can it return to an **Operational** mode.

To return to the **Operational** mode, click Go to Dashboard on the Maintenance Mode page options bar. Go to Dashboard is only active when all of the internal system checks have completed and the progress bar indicates that all stages have been completed.

ℹ **NOTE:** You may encounter issues when using data management agents (DMAs) such as NetBackup with expired backup images when the DR Series system is in its **Maintenance** mode.

ℹ **NOTE:** When in **Maintenance** mode, image expiration fails because the DR Series system is in a read-only state. If this occurs, the DMA assumes that the backup images have expired. However, QoreStor administrator may be unaware that the backup data images still reside on QoreStor.

Filesystem Check — Unsuccessful: when the **Maintenance** mode halts at the Completed Generating Report stage, this indicates that the filesystem check detected some repairable files, and listed them in the Repair Report pane on the **Maintenance Mode** page.

To return to the **Operational** mode, click Confirm Repair Filesystem on the Maintenance Mode page options bar to repair the files listed in the Repair Report. Confirm Repair Filesystem is the only active option you can select when the progress bar indicates that some filesystem files are in need of repair.

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**

     ℹ **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.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product