12.11.2 Backup Facts

A *backup* is a copy of data that is archived and which can be used to restore corrupt or lost data in the event of a hardware or system failure. Backups must be performed while the system is in good working order. In other words, you must plan for disasters ahead of time and take the necessary actions to protect your system before there is a problem.

Backup tools may be used to protect different types of data:

- *System state* data includes all of the files required to boot and run the computer. System state data includes the operating system files, the registry, drivers, and any configuration files.
- *User data* includes all data files saved and modified by users or applications that users run. The user data is the most important data for a company. Because user data changes constantly, back up the user data frequently and on a regular schedule.
- *Application data* includes files installed by an application and application configuration files. Application data changes only following the installation of an application or following a configuration change. Depending on the system you are using, a backup of system state data might include backing up all application files as well.

Use the following two tools to protect Windows 10 systems:

Windows Version	Tools
Backup and Restore (Windows 7)	Microsoft 10 includes the Backup and Restore feature from Windows 7. Backup and Restore (Windows 7) was available in Windows 8, removed in Windows 8.1, but was returned in Windows 10. The Backup and Restore (Windows 7) tool is intended to allow you to restore any of your old Windows 7 backups onto your Windows 10 computer. The tool can also back up your Windows 10 PC in the exact same way you would back up a Windows 7 PC. This Backup and Restore (Windows 7) process can be found by doing the following steps: 1. Select **Start**. 2. Select **Windows System**. 3. Select **Control Panel**. 4. In Control Panel, **System and Security**. 5. Select **Backup and Restore (Windows 7)**. A *create a system image* backs up everything on the system to a .vhd file, including the operating system, installed programs, drivers, and user data files. A system image backup is the most complete type of backup, but also takes the longest time to create. A *file backup* backs up specific files and folders up to a compressed file. File backups do not include system files, program files, encrypted files, files in the Recycle Bin, user profile settings, or temporary files. On Backup and Restore (Windows 7), backups can be saved to several different types of storage media: - Secondary internal hard drives - External hard drives - Optical drives - USB flash drives - Network shares Backup files cannot be saved to: - The same disk that is being backed up - A disk containing the Windows operating system - A tape drive System images created with the Backup and Recovery Console cannot be saved to: - Flash memory - A tape drive - A recordable DVD On Backup and Restore (Windows 7), file backups occur every Sunday at 7:00 pm by default. However, the backup schedule can be customized. A system image backup cannot be scheduled, but a system image backup can be included within a scheduled file backup. Backup and Restore (Windows 7) also provides a System Protection feature which can be enabled for volumes used to store user data. With System Protection enabled, you can restore previous versions of data files when needed.
File History	The Backup and Restore console used to backup data on Windows 7 is not included in Windows 8.1. Instead, *File History* is used in Windows 8.1. Both are available for Windows 8.1 and Windows 10 to backup user profiles. A profile backup includes all of the information stored in the user's library folders: - User data files, such as documents, music, and videos - User preferences, such as the desktop background, screensaver, color schemes, contacts, browser favorites, and so on - User account details, such as the username, password, and so on

File History does not back up the entire system. Only the data in a user's profile is backed up. However, a user can add folders to a library to back them up using File History. File history backs up files in the background. Once every hour, File History creates a shadow copy of user account files. This creates a snapshot of user account's files at a particular point in time. After creating the shadow copy, Windows keeps track of the prior versions of those files. Once done, users can browse and restore previous versions of files.

File History is disabled by default. When enabling File History, the location for storing the backup must be specified. A drive other than the drive the user files are already on must be specified. At least two drives must be implemented for the system to use File History. A best practice is to use a second internal hard disk drive. However, external flash drives or hard disks can also be used. In this configuration, File History must be disabled before disconnecting the external drive.

When File History is enabled, Windows monitors users' libraries, desktop, contacts, and Internet Explorer favorites. By default, File History checks once an hour to see if any data has changed since the last check. If it has, File History saves copies of the changed files to the configured location. Once done, a previous version of a file can be restored if a file gets lost or corrupted.

Windows 10 also supports the creation of system images. Where File History backs up only user files, a system image backs up the entire system, including operating system files, registry settings, installed applications, and so on.

Keep the following considerations in mind about File History:

- To protect user data, File History is the best option because lost or corrupted files can be quickly restored.
- To protect the system itself, a system image is the best choice because it can be used to restore the entire computer. Individual files can't be restored from a system image backup.

Keep the following facts in mind when configuring backups:

- Back up user data more often than system state data (it changes more frequently).
- Back up system state data and applications (or make a restore point) before you make a system change.
- During a system state backup, all system configuration information is backed up (system data cannot be backed up selectively in portions).
- Be sure to test your backup and restore strategy. It does no good to back up your data if you can't restore it.
- Backup media should be stored offsite to prevent the same disaster from affecting the network and the backup media.
- Backups can be scheduled using the tools within the backup utility, or by creating a new task in the Scheduled Tasks folder in the Control Panel.