The term backup has become synonymous with data protection over the past several decades and may be accomplished via several methods. Backup software applications have been developed to reduce the complexity of performing backup and recovery operations. Backing up data is only one part of a disaster protection plan, and may not provide the level of data and disaster recovery capabilities desired without careful design and testing.

The purpose of most backups is to create a copy of data so that a particular file or application may be restored after data is lost, corrupted, deleted or a disaster strikes. Thus, backup is not the goal, but rather it is one means to accomplish the goal of protecting data. Testing backups is just as important as backing up and restoring data. Again, the point of backing up data is to enable restoration of data at a later point in time. Without periodic testing, it is impossible to guarantee that the goal of protecting data is being met.

Backing up data is sometimes confused with archiving data, although these operations are different. A backup is a secondary copy of data used for data protection. In contrast, an archive is the primary data, which is moved to a less-expensive type of media (such as tape) for long-term, low-cost storage.

Backup applications have long offered several types of backup operations. The most common backup types are a full backup, incremental backup and differential backup. Other backup types include synthetic full backups, mirroring, reverse incremental and continuous data protection (CDP).

Full backups

The most basic and complete type of backup operation is a full backup. As the name implies, this type of backup makes a copy of all data to another set of media, which can be tape, disk or a DVD or CD. The primary advantage to performing a full backup during every operation is that a complete copy of all data is available with a single set of media. This results in a minimal time to restore data, a metric known as a recovery time objective (RTO). However, the disadvantages are that it takes longer to perform a full backup than other types (sometimes by a factor of 10 or more), and it requires more storage space.

Thus, full backups are typically run only periodically. Data centers that have a small amount of data (or critical applications) may choose to run a full backup daily, or even more often in some cases. Typically, backup operations employ a full backup in combination with either incremental or differential backups.

Incremental backups

An incremental backup operation will result in copying only the data that has changed since the last backup operation of any type. The modified time stamp on files is typically used and compared to the time stamp of the last backup. Backup applications track and record the date and time that backup operations occur in order to track files modified since these operations.

Because an incremental backup will only copy data since the last backup of any type, it may be run as often as desired, with only the most recent changes stored. The benefit of an incremental backup is that they copy a smaller amount of data than a full. Thus, these operations will complete faster, and require less media to store the backup.

Differential backups

A differential backup operation is similar to an incremental the first time it is performed, in that it will copy all data changed from the previous backup. However, each time it is run afterwards, it will continue to copy all data changed since the previous full backup. Thus, it will store more data than an incremental on subsequent operations, although typically far less than a full backup. Moreover, differential backups require more space and time to complete than incremental backups, although less than full backups.