

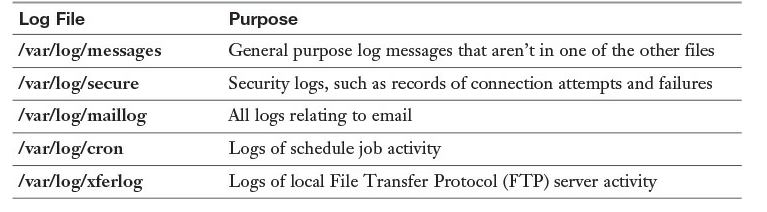
Most of the patterns in [Example 18-6](ch18.html#ch18ex06) have a single facility and a selector of \*, which means any severity will match. This could also have been written with a severity of **debug**, as that is the lowest severity possible. Thus, **authpriv.\*** matches all the private authentication messages. If the destination part of the rule is a filename, the logs go to that file.

The line associated with the mail facility has a dash (**-**) in front of the destination. This tells syslogd that it shouldn’t commit each log entry to disk as it’s logged but to let the kernel write to disk when it has time, as the mail facility can log heavily and this improves performance at a cost of potential lost data after a crash.

The second selector has more than one pattern; each is separated by a semicolon (**;**). The first pattern matches any facility at info level or greater, and the remaining three use the special **none** severity to ignore any log coming from mail, authpriv, or cron. This is because those logs have their own files and this eliminates duplication.

The **\*.emerg** selector matches any log at the emergency level and sends it to a special destination of **\***, which means to send a message to the console of anyone logged in to the system.

While individuals are free to place logs wherever they want, several conventions have emerged to make logs easier to find as you move from system to system (see [Table 18-5](ch18.html#ch18tab05)).



**Table 18-5** Common Logs and Their Location

Splitting each major application into its own log files makes it easier to find what you want and doesn’t mingle logs between two applications when you are reviewing them. A common pattern is to watch a log in real time, also called “following a log.” To follow a log, run **tail -f logfile**, such as **tail -f /var/log/secure** to watch for people logging in.