Volumes overview

Snapshots, replicas, and clones are based on volumes. Unlike most SAN solutions, CompanyX clones can be created instantly and use almost zero storage capacity by sharing identical blocks with the source volume. They are often used to develop or test applications before putting them into production. Most volume properties are set at the time you create a volume, but some modifications can be made to volumes later.

Proper planning will minimize the need for adjustments. Before creating volumes, you should understand space management, the workload, and application space requirements.

➡ **Note:** In the context of the CompanyX array, the term "volume" and "LUN" (logical unit number) are synonymous and interchangeable.

Logical vs Physical Space

When working with volumes, it is important to understand the difference between logical space and physical space.

Physical storage resources are aggregated into storage pools from which the logical storage is created. It allows you to have a logical space for data storage on physical storage disks by mapping space to the physical location. Physical space is the actual space on the hardware that is used. For example, when you set a volume or snapshot reserve, that physical space is reserved and taken out of the general pool of space. It is physical resource consumption.

Logical space is space that the system manages, such as the volume size. In this case, the volume size is not (necessarily) the actual amount of space on a physical disk, but the amount of space defined for a volume, which may span multiple physical disks.

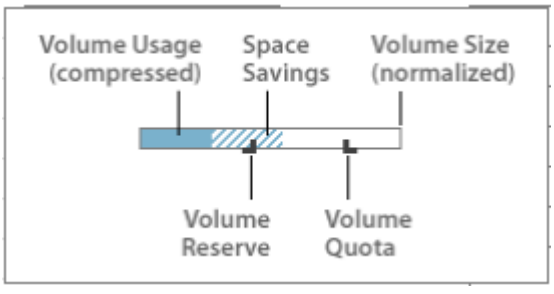
Space management

The CompanyX array has built-in capacity saving mechanisms such as inline compression and thin provisioning. The following considerations help you plan your space configuration for volumes and snapshots.

The simplest form of space management is to not use reserves at all. This means that there is no dedicated (pre-reserved) space per volume taken from the general storage pool, so all volumes can consume what they need as it is needed. This method requires that you monitor space usage to ensure that there is always space available.

However, for critical volumes, such as those hosting business-critical data, it may be more important for you to set a reserve to ensure that the volume will always have enough space. Setting the reserve immediately takes the reserve amount of space from the storage pool.

When you create a volume, you define a certain amount of space for that volume. This is the **volume size**: it is the size that is reported to your application.



The **volume reserve** is the guaranteed minimum amount of physical space reserved for the volume. Reserved space is set aside for the volume and is immediately withdrawn from the general storage pool. Set the volume

reserve from 100% (the entire physical space is reserved) to 0% (no physical space is reserved). As new data is written to the volume, the free space within the volume reserve decreases. You can increase the volume reserve if needed. One consideration when setting volume sizes and reserves is the level of compression you get for a particular application or data set. For example, most volumes should see 2 to 4x compression, so a volume reserve set to 10 GB will be able to store far more than the actual 10 GB space if it were uncompressed. In other words, 10 GB space of application data will only use between 2.5 GB and 5 GB when compressed.

Thin provisioning is a storage virtualization technology that uses physical storage only when data is written instead of traditional provisioning, which reserves all the capacity up-front when an application is configured. This method addresses overprovisioning and its associated costs. Often, volumes reserve excessive space against unexpected growth. Often this growth does not materialize, or materializes much later than expected. With thin provisioning, you create volumes and assign them to servers and applications, but the physical resources are only assigned when the data is written. Physical storage not being used remains available to other volumes. No unnecessary storage is reserved for use by any single application. **Setting the reserve to 100% effectively disables thin provisioning**.

For example, like most SANs, your array must support several applications. Projections show that eventually the total storage needed by all applications will reach 3 TB. However, for the first few quarters of the year, these applications should only use about 300 GB. Instead of creating the volumes using the total 3 TB that you expect to need, with thin provisioning you can create three 1 TB volumes, but set the reserve to only 150 GB for each volume. Especially when you factor in compression savings, the applications should not use the full 3 TB until the next purchasing window, minimizing the cost of buying more capacity until it is needed.

➡ **Note:** When formatting a CompanyX array volume always use the "quick format" option. Do not defragment volumes on a CompanyX array.

Best practices for thinly provisioned LUNs can be found at in the article at *http://support.microsoft.com/kb/959613* of the Microsoft Knowledge Base.

Volume quotas determine how much of volume can be consumed before writes are disallowed.

Best practice: Set the quota to 100% (no quota). Some applications do not tolerate changes to volume sizes. Quotas were developed to address this issue: using quotas lets you set a limit but leave room in case more space is needed.

For example, if you have an application that you do not want to fill all the space on the volume before more space is available for expansion, set a quota for the volume. You now have a safety factor: when the quota is met, you can reset the quota, giving more space to the application. You can then plan for further expansion if necessary.

If the volume is approaching the quota limit, an event is logged. If enforcement is enabled, the administrator can access the system log to determine what follow-up actions to take, such as preventing the user from accessing more disk space or allocating additional disk space to the user.

A write is successfully acknowledged only after the system ensures that there is space for it on the dense disk and the write is stabilized in NVRAM.

Cloning space considerations

Clones are space-efficient copies of a volume that can be used independently of the source volume. When created, they have the same settings as the volume from which they were created. Clones share blocks that are identical with the source volume, and only begin to use space when changes are made.

It is strongly recommended that you lower the reserve settings for clones. When determining the reserve settings, factors to consider include how long-lived the clone will be and how much the clone will vary from its source. For example, the reserve settings may not need to be very high if the close is being run to test a new application against, will not be changed much, and will be deleted after the testing is complete.

You cannot delete the source volume of a clone unless the clone is also deleted.

Network connections

Volumes appear on the network as iSCSI targets. The iSCSI target name is generated internally: you do not create the name. When your iSCSI initiator connects to the target (volume), the volume can be mapped to your network and appear just like any other mapped drive. Initiators work like clients to the array and servers to the application. You can track how many connections there are to each volume from the **Monitor** > **Connections** menu.

Protecting data using snapshots

Snapshots ensure that data stored in volumes is always recoverable.

Merging primary and backup storage on the CompanyX array makes snapshots an efficient method to protect data. Because no data needs to be copied outside the array, snapshots can be created and can be used to restore data almost instantaneously.

Snapshots are part of the converged storage and backup, and because they are so efficient, consider the implications when creating snapshots. For some applications, the amount of storage used for snapshots may equal or exceed the storage needed for the source volume. Reserving storage for snapshots does not reserve the space from the space allocated to the volume, but from the general storage pool.

You may need to synchronize the snapshot schedules with certain applications (such as Microsoft Exchange or SQL servers) to avoid inconsistent snapshots.

Volume collections let you automate snapshot schedules based on common usage scenarios. Create your own sets, using the predefined collections provided as templates. For details, see *Creating a volume collection*.

➡ **Important:** Only one schedule within the set can use replication. You can create daily, weekly, and monthly schedules for a volume collection, but only one of those schedules can be replicated.

Even if you plan to take snapshots of volumes manually or using a third-party program such as Backup Exec, create a volume collection without schedules on those volumes whose snapshots are being done manually.

Limiting access to volumes

Security is important when managing a SAN. The CompanyX array offers two methods to limit access to each volume in the system: iSCSI initiator groups and CHAP authentication. Use either method individually, or use both for more security.

Access to snapshots taken from the volume are inherited by the volume controls, and is set when you create the volume. Access can be modified after the initial creation.

iSCSI Initiator Groups

A common method for limiting access is to create groups of iSCSI initiators that are managed as a single unit. iSCSI initiator groups can be based on OS, application, or any other logical common requirement. All members of the iSCSI group are granted access to the target volume.

See *iSCSI initiators* for details about iSCSI initiators and their role.

For information about creating iSCSI initiator groups, see your iSCSI documentation. You can create iSCSI initiator groups using the CLI command `initiatorgrp --create`. See the *Command Line Reference* for details.

CHAP Authentication

Another way to manage access is *Challenge Handshake Authentication Protocol*, or CHAP. Many administrators find this a more convenient method, because it uses names and passwords instead of iSCSI initiator names that can be long and complicated.