Qumulo Documentation

Table of Contents

Qumulo Administrator Guide

Qumulo Documentation

Qumulo Documentation Portal

Welcome. This site is a new documentation portal for Qumulo that uses docs-as-code principles . As we continue to add new content to this portal, we want you to ask questions and share your ideas with us—click **Edit on GitHub** on any page.

Table of Contents

Visit the Knowledge Base

For a deeper dive into Qumulo features and advanced functionality such as cluster administration, visit the Qumulo Care portal. Qumulo Care lets you open a case, read articles and watch videos from our content library, review product release notes, and get involved in the Qumulo community.

Reach Out to Us

If you have any additional questions or want to give us feedback, open a case , send an email to care@qumulo.com, or ping us in your private qumulocare Slack channel.

Qumulo on Azure as a Service Administrator Guide

Qumulo Administrator Guide

The Qumulo Administrator Guide is a growing collection of information about configuring, managing, and troubleshooting Qumulo Core and you Qumulo nodes and clusters.

Table of Contents

Qumulo Administrator Guide Document History

Qumulo Administrator Guide Document History

The following table lists changes to the *Qumulo Administrator Guide*.

Date	Documentation Update
Nov. 10, 2021	Added the following sections: • Enabling and Using NFSv4.1 on a Qumulo Cluster (page 0) • Managing File Access Permissions Using NFSv4.1 Access Control Lists (ACLs) (page 0)
Nov. 2, 2021	Added the Using Qumulo Shift-To to Copy Objects to Amazon S3 (page 0) section.
Oct. 22, 2021	Added the following sections: • Replacing the Chassis of C-192T and C-432T Nodes (page 0) • Choosing NICs, Transceivers, and Cables for Your Qumulo Node (page 0)
Sep. 20, 2021	Added the Using Qumulo Shift-From for Amazon S3 to Copy Objects (page 0) section.

Enabling and Using NFSv4.1 on a Qumulo Cluster

Enabling and Using NFSv4.1 on a Qumulo Cluster

Qumulo Core 4.3.0 (and higher) supports Network File System version 4.1 (NFSv4.1). This section explains how you can configure your cluster for a supported export configuration and enable or disable NFSv4.1 on your cluster. It also provides detail about supported and unsupported features. For more information about NFSv4.1 and file access permissions, see Managing File Access Permissions Using NFSv4.1 Access Control Lists (ACLs) (page 12).

Important: Currently, Qumulo Core supports only NFSv4.1. Mounting with version 4.0 or 4.2 isn't supported.

Configuring and Using Exports for NFSv4.1

Qumulo's NFS exports can present a view of your cluster over NFS that might differ from the contents of the underlying file system. You can mark NFS exports as read-only, restricted (to allow access only from certain IP adresses), or configure specific user mappings. For more information, see Create an NFS Export in Qumulo Care.

While NFSv3 and NFSv4.1 share each cluster's NFS export configuration, exports behave differently when you access them using NFSv4.1. This section explains these differences and the new requirements for export configurations with NFSv4.1.

Differences Between NFSv3 and NFSv4.1 Exports

In the following example, a Qumulo cluster has the following export configuration.

Export Name	File System Path	Read-Only
/home	/home	No
/files	/home/admin/files	No

Export Name	File System Path	Read-Only
/read_only/home	/home	Yes
/read_only/files	/home/admin/files	Yes

NFSv3 lets you mount one of these exports by specifying the full export name, for example:

```
mount -onfsvers=3 cluster.qumulo.com:/read_only/home /mnt/cluster/home
```

This command gives read-only access to the /home directory on the cluster using the path /mnt/cluster/home . However, the following command fails with the No such file or directory message.

```
mount -onfsvers=3 cluster.qumulo.com:/read_only /mnt/cluster/read_only
```

NFSv4.1 still lets you mount exports by specifying the full export name. However, NFSv4.1 also supports navigating *above* exports, as if they are part of the file system. The following command succeeds.

```
mount -onfsvers=4.1 cluster.qumulo.com:/read_only /mnt/cluster/read_only
```

At the mount, the exports under /read_only are visible: /mnt/cluster/read_only displays virtual directories named files/ and home/ with the contents of the corresponding directories in the file system, for example:

```
/mnt/cluster/read_only/
|--- files/<file system contents>
|--- home/
|------ admin/files/<file system contents>
|------ <other file system contents>
```

This presentation of exports lets you view existing exports using the file system's own interface. It also lets you view new exports as soon as someone creates or modifies them without remounting.

Preparing Export Configurations for NFSv4.1

Qumulo's implementation of NFSv4.1 distinguishes between navigating *above* exports and *inside* an export. To avoid confusion between paths that refer to a virtual directory above an export or a real file system directory inside an export, no export name can be a prefix of another export name when NFSv4.1 is enabled.

In the following example, a Qumulo cluster has the following export configuration.

Export Name	File System Path
/	/
/admin	/home/admin

Because `/` is a prefix of `/admin`, you can't enable NFSv4.1 with this export configuration. This restriction prevents the situation where the path `/admin` can refer to both the export of `/home/admin` or the actual file system path `/admin`.

To prepare this configuration for NFSv4.1, you can do one of the following:

- Delete the `/` export and use NFSv4.1 presentation of exports when mounting `/`.

- Delete the `/admin` export.

- Give the `/` export a name that doesn't use other exports as a prefix, for example:

Export Name	File System Path
/root	/
/admin	/home/admin

Visibility of IP-Restricted Exports

Note: The names of exports are public to all NFSv4.1 clients, regardless of IP restrictions. You can't disable this behavior.

NFSv4.1 respects IP restrictions on exports: only clients with allowed IP addresses can access the contents of an export. However, clients without access to an export can still view the export as a directory when they traverse *above* exports. The restrictions apply only when a client attempts to access the contents of the export.

32-Bit Sanitization

- In NFSv3, you can configure specific exports to return 32-bit sanitized data for individual fields. NFSv3 converts any data larger than 32 bits in configured fields to 32-bit data and returns the data. For example, it can sanitize file size to 32-bit format. This truncates the field to `max_uint32` whenever the NFSv3 server returns the attribute.

- NFSv4.1 doesn't support 32-bit sanitization and ignores any sanitizations configured for an export.

Using Unique Hostnames for NFS Clients

The NFSv4.1 protocol requires clients to provide the server with globally unique identifiers. However, the NFSv4.1 client for Linux uses the machine's hostname by default. Because the Linux client doesn't support using the same hostname to connect to an NFSv4.1 server, an unpredictable failure can occur. We recommend configuring all NFS clients to use unique hostnames. For more information, see NFS Client in the Linux Kernel User's and Administrator's Guide.

Enabling NFSv4.1 on a Qumulo Cluster

Note: Currently, you can enable NFSv4.1 only using the CLI.

You can enable NFSv4.1 on your Qumulo cluster using a single cluster-wide configuration command, for example:

```
qq nfs_modify_settings --enable-v4
```

When you enable NFSv4.1, all NFS exports are accessible using NFSv3 and NFSv4.1.

Specifying the NFS Mount Option

Typically, NFS clients find and use the highest version of the protocol that both the client and server support. For example, the following command mounts using NFSv4.1 (if it is enabled) and using NFSv3 otherwise:

```
mount -t nfs your.qumulo.cluster:/mount_path /path/to/mountpoint
```

Because Qumulo's NFSv4.1 implementation currently doesn't have full feature parity with NFSv3, you must provide the `nfsvers=3` option for any mounts that require features (such as snapshot access) that only NFSv3 supports, for example:

```
mount -t nfs -o nfsvers=3 your.qumulo.cluster:/mount_path /path/to/mountpoint
```

Note: We recommend specifying the `nfsvers=4` or `nfsvers=4.1` option for any mounts that use NFSv4.1.

Checking Whether NFSv4.1 is enabled

To check whether NFSv4.1 is enabled on your cluster, use the following CLI command:

```
qq nfs_get_settings
```

Disabling NFSv4.1 on a Qumulo Cluster

Important: Disabling NFSv4.1 makes any NFSv4.1 mounts unusable immediately. We recommend switching any NFSv4.1 mounts to NFSv3 before disabling NFSv4.1.

To disable NFSv4.1 on an entire Qumulo cluster, use the following CLI command:

```
qq nfs_modify_settings --disable-v4
```

Configuring Floating IPs for Nodes

Currently, each Qumulo node is limited to 1,000 clients connected using NFSv4.1 simultaneously. To account for nodes going down, we recommend balancing the number of client connections across your nodes by configuring a sufficient number of floating IP addresses per node. This prevents a node failover event from overloading the nodes to which the clients might fail over.

For example, if you configure only one IP address per node, on a cluster with 600 clients per node a single node failure might overload one of the remaining nodes, preventing 200 clients from connecting. If you assign multiple floating IP addresses to each node, the clients' connections are distributed across multiple nodes.

Supported and Unsupported Features in Qumulo's Implementation of NFSv4.1

Qumulo's implementation of NFSv4.1 currently supports:

- General file system access (reading, writing, and navigating files)

- Unstable writes

- Full use of the NFS exports configuration shared with NFSv3

- Navigation in the pseudo-file system above your exports

- NFSv3-style `AUTH_SYS` or `AUTH_UNIX` authentication

- Fine-grained control over file permissions using access control lists (ACLs)

Qumulo Core doesn't support the following NFSv3 features through NFSv4.1:

- Quota sizes don't appear through NFSv4.1 with certain commands, such as `df` (however, Qumulo Core respects directory quotas)

- You can't access snapshots through NFSv4.1

- File locking (for example, using the `fcntl` command)

Qumulo Core doesn't currently support the following NFSv4.1 features:

- Secure authentication using Kerberos

- Delegations

Managing File Access Permissions Using NFSv4.1 Access Control Lists (ACLs)

NFSv4.1 lets you use access control lists (ACLs) to manage access permissions for files. The Qumulo Core implementation of NFSv4.1 supports ACLs using `AUTH_SYS` or `AUTH_UNIX` credentials. You can allow or deny various operations using the CLI tools in the `nfs-acl-tools` Linux package.

For more information about NFSv4.1, see Enabling and Using NFSv4.1 on a Qumulo Cluster (page 5).

Using the NFSv4.1 CLI Commands to Manage ACLs

In most Linux distributions, the `nfs-acl-tools` package contains the NFSv4.1 commands that let you manage ACLs for files.

Showing the ACL of a File

To show the ACL of a file, use the `nfs4_getfacl` command. In the following example, we create the file `my-file` and then show the ACL for it.

```
$ touch /mnt/qumulo/my-file
$ nfs4_getfacl /mnt/qumulo/my-file
A::1001:rwatTnNcy
A:g:1001:rwatTnNcy
A::EVERYONE@:rtncy
```

The entries in the access control list have four parts separated by colons. For a detailed description, see the man page for `nfs4_acl` in the Linux Documentation.

1. The type of access control entry (ACE). In this example, all three ACEs are set to `A` (allow).

   Note: Qumulo Core supports only `A` and `D` ACEs.

   - **A:** Allow

   - **D:** Deny

   - **U:** Audit

   - **L:** Alarm

2. Additional ACE flags. In this example, the second ACE has the flag `g` that shows that the ID in the following part represents a *group* (rather than a user).

   Note: Qumulo Core doesn't support The `S` and `F` flags.

3. Whom the ACE applies to. The available options are:

   - `AUTH_SYS` or `AUTH_UNIX` : A user authenticated at the client

   - `EVERYONE@` : Any user of the file system

   - `GID` : The GID of the file

   - `GROUP@` : The group owner of the file

   - `UID` : The UID of the file

   - `OWNER@` : The owner of the file

   Note: Currently, Qumulo Core doesn't support Kerberos principals in ACLs.

4. The access types the ACE applies to. For example:

   - `r` : Read

   - `t` : Read attributes

   - `w` : Write

   The `nfs4_setfacl` command also lets you use the following shorthand:

   - `R` : Generic read

   - `W` : Generic write

   - `X` : Execute permissions

   For a detailed description, see the man page for `nfs4_setfacl` in the Linux Documentation.

The ACL in this example corresponds the the `664` mode: The owner and group of the file are allowed to read and write, while others (`EVERYONE@`) are allowed to only read. To check the current mode, run the `stat` command, for example:

```
$ stat -c %a /mnt/qumulo/my-file
664
```

Editing the ACL of a File

To edit the ACL of a file using the text editor specified in the `$EDITOR` environment variable, use the `nfs4_editfacl` (or `nfs4_setfacl -e`) command. For a detailed description, see the man page for `nfs4_editfacl` and `nfs4_setfacl` in the Linux Documentation.

Setting the ACL of a File

To set the ACL of a file, you can use one of the following commands:

- **Add a Single ACE:** `nfs4_setfacl -a <ace>`
- **Set an Entire ACL:** `nfs4_setfacl -s <acl>`

Using Special NFSv4.1 Identifiers

Qumulo supports three of the special identifiers that NFSv4.1 defines. These identifiers get the ACE to apply to:

- `EVERYONE@` : Any user of the file system
- `GROUP@` : The group owner of the file
- `OWNER@` : The owner of the file

Managing NFSv4.1 Permissions with ACLs and POSIX-Style Modes

You can manage NFSv4.1 access permissions with ACLs, POSIX-style modes, or a combination of both.

- If you set an ACL on a file and then also set a mode on it, the restrictions that the mode espresses are also applied to the ACL. These restrictions change or remove ACEs that apply to the owner, group, or other users.

- If you use the `OWNER@` or `GROUP@` identifiers in an ACL that allows read, write, or execute permissions, the identifiers appear in the `owner` or `group` bits of the mode when you read the file's mode.

Note: Because the `EVERYONE@` identifier includes the owner and group of a file and the `other` bits of a mode don't apply to the owner or group, the permissions you grant to the `EVERYONE@` identifier are more broad than a mode's `other` bits.

Using NFSv4.1 ACLs with SMB Access Control

NFSv4.1 ACLs are comparable with SMB access controls. In most cases, you can write and read using both protocols without issues.

Often, the identities in ACEs map to an NFS UID or GID. These mappings succeed when you:

- Connect your cluster to an Active Directory (AD) domain.

- Enable RFC2307 (An Approach for Using LDAP as a Network Information Service) .

- Associate all NFS UIDs or GIDs with AD users or groups in your AD configuration.

Alternatively, you can configure UID or GID mappings for the cluster's local users or groups. When SMB ACLs refer to users or groups not mapped to a corresponding NFS UID or GID, the users or groups appear with the `NOBODY` UID (`65534`).

To discover which mappings your cluster can perform for a file, use the following CLI commands:

- `qq auth_expand_identity` : Find equivalent identities and full group membership for an `auth_id`

- `qq auth_find_identity` : Find all representations for an `auth_id`

- `qq fs_get_acl` : Get the ACL for a file or directory

Changing File Owners

When you change the owner of a file, the ACEs that refer to the owner change to the new owner, for example:

```
$ nfs4_getfacl /mnt/qumulo/my-file
A::1001:rwatTnNcy
A:g:1001:rwatTnNcy
A::EVERYONE@:rtncy

$ sudo chown 1002 /mnt/qumulo/my_file

$ nfs4_getfacl /mnt/qumulo/my-file
A::1002:rwatTnNcy
A:g:1001:rwatTnNcy
A::EVERYONE@:rtncy
```

Using Qumulo Shift-To to Copy Objects to Amazon S3

Using Qumulo Shift-To for Amazon S3 to Copy Objects

This guide explains how you can use Qumulo Shift-To to copy objects from a directory in a Qumulo cluster to a folder in an Amazon Simple Storage Service (Amazon S3) bucket (cloud object store). For more information about copying objects from S3 to Qumulo, see Using Qumulo Shift-From for Amazon S3 to Copy Objects (page 32).

The guide describes how a Shift-To relationship works and includes information about the prerequisites, IAM permissions, and CLI commands that you can use to copy files and manage Shift relationships.

Prerequisites

- A Qumulo cluster with:
    - Qumulo Core 3.2.1 (and higher) for the CLI and 3.2.5 (and higher) for the Web UI
    - HTTPS connectivity to `s3.<region>.amazonaws.com` though one of the following means:
        - Public Internet
        - VPC endpoint
        - AWS Direct Connect

        For more information, see AWS IP address ranges in the AWS General Reference.
- Membership in a Qumulo role with the following privileges:
    - `PRIVILEGE_REPLICATION_OBJECT_WRITE` : This privilege is required to create a Shift relationship.
    - `PRIVILEGE_REPLICATION_OBJECT_READ` : This privilege is required to view the status of a Shift relationship.

    Notes:

- For any changes to take effect, user accounts with newly assigned roles must log out and log back in (or their sessions must time out).

- Use special care when granting privileges to roles and users because certain privileges (such as replication-write privileges) can use system privileges to overwrite or move data to a location where a user has greater permissions. This can give a user access to all directories and files in a cluster regardless of any specific file and directory settings.

- An existing bucket with contents in Amazon S3

- AWS credentials (access key ID and secret access key) with the following permissions:

  - `s3:AbortMultipartUpload`

  - `s3:GetObject`

  - `s3:PutObject`

  - `s3:ListBucket`

  For more information, see Understanding and getting your AWS credentials in the AWS General Reference

Example IAM Policy

In the following example, the IAM policy gives permission to read from and write to the `my-folder` folder in the `my-bucket` . This policy can give users the permissions required to run Shift-To jobs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::my-bucket"
    },
    {
      "Action": [
        "s3:AbortMultipartUpload",
        "s3:GetObject",
        "s3:PutObject"
      ]
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::my-bucket/my-folder/*"
    }
  ]
}
```

How Shift-To Relationships Work

Qumulo Core performs the following steps when it creates a Shift-To relationship.

1. Verifies that the directory exists on the Qumulo cluster and that the specified S3 bucket exists, is accessible using the specified credentials, and contains downloadable objects.

2. Creates the Shift-To relationship.

3. Starts a job using one of the nodes in the Qumulo cluster.

   Note: If you perform multiple Shift operations, Qumulo Core uses multiple nodes.

4. To ensure that the copy is point-in-time consistent, takes a temporary snapshot of the directory (for example, named `replication_to_bucket_my_bucket`).

5. Recursively traverses the directories and files in the snapshots and copies each object to a corresponding object in S3.

6. Preserves the file paths in the local directory in the keys of replicated objects.

For example, the file `/my-dir/my-project/file.text`, where `my-dir` is the directory on your Qumulo cluster, is uploaded to S3 as the following object, where `my-folder` is the specified S3 folder.

```
https://my-bucket.s3.us-west-2.amazonaws.com/my-folder/my-project/file.txt
```

Note: This process doesn't encode or transform your data in any way. Shift-To replicates only the data in a regular file's primary stream, excluding alternate data streams and file system metadata such as access control lists (ACLs). To avoid transferring data across the public Internet, a server-side S3 copy operation also copies any hard links to files in the replication local directory to S3 as full copies of objects, with identical contents and metadata.

The following table explains how entities in the Qumulo file system map to entities in an S3 bucket.

Entity in the Qumulo File System	Entity in an Amazon S3 Bucket
Access control list (ACL)	Not copied
Alternate data streams	Not copied
Directory	Not copied (directory structure is preserved in the object key for objects created for files)
Hard link to a non-regular file	Not copied
Hard link to a regular file	Copy of the S3 object
Holes in sparse files	Zeroes (holes are expanded)

Entity in the Qumulo File System	Entity in an Amazon S3 Bucket
Regular file	S3 object (the object key is the file system path and the metadata is the field data)
SMB extended file attributes	Not copied
Symbolic link	Not copied
Timestamps (`mtime`, `ctime`, `atime`, `btime`)	Not copied
UNIX device file	Not copied

7. Checks whether a file is already replicated. If the object exists in the remote S3 bucket, and neither the file nor the object are modified since the last successful replication, its data is not retransferred to S3.

   Note: Shift never deletes files in the remote S3 folder, even if the files are removed from the local directory since the last replication.

8. Deletes the temporary snapshot.

Storing and Reusing Relationships

The Shift-To relationship remains on the Qumulo cluster. You can monitor the completion status of a job, start new jobs for a relationship after the initial job finishes, and delete the relationship (when you no longer need the S3-folder-Qumulo-directory pair). To avoid redownloading objects that a previous copy job downloaded, relationships take up approximately 100 bytes per object. To free this storage, you can delete relationships that you no longer need.

If you repeatedly copy from the same Qumulo directory, you can speed up the download process (and skip already downloaded files) by using the same relationship.

A new relationship for subsequent downloads doesn't share any tracking information with previous relationships associated with a directory and might recopy data that is already downloaded.

Using the Qumulo Web UI to Copy Files and Manage Relationships

This section describes how you can use the Qumulo Web UI 3.2.5 (and higher) to copy files from a Qumulo cluster to Amazon S3, review Shift relationship details, stop a running copy job, repeat a completed copy job, and delete a relationship.

To Copy Files to Amazon S3

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

3. On the **Copy to/from S3** page, click **Create Copy**.

4. On the **Create Copy to/from S3** page, click **Local ⇨ Remote** and then enter the following:

   a. The **Directory Path** on your cluster (`/` by default)

   b. The S3 **Bucket Name**

   c. The **Folder** in your S3 bucket

   d. The **Region** for your S3 bucket

   e. Your AWS **Region** (`/` by default)

   f. Your AWS **Access Key ID** and **Secret Access Key**.

5. (Optional) For additional configuration, click **Advanced S3 Server Settings**.

6. Click **Create Copy**.

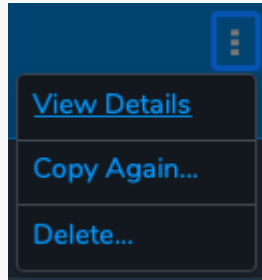7. In the **Create Copy to S3?** dialog box, review the Shift relationship and then click **Yes, Create**.

   The copy job begins.

To View Configuration Details and Status of Shift Relationships

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

The **Copy to/from S3** page lists all existing Shift relationships.

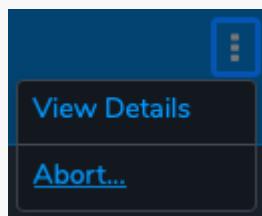3. To get more information about a specific Shift relationship, click ⋮ **> View Details**.

The **Copy to/from S3 Details** page displays the following information:

- **Throughput:** average

- **Run Time**

- **Data:** total, transferred, and unchanged

- **Files:** total, transferred, and unchanged

To Stop a Copy Job in Progress

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

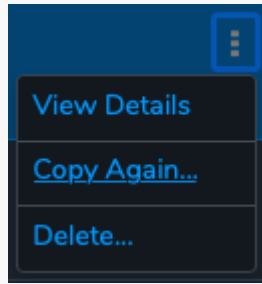3. To stop a copy job for a specific relationship, click ⋮ **> Abort**.

4. In the **Abort copy from?** dialog box, review the Shift relationship and then click **Yes, Abort**.

   The copy job stops.

To Repeat a Completed Copy Job

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

3. To stop a copy job for a specific relationship, click ⋮ **> Copy Again**.

4. In the **Copy again?** dialog box, review the Shift relationship and then click **Yes, Copy Again**.

   The copy job repeats.

To Delete a Shift Relationship

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

3. To stop a copy job for a specific relationship, click ⋮ **> Delete**.

4. In the **Delete copy from?** dialog box, review the Shift relationship and then click **Yes, Delete**.

   The copy job is deleted.

Using the Qumulo CLI to Copy Files and Manage Relationships

This section describes how you can use the Qumulo CLI 3.2.5 (and higher) to copy files from a Qumulo cluster to Amazon S3, review Shift relationship details, stop a running copy job, repeat a completed copy job, and delete a relationship.

Copying Files from Amazon S3

To copy files, use the `replication_create_object_relationship` command and specify the following:

- Local directory path on Qumulo cluster

- Copy direction (copy-to)

- S3 object folder

- S3 bucket

- AWS region

- AWS access key ID

- AWS secret access key

The following example shows how you can create a relationship between the directory `/my-dir/` on a Qumulo cluster and the S3 bucket `my-bucket` and folder `/my-folder/` in the `us-west-2` AWS region. The secret access key is associated with the access key ID.

```
qq replication_create_object_relationship \
  --source-directory-path /my-dir/ \
  --direction COPY_TO_OBJECT \
  --object-folder /my-folder/ \
  --bucket my-bucket \
  --region us-west-2 \
  --access-key-id AKIAIOSFODNN7EXAMPLE \
  --secret-access-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

The CLI returns the details of the relationship in JSON format, for example:

```
{
  "access_key_id": "ABC",
  "bucket": "my-bucket",
  "object_store_address": "s3.us-west-2.amazonaws.com",
  "id": "1c23b4ed-5c67-8f90-1e23-a4f5f6ceff78",
  "object_folder": "my-folder/",
  "port": 443,
  "ca_certificate": null,
  "region": "us-west-2",
  "source_directory_id": "3",
  "direction": "COPY_TO_OBJECT",
}
```

Viewing Configuration Details and Status of Shift Relationships

- To view configuration details for all Shift relationships, use the `replication_list_object_relationships` command.

- To view configuration details for a specific relationship, use the `replication_get_object_relationship` command followed by the `--id` and the Shift relationship ID (GUID), for example:

```
  qq replication_get_object_relationship --id 1c23b4ed-5c
67-8f90-1e23-a4f5f6ceff78
```

- To view the status of a specific relationship, use the `replication_get_object_relationship_status` command followed by the `--id` and the Shift relationship ID.

- To view the status of all relationships, use the `replication_list_object_relationship_statuses` command.

  The CLI returns the details of all relationships in JSON format, for example:

```
[
  {
    "direction": "COPY_TO_OBJECT",
    "access_key_id": "AKIAIOSFODNN7EXAMPLE",
    "bucket": "my-bucket",
    "object_store_address": "s3.us-west-2.amazonaws.co
m",
    "id": "1c23b4ed-5c67-8f90-1e23-a4f5f6ceff78",
    "object_folder": "my-folder/",
    "port": 443,
    "ca_certificate": null,
    "region": "us-west-2",
    "source_directory_id": "3",
    "source_directory_path": "/my-dir/",
    "state": "REPLICATION_RUNNING",
    "current_job": {
      "start_time": "2020-04-06T17:56:29.659309904Z",
      "estimated_end_time": "2020-04-06T21:54:33.2440955
93Z",
      "job_progress": {
        "bytes_transferred": "178388608",
        "bytes_unchanged": "0",
        "bytes_remaining": "21660032",
        "bytes_total": "200048640",
        "files_transferred": "17",
        "files_unchanged": "0",
        "files_remaining": "4",
        "files_total": "21",
        "percent_complete": 0.890368314738253,
        "throughput_current": "12330689",
        "throughput_overall": "12330689"
      }
    },
    "last_job": null
  }
]
```

The `state` field indicates a `REPLICATION_RUNNING` status and `current_job` shows ongoing progress. When Qumulo Core copies files from S3, details for the most recent completed job become available in the `last_job` field, the `state` field changes to `REPLICATION_NOT_RUNNING` and the `current_job` field reverts to `null`.

Note: If you already ran a job for a relationship, it is possible for both the `current_job` and `last_job` fields to be non-null while you run a new job.

Stopping a Copy Job in Progress

To stop a copy job already in progress, use the `replication_abort_object_relationship` command followed by the `--id` and the Shift relationship ID.

Repeating a Completed Copy Job

To repeat a completed copy job, use the `replication_start_object_relationship` command followed by the `--id` and the Shift relationship ID.

This command begins a new job for the existing relationship and downloads any content that changed in the S3 bucket or on the Qumulo cluster since the time the previous job ran.

Deleting a Shift Relationship

After your copy job is complete, you can delete your Shift relationship. To do this, run the `replication_delete_object_relationship` command followed by the `--id` and the Shift relationship ID.

Note: You can run this command only against a relationship that doesn't have any active jobs running.

This command removes the copy job's record, leaving locally stored objects unchanged. Any storage that the relationship used to track downloaded objects becomes available when you delete the relationship.

Troubleshooting Copy Job Issues

Any fatal errors that occur during a copy job cause the job to fail, leaving a partially copied set of files in the directory in your S3 bucket. However, to let you review the Shift relationship status any failure messages, the Shift relationship continues to exist. You can start a new job to complete the copying of objects to the S3 bucket—any successfully transferred files from the previous job aren't retransferred from your Qumulo cluster.

Whenever Qumulo Core doesn't complete an operation successfully and returns an error from the API or CLI, the `error` field within the `last_job` field (that the `replication_list_object_relationship_statuses` command returns) contains a detailed failure message. For more troubleshooting details, see `qumulo-replication.log` on your Qumulo cluster.

Best Practices

We recommend the following best practices for working with Qumulo Shift-To for Amazon S3.

- **Bucket Lifecycle Policy:** To abort any incomplete uploads older than several days and ensure the automatic clean-up of any storage that incomplete parts of large objects (left by failed or interrupted replication operations) use, configure a bucket lifecycle policy. For more information, see Uploading and copying objects using multipart upload in the *Amazon Simple Storage Service User Guide*.

- **VPC Endpoints:** For best performance when using a Qumulo cluster in AWS, configure a VPC endpoint to S3. For on-premises Qumulo clusters, we recommend AWS Direct Connect or another high-bandwidth, low-latency connection to S3.

- **Unique Artifacts:** To avoid collisions between different data sets, specify a unique object folder or unique bucket for each replication relationship from a Qumulo cluster to S3.

- **Object Versioning:** To protect against unintended overwrites, enable object versioning. For more information, see Using versioning in S3 buckets in the *Amazon Simple Storage Service User Guide*.

- **Completed Jobs:** If you don't plan to use a Shift relationship to download updates from S3, delete the relationship to free up any storage associated with it.

- **Concurrent Replication Relationships:** To increase parallelism, especially across distinct datasets, use concurrent replication relationships to S3. To avoid having a large number of concurrent operations impact client I/O to the Qumulo cluster, limit the number of concurrent replication relationships. While there is no hard limit, we don't recommend creating more than 100 concurrent replication relationships on a cluster (including both Shift and Qumulo local replication relationships).

Restrictions

- **Object-Locked Buckets:** You can't use buckets configured with S3 Object Lock and a default retention period for Shift-To. If possible, either remove the defauly retention period and set retention periods explicitly on objects uploaded outside of Shift or use a different S3 bucket without S3 Object Lock enabled. For more information, see How S3 Object Lock works in the *Amazon Simple Storage Service User Guide*.

- **File Size Limit:** The size of an individual file can't exceed 5 TiB (this is the maximum object size that S3 supports). There is no limit on the total size of all your files.

- **File Path Limit:** The length of a file path must be shorter than 1,024 characters, including the configured object folder prefix, excluding the local directory path.

- **Hard Links:** Qumulo Core 3.2.3 (and higher) supports hard links, up to the maximum object size that S3 supports.

- **Objects Under the Same Key:** Unless an object contains Qumulo-specific hash metadata that matches a file, any object that exists under the same key that a new relationship replicates *is overwritten*. To retain older versions of overwritten objects, enable versioning for your S3 bucket. For more information, see Using versioning in S3 buckets in the *Amazon Simple Storage Service User Guide*.

- **Object Checksums:** All files replicated using S3 server-side integrity verification (during upload) use a SHA256 checksum stored in the replicated object's metadata.

- **S3-Compatible Object Stores:** S3-compatible object stores aren't supported. Currently, Qumulo Shift-To supports replication only to Amazon S3.

- **HTTP:** HTTP isn't supported. All Qumulo connections are encrypted using HTTPS and verify the S3 server's SSL certificate.

- **Anonymous Access:** Anonymous access isn't supported. You must use valid AWS credentials.

- **Replication without Throttling:** Replication provides no

throttling and might use all available bandwidth. If necessary, use Quality of Service rules on your network.

- **Amazon S3 Standard Storage Class:** Qumulo Shift-To supports uploading only objects stored in the Amazon S3 Standard storage class. You can't download objects stored in the Amazon S3 Glacier or Deep Archive storage classes and any buckets that contain such objects cause a copy job to fail.

- **Content-Type Metadata:** Because all objects are stored in S3 using the default `binary/octet-stream` content type, they might be interpreted as binary data if you download them using a browser. To attach content-type metadata to your objects, use the AWS Console.

Using Qumulo Shift-From to Copy Objects from Amazon S3

Using Qumulo Shift-From for Amazon S3 to Copy Objects

This guide explains how you can use Qumulo Shift-From to copy objects from a folder in an Amazon Simple Storage Service (Amazon S3) bucket (cloud object store) to a directory in a Qumulo cluster. For more information about copying objects from Qumulo to S3, see Using Qumulo Shift-To for Amazon S3 to Copy Objects (page 17) in Qumulo Care.

The guide describes how a Shift-From relationship works and includes information about the prerequisites, IAM permissions, and CLI commands that you can use to copy files and manage Shift relationships.

Prerequisites

- A Qumulo cluster with:

    ◦ Qumulo Core 4.2.3 (or higher)

    ◦ HTTPS connectivity to `s3.<region>.amazonaws.com` though one of the following means:

        ▪ Public Internet

        ▪ VPC endpoint

        ▪ AWS Direct Connect

        For more information, see AWS IP address ranges in the AWS General Reference.

- Membership in a Qumulo role with the following privileges:

    ◦ `PRIVILEGE_REPLICATION_OBJECT_WRITE` : This privilege is required to create a Shift relationship.

    ◦ `PRIVILEGE_REPLICATION_OBJECT_READ` : This privilege is required to view the status of a Shift relationship.

    Notes:

- For any changes to take effect, user accounts with newly assigned roles must log out and log back in (or their sessions must time out).

- Use special care when granting privileges to roles and users because certain privileges (such as replication-write privileges) can use system privileges to overwrite or move data to a location where a user has greater permissions. This can give a user access to all directories and files in a cluster regardless of any specific file and directory settings.

- An existing bucket with contents in Amazon S3

- AWS credentials (access key ID and secret access key) with the following permissions:

  - `s3:GetObject`

  - `s3:ListBucket`

  For more information, see Understanding and getting your AWS credentials in the AWS General Reference

Example IAM Policy

In the following example, the IAM policy gives permission to read from and write to the `my-folder` folder in the `my-bucket` . This policy can give users the minimal set of permissions required to run Shift-From jobs. (Shift-To jobs require a less-restrictive policy. For more information and an example, see Using Qumulo Shift-To for Amazon S3 to Copy Objects (page 17).)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::my-bucket"
    },
    {
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::my-bucket/my-folder/*"
    }
  ]
}
```

How Shift-From Relationships Work

Qumulo Core performs the following steps when it creates a Shift-From relationship.

1. Verifies that the directory exists on the Qumulo cluster and that the specified S3 bucket exists, is accessible using the specified credentials, and contains downloadable objects.

2. Creates the Shift-From relationship.

3. Starts a job using one of the nodes in the Qumulo cluster.

   Note: If you perform multiple Shift operations, Qumulo Core uses multiple nodes.

4. Lists the contents of the S3 folder and downloads the objects to the specified directory on your Qumulo cluster.

5. Forms the full path of the file on the Qumulo custer by appending the path of the object (relative to the S3 folder) to the directory path on the Qumulo cluster.

   For example, the following object is downloaded to `/my-dir/my-project/file.text`, where `my-folder` is the specified S3 folder and `my-dir` is the directory on your Qumulo cluster.

```
https://my-bucket.s3.us-west-2.amazonaws.com/my-folder/m
y-project/file.txt
```

Note: This process doesn't encode or transform your data in any way. Shift-From attempts only to map every S3 object in the specified folder to a file on your Qumulo cluster.

6. Avoids redownloading an unchanged object in a subsequent job by tracking the information about an object and its replicated object.

   Note: If you rename or move an object or local file between jobs, or if there are any metadata changes in S3 or Qumulo, the object is replicated again.

Storing and Reusing Relationships

The Shift-From relationship remains on the Qumulo cluster. You can monitor the completion status of a job, start new jobs for a relationship after the initial job finishes, and delete the relationship (when you no longer need the S3-folder-Qumulo-directory pair). To avoid redownloading objects that a previous copy job downloaded, relationships take up approximately 100 bytes per object. To free this storage, you can delete relationships that you no longer need.

If you repeatedly download from the same S3 folder, you can speed up the download process (and skip already downloaded files) by using the same relationship.

A new relationship for subsequent downloads doesn't share any tracking information with previous relationships associated with a directory and might recopy data that is already downloaded.

Using the Qumulo Web UI to Copy Files and Manage Relationships

This section describes how you can use the Qumulo Web UI 4.2.5 (and higher) to copy files from Amazon S3 to a Qumulo cluster, review Shift relationship details, stop a running copy job, repeat a completed copy job, and delete a relationship.
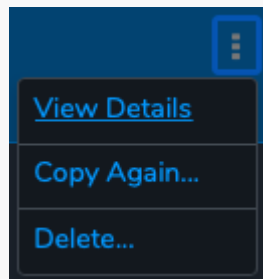
To Copy Files from Amazon S3

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

3. On the **Copy to/from S3** page, click **Create Copy**.

4. On the **Create Copy to/from S3** page, click **Local ⇦ Remote** and then enter the following:

   a. The **Directory Path** on your cluster (**/** by default)

   b. The S3 **Bucket Name**

   c. The **Folder** in your S3 bucket

   d. The **Region** for your S3 bucket

   e. Your AWS **Region** (**/** by default)

   f. Your AWS **Access Key ID** and **Secret Access Key**.

5. (Optional) For additional configuration, click **Advanced S3 Server Settings**.

6. Click **Create Copy**.

7. In the **Create Copy from S3?** dialog box, review the Shift relationship and then click **Yes, Create**.

   The copy job begins.

To View Configuration Details and Status of Shift Relationships

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

   The **Copy to/from S3** page lists all existing Shift relationships.

3. To get more information about a specific Shift relationship, click ⠿ **> View Details**.
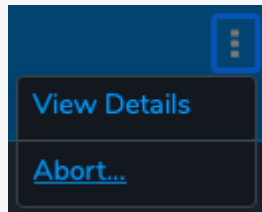

The **Copy to/from S3 Details** page displays the following information:

- **Throughput:** average

- **Run Time**

- **Data:** total, transferred, and unchanged

- **Files:** total, transferred, and unchanged

To Stop a Copy Job in Progress

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

3. To stop a copy job for a specific relationship, click ⋮ **> Abort**.

4. In the **Abort copy from?** dialog box, review the Shift relationship and then click **Yes, Abort**.

   The copy job stops.

To Repeat a Completed Copy Job

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

3. To stop a copy job for a specific relationship, click ⋮ **> Copy Again**.

4. In the **Copy again?** dialog box, review the Shift relationship and then click **Yes, Copy Again**.

   The copy job repeats.

To Delete a Shift Relationship

1. Log in to Qumulo Core.

2. Click **Cluster > Copy to/from S3**.

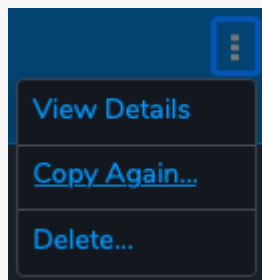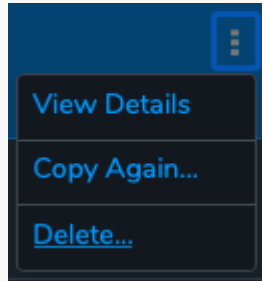3. To stop a copy job for a specific relationship, click ⋮ **> Delete**.

4. In the **Delete copy from?** dialog box, review the Shift relationship and then click **Yes, Delete**.

   The copy job is deleted.

Using the Qumulo CLI to Copy Files and Manage Relationships

This section describes how you can use the Qumulo CLI to copy files from Amazon S3 to a Qumulo cluster, review Shift relationship details, stop a running copy job, repeat a completed copy job, and delete a relationship.

Copying Files from Amazon S3

To copy files, use the `replication_create_object_relationship` command and specify the following:

- Local directory path on Qumulo cluster

- Copy direction (copy-from)

- S3 object folder

- S3 bucket

- AWS region

- AWS access key ID

- AWS secret access key

The following example shows how you can create a relationship between the directory `/my-dir/` on a Qumulo cluster and the S3 bucket `my-bucket` and folder `/my-folder/` in the `us-west-2` AWS region. The secret access key is associated with the access key ID.

```
qq replication_create_object_relationship \
  --local-directory-path /my-dir/ \
  --direction COPY_FROM_OBJECT \
  --object-folder /my-folder/ \
  --bucket my-bucket \
  --region us-west-2 \
  --access-key-id AKIAIOSFODNN7EXAMPLE \
  --secret-access-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

The CLI returns the details of the relationship in JSON format, for example:

```
{
  "access_key_id": "ABC",
  "bucket": "my-bucket",
  "object_store_address": "s3.us-west-2.amazonaws.com",
  "id": "1c23b4ed-5c67-8f90-1e23-a4f5f6ceff78",
  "object_folder": "my-folder/",
  "port": 443,
  "ca_certificate": null,
  "region": "us-west-2",
  "local_directory_id": "3",
  "direction": "COPY_FROM_OBJECT",
}
```

Viewing Configuration Details and Status of Shift Relationships

- To view configuration details for all Shift relationships, use the `replication_list_object_relationships` command.

- To view configuration details for a specific relationship, use the `replication_get_object_relationship` command followed by the `--id` and the Shift relationship ID (GUID), for example:

```
  qq replication_get_object_relationship --id 1c23b4ed-5c
67-8f90-1e23-a4f5f6ceff78
```

- To view the status of a specific relationship, use the
  `replication_get_object_relationship_status` command
  followed by the `--id` and the Shift relationship ID.

- To view the status of all relationships, use the
  `replication_list_object_relationship_statuses` command.

  The CLI returns the details of all relationships in JSON format,
  for example:

```json
[
  {
    "direction": "COPY_FROM_OBJECT",
    "access_key_id": "AKIAIOSFODNN7EXAMPLE",
    "bucket": "my-bucket",
    "object_store_address": "s3.us-west-2.amazonaws.co
m",
    "id": "1c23b4ed-5c67-8f90-1e23-a4f5f6ceff78",
    "object_folder": "my-folder/",
    "port": 443,
    "ca_certificate": null,
    "region": "us-west-2",
    "local_directory_id": "3",
    "local_directory_path": "/my-dir/",
    "state": "REPLICATION_RUNNING",
    "current_job": {
      "start_time": "2020-04-06T17:56:29.659309904Z",
      "estimated_end_time": "2020-04-06T21:54:33.2440955
93Z",
      "job_progress": {
        "bytes_transferred": "178388608",
        "bytes_unchanged": "0",
        "bytes_remaining": "21660032",
        "bytes_total": "200048640",
        "files_transferred": "17",
        "files_unchanged": "0",
        "files_remaining": "4",
        "files_total": "21",
        "percent_complete": 0.890368314738253,
        "throughput_current": "12330689",
        "throughput_overall": "12330689"
      }
    },
    "last_job": null
  }
]
```

The `state` field indicates a `REPLICATION_RUNNING` status and
`current_job` shows ongoing progress. When Qumulo Core
copies files from S3, details for the most recent completed job
become available in the `last_job` field, the `state` field changes
to `REPLICATION_NOT_RUNNING` and the `current_job` field reverts
to `null`.

Note: If you already ran a job for a relationship, it is possible for both the `current_job` and `last_job` fields to be non-null while you run a new job.

Stopping a Copy Job in Progress

To stop a copy job already in progress, use the `replication_abort_object_relationship` command followed by the `--id` and the Shift relationship ID.

Repeating a Completed Copy Job

To repeat a completed copy job, use the `replication_start_object_relationship` command followed by the `--id` and the Shift relationship ID.

This command begins a new job for the existing relationship and downloads any content that changed in the S3 bucket or on the Qumulo cluster since the time the previous job ran.

Deleting a Shift Relationship

After your copy job is complete, you can delete your Shift relationship. To do this, run the `replication_delete_object_relationship` command followed by the `--id` and the Shift relationship ID.

Note: You can run this command only against a relationship that doesn't have any active jobs running.

This command removes the copy job's record, leaving locally stored objects unchanged. Any storage that the relationship used to track downloaded objects becomes available when you delete the relationship.

Troubleshooting Copy Job Issues

Any fatal errors that occur during a copy job cause the job to fail, leaving a partially copied set of files in the directory on your Qumulo cluster. However, to let you review the Shift relationship status any failure messages, the Shift relationship continues to exist. You can start a new job to complete the copying of objects from the S3 bucket—any successfully transferred files from the previous job aren't retransferred to your Qumulo cluster.

Whenever Qumulo Core doesn't complete an operation successfully and returns an error from the API or CLI, the `error` field within the `last_job` field (that the `replication_list_object_relationship_statuses` command returns) contains a detailed failure message. For more troubleshooting details, see `qumulo-replication.log` on your Qumulo cluster.

Best Practices

We recommend the following best practices for working with Qumulo Shift-From for Amazon S3.

- **Inheritable Permissions:** Because the system user creates the files copied using Shift-From for S3, the system owns these files. By default, Everyone will be granted Read permissions, and administrators always have full access to the files.

  To assign the necessary permissions to copied files, you must assign the necessary inheritable permissions to the root directory of the relationship **before** creating a Copy from S3 relationship. This ensures that the copied subdirectories and files inherit the permissions.

  Windows Security Dialog or `qq fs_modify_acl` can be used to edit permissions on a directory. See Qumulo-File-Permissions-Overview to learn more about file permissions.

- **VPC Endpoints:** For best performance when using a Qumulo cluster in AWS, configure a VPC endpoint to S3. For on-premises Qumulo clusters, we recommend AWS Direct Connect or another high-bandwidth, low-latency connection to S3.

- **Repeated Synchronization:** If you need to repeatedly synchronize an S3 folder with a Qumulo directory, we recommend reusing the same relationship. This lets you avoid repeated downloading of unchanged objects that already exist locally.

- **Completed Jobs:** If you don't plan to use a Shift relationship to download updates from S3, delete the relationship to free up any storage associated with it.

- **Concurrent Replication Relationships:** To increase parallelism, especially across distinct datasets, use concurrent replication relationships from S3. To avoid having a large number of concurrent operations impact client I/O to the Qumulo cluster, limit the number of concurrent replication

relationships. While there is no hard limit, we don't recommend creating more than 100 concurrent replication relationships on a cluster (including both Shift and Qumulo local replication relationships).

Restrictions

- **S3-Compatible Object Stores:** S3-compatible object stores aren't supported. Currently, Qumulo Shift-From supports replication only from Amazon S3.

- **HTTP:** HTTP isn't supported. All Qumulo connections are encrypted using HTTPS and verify the S3 server's SSL certificate.

- **Anonymous Access:** Anonymous access isn't supported. You must use valid AWS credentials.

- **Replication without Throttling:** Replication provides no throttling and might use all available bandwidth. If necessary, use Quality of Service rules on your network.

- **Amazon S3 Standard Storage Class:** Qumulo Shift-From supports downloading only objects stored in the Amazon S3 Standard storage class. You can't download objects stored in the Amazon S3 Glacier or Deep Archive storage classes and any buckets that contain such objects cause a copy job to fail.

- **Disallowed Amazon S3 Paths in Qumulo Clusters:** Certain allowed Amazon S3 paths can't be copied to Qumulo clusters and cause a copy job to fail. Disallowed paths contain:

    - A trailing slash (`/`) character (with non-zero object content length)

    - Consecutive slash (`/`) characters

    - Single and double period (`.` , `..`) characters

    - The path component `.snapshot`

- **Disallowed Conflicting Types:** When content in an S3 bucket or Qumulo directory changes over time, a conflict related to type mismatches might arise, the Shift-from job fails, and an error message gives details about the conflict. For example, a conflict might occur when a remote object maps to a local file system directory entry which:

    - Is a regular file with two or more links

- ◦ Isn't a regular file (for example, a directory or a special file)

- **Disallowed Amazon S3 Path Configurations:** Because of conflicting type requirements, Qumulo Core can't recreate certain allowed Amazon S3 path configurations on Qumulo clusters. For example, if an S3 bucket contains objects `a/b/c` and `a/b` , then path `a/b` must be both a file and directory on a Qumulo cluster. Because this isn't possible, this configuration causes a copy job to fail.

- **Directories in Multiple Relationships:** A directory on a Qumulo cluster for one Shift relationship can't overlap with a directory used for another Shift relationship, or with a remote directory for a Qumulo-to-Qumulo replication relationship. This causes the relationship creation to fail.

- **Changes to S3 Folder During Copy Job:** Currently, Shift-From assumes that the S3 folder remains unchanged throughout the copy job. Any changes (deleting, archiving, or modifying an object) during the copy job might cause a copy job to fail.

- **Read-Only Local Directory:** When the Shift-From copy job begins, the local directory on the Qumulo cluster becomes read-only. While no external clients can modify anything in the directory or its subdirectories, all content remains readable. When the copy job is complete, the directory reverts to its previous permissions.

- **Partially Downloaded Files:** If a copy job is interrupted or encounters a fatal error (that can't be resolved by retrying the operation), Qumulo Core attempts to delete partially downloaded files. Because this is a best-effort process, certain interruptions can prevent the cleanup of partially downloaded files.

Identifying NICs and Choosing Transceivers and Cables for Your Qumulo Node

Identifying NICs and Choosing Transceivers and Cables for Your Qumulo Node

This section explains how to identify your node's NICs and choose the correct transceivers and cables for your Qumulo nodes.

Identifying the NICs in Your Node

The following table lists node types and their NICs and the NICs' speed and latest firmware that Qumulo supports.

Node Type	NIC	Speed	Latest Firmware Qumulo Supports
C-192T	ConnectX-5	100 Gbps	16.28.1002
C-432T	ConnectX-5	100 Gbps	16.28.1002
HPE ProLiant DL325 Gen10 Plus	ConnectX-6	100 Gbps	22.31.1014
K-432T	ConnectX-5	25 Gbps	16.28.1002
P-23T	ConnectX-5	100 Gbps	16.28.1002
P-92T	ConnectX-5	100 Gbps	16.28.1002
P-184T	ConnectX-5	100 Gbps	16.28.1002

Node Type	NIC	Speed	Latest Firmware Qumulo Supports
P-368T	ConnectX-5	100 Gbps	16.28.1002
Supermicro A+ WIO 1114S-WN10RT	ConnectX-6	100 Gbps	22.31.1014

Choosing Transceivers for Your Node

The two main types of fiber optic cables are the Lucent connector (LC) with two fibers (commonly used for 10 Gbps and 25 Gbps connections) and the multi-fiber push on (MPO) connector with eight fibers (commonly used for 40 Gbps connections). Although there are transceivers that can use LC fiber optic cables for 40 Gbps and 100 Gbps connections, these transceivers are generally more expensive, consume more power, and are mainly intended for reusing LC cabling or for long-distance applications.

Newer switches have 100 Gbps connections using double 50 Gbps PAM4 connections instead of the more common four 25 Gbps connections. However, the most common and cost-efficient transmission standard for 100 Gbps is SR4, with four QSFP28 connections over an eight-fiber cable. The maximum range for SR4 is 100 m. The most common transmission standard for 25 Gbps is the Lucent connector duplex (LC duplex) with two fibers. The maximum short-range connection is 100 m and long-range connection is 10 km. There is also an extended-range standard with a maximum of 40 km.

Recommended Optical Transceivers for 100 Gbps Connections

Note: Mellanox 100 Gbps NICs also work with 40 Gbps connections.

Speed	Part Number	Description
100 Gbps LR4	MMA1L10-CR	Mellanox QSFP28 Long-Range Transceiver
100 Gbps SR4	MMA1B00-C100D	Mellanox QSFP28 Short-Range Transceiver

Speed	Part Number	Description
100 Gbps SR4	QSFP28-SR4-100G	FS Arista and Mellanox Short-Range Transceivers

Recommended Optical Transceivers for 25 Gbps Connections

Speed	Part Number	Description
25 Gbps LR	MMA2L20-AR	Mellanox SFP28 Long-Range Transceiver
25 Gbps SR	MMA2P00-AS	Mellanox SFP28 Short-Range Transceiver
25 Gbps SR	SFP28-25GSR-85	FS Arista and Mellanox Short-Range Transceivers

Choosing Cables for Your Transceiver

- **Optical Cables:** We recommend using optical cables and optical transceivers that both the NIC and the switch support.

- **Direct Attach Cables (DACs):** Although these cables are significantly cheaper than optical cables and are less prone to compatibility and thermal issues, they are limited in length (2-3 m, up to 5 m maximum).

- **Active Optical Cables (AOCs):** Although these cables are cheaper than dedicated transceivers and fiber optic cables, they might cause compatibility issues, or your NIC or switch might not support them.

Note: If you use DAC or AOC cables, ensure that Mellanox and the maker of your network switch both support your cables.

Recommended 100 Gbps DAC and AOC Cables

Manufacturer	Part Number	Description	Length
Amphenol	NDAAFF-C403	100 Gbps Passive Copper Cable	3 m

Manufacturer	Part Number	Description	Length
FS	Q28-PC02	100 Gbps Passive Copper Cable	2 m
FS	Q28-PC03	100 Gbps Passive Copper Cable	3 m
Leoni	L45593-D218-B50	100 Gbps Passive Copper Cable	3 m

Replacing the Chassis of C-192T and C-432T Nodes

Replacing the Chassis of C-192T and C-432T Nodes

This section explains how you can replace the chassis in C-192T and C-432T nodes.

Prerequisites

Before you begin, ensure that you have C-192T or C-432T hardware and the replacement chassis.

Step 1: To Prepare for Chassis Replacement

**Note:** We strongly suggest having another person help you with this process.

1. To shut down the node, use the power button at the front or connect using SSH and run the `sudo shutdown -h now` command.

2. Disconnect all cables from the back of the node.

3. To pull the node out from the rack, release the small, white tabs on the rails that hold the chassis in place.

4. Place the node on a flat surface.

5. To release the lid, remove the small screw on the upper-right side of the node (viewed from the rear).

6. Press the large **PUSH** button on each side of the chassis frame.

The inner components of the node are exposed.

Step 2: To Replace the M.2 Boot Drive, NVMe SSDs, and HDDs

1. Remove the internal M.2 boot drive and then transfer it into the replacement chassis Qumulo provided to you.
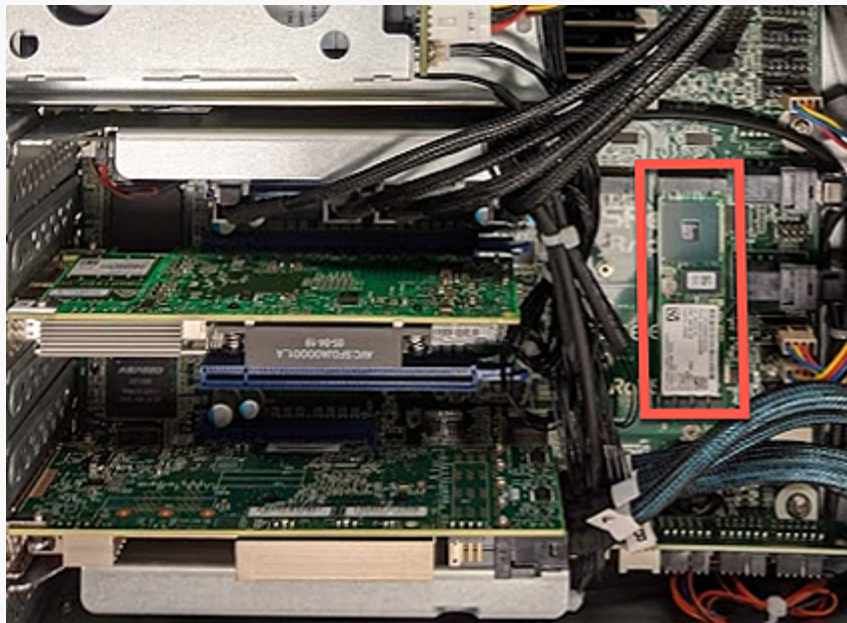
2. Remove the rear NVMe SSDs and then transfer them into the replacement chassis. The following is the mapping for the drives.

6	4	2

5   3   1

3. To allow the HDD trays to slide open, ensure that any shipping screws are removed from the replacement chassis.

4. Install the replacement chassis in an appropriate location in your server rack.

5. Starting with the top drawer, transfer the HDDs from each tray in the original chassis into a corresponding slot in the replacement chassis. For more information about drive locations, see C-Series Drive Diagrams in Qumulo Care.

    Important: Work on one drawer at a time. If you apply 2 kg (or more) of downward force to a drawer, it might deform while opened.

    a. To open the HDD drawer, use the blue lever at the front of the node.

    b. To remove an HDD from the original chassis, gently lift up the drive tray knob. This lets the drive move forward and unlatch.
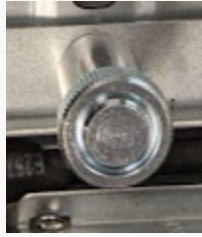
c. To insert an HDD into the replacement chassis, gently slide the drive tray knob backwards. This latches the drive and knob in place.

6. Reconnect the power and networking cables to the node.

7. Power on the node.

Step 3: (Optional) Reconfiguring the Out-of-Band Management (IPMI) Settings

If the current IPMI settings for your node are configured statically (rather than using DHCP), you must reapply the static IPMI settings to the replacement node. For more information, see IPMI Quick Reference Guide for Qumulo C-Series in Qumulo Care.