When you install Windows and configure various server roles, special shared resources are created to support those roles. You shouldn't disturb these special shares unless you know what you're doing. Table 13-3 lists some of the most common special shares.

TABLE 13-3 **Special Shares**

Share Name	Description
`drive$`	The root directory of a drive.
`ADMIN$`	Used for remote administration of a computer. This share points to the OS folder (usually, C:\Windows).
`IPC$`	Used by named pipes, a programming feature that lets processes communicate with one another.
`NETLOGON`	Required for domain controllers to function.
`SYSVOL`	Another required domain controller share.
`PRINT$`	Used for remote administration of printers.
`FAX$`	Used by fax clients.

Notice that some of the special shares end with a dollar sign ($). These shares are hidden shares, not visible to users. You can still access them, however, by typing the complete share name (including the dollar sign) when the share is needed. The special share `C$`, for example, is created to allow you to connect to the root directory of the `C:` drive from a network client. You wouldn't want your users to see this share, would you? (Shares such as `C$` are also protected by permissions, of course, so if an ordinary user finds out that `C$` is the root directory of the server's `C:` drive, he still can't access it.)

Managing Your File Server

To manage shares on a Windows Server 2019 system, open the Server Manager, and select File and Storage Services in the task pane on the left side of the window. Then click Shares to reveal the management console shown in Figure 13-1.

The following sections describe some of the most common procedures that you'll use when managing your file server.