9.13.2 Backup and Restore Facts

Backup is the process of copying data to a second form of storage, such as tape, recordable optical media (CD-R and DVD-R), removable hard disk, flash drive or solid state drive. Backups protect data by providing a second copy that can be available in case the original data is lost, modified, or corrupted.

Most backup methods use the archive bit on a file to identify files that need to be backed up. When a file is modified, the system automatically flags the file as ready to be archived. When the file is backed up, the backup method may reset (clear) the archive bit to indicate that the file has been backed up.

The following table compares how different backup types work:

Backup Type	Function	Resets the Archive Bit
Full	Backs up all files regardless of the archive bit.	Yes
Incremental	Backs up files on which the archive bit is set. This will back up only the data changed since the last full or incremental backup.	Yes
Differential	Backs up files on which the archived bit is set. This will back up only the data changed since the last full backup.	No
Image	Takes a bit-level copy of a disk or partition. Individual files are not examined, so all data is copied regardless of the archive bit. A snapshot is an example of an image.	No
Copy	Backs up all files regardless of the archive bit status.	No
Daily	Backs up all files modified that day regardless of the archive bit status.	No

Most of the time, you will perform backups using a strategy that combines backup types. The following table compares common backup strategies:

Strategy	Characteristics	Restore Characteristics
Full Backup	Requires large amounts of storage for each backup. Takes the longest time to perform each backup.	To restore, restore only the last backup. This is the fastest restore method.
Full + Incremental	Full backup performed periodically (for example, once per week), followed by incremental backups (for example, once each day). Incremental backups are quick to perform. This is the fastest backup method.	To restore, restore the full backup and every subsequent incremental backup.
Full + Differential	Full backup performed periodically (for example, once per week) followed by differential backups (for example, once each day). Differential backups take progressively longer to complete as the period of time increases since the last full backup.	To restore, restore the last full backup and the last differential backup. Next to a full backup, this is the fastest restore method.

Restore is the process of copying backup data to its original storage location. Backup data is of no use unless it can be properly read and restored.

If data has been corrupted by malicious attacks, attempts to restore clean data may result in the data being re-infected by malicious logic that is present as part of the attack. You may need to use live boot media to perform the restore, especially if you are restoring the operating system. *Live boot media* is a complete bootable computer installation that contains an operating system. It is usually written to a CD, DVD or USB flash drive. When booted, this operating system runs entirely from memory without mounting any other media, including a hard drive that may contain malicious logic. Using live boot media, you can overwrite a corrupted disk from uncorrupted backups.