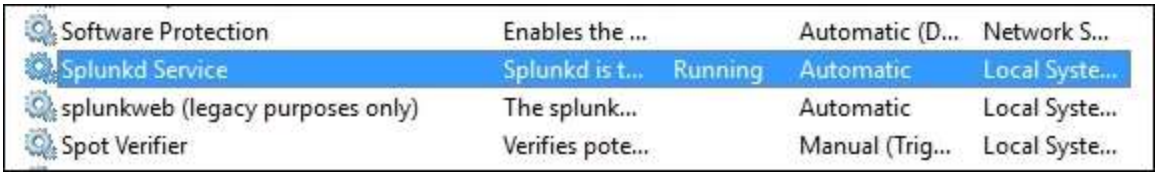
Controlling Splunk

There are several different ways to stop, start, or restart Splunk. The easiest way is to do it from the web interface, as demonstrated in the preceding section. The web interface, however, only allows you to restart your Splunk instance. It does not offer any other control options.

In Windows, you can also control Splunk through the **Splunkd Service** as shown in the following screenshot. The *d* in the service name, denoting *daemon*, means a background process. Note that the second service, **splunkweb**, is not running. Do not try to start **splunkweb** as it is deprecated and is only there for legacy purposes. The Splunk web application is now bundled in **Splunkd Service:**



The best way to control Splunk is by using the **command-line interface**(**CLI**). It may require a little effort to do it, but using the CLI is an essential skill to learn. Remember to always use command prompts in Administrator mode.

In the console or command prompt, type in the following command and hit **Enter** on your keyboard:

```
C:\> cd \Splunk\bin
```

Here `cd` is a command that means *change directory*.

While in the `C:\Splunk\bin` directory, issue the following command to restart Splunk:

```
C:\> C:\Splunk\bin> splunk restart
```

After issuing this command, splunkd will go through its restart process. Here are the other basic parameters that you can pass to the Splunk application to control Splunk:

- `splunk status`: Tells you if splunkd is running or not
- `splunk stop`: Stops splunkd and all its processes
- `splunk start`: Starts splunkd and all its processes
- `splunk restart`: Restarts splunkd and all its processes

Doing this in the console gives the added benefit of verbose messages. A verbose message is a message with a lot of information in it. Such messages can be useful for making sure the system is working correctly or troubleshooting any errors.

A successful restart of splunkd has the following output (which may vary):