NAME

cups-lpd − receive print jobs and report printer status to lpd clients

SYNOPSIS

cups-lpd [**−h** *hostname*[**:***port*]] [**−n**] [**−o** *option*=*value*]

DESCRIPTION

cups-lpd is the CUPS Line Printer Daemon ("LPD") mini-server that supports legacy client systems that use the LPD protocol. **cups-lpd** does not act as a standalone network daemon but instead operates using any of the Internet "super-servers" such as **inetd**(8), **launchd**(8), and **systemd**(8).

OPTIONS

-h *hostname*[**:***port*]
: Sets the CUPS server (and port) to use.

−n
: Disables reverse address lookups; normally **cups-lpd** will try to discover the hostname of the client via a reverse DNS lookup.

-o *name=value*
: Inserts options for all print queues. Most often this is used to disable the "l" filter so that remote print jobs are filtered as needed for printing; the **inetd**(8) example below sets the "document-format" option to "application/octet-stream" which forces autodetection of the print file format.

CONFORMING TO

cups-lpd does not enforce the restricted source port number specified in RFC 1179, as using restricted ports does not prevent users from submitting print jobs. While this behavior is different than standard Berkeley LPD implementations, it should not affect normal client operations.

The output of the status requests follows RFC 2569, Mapping between LPD and IPP Protocols. Since many LPD implementations stray from this definition, remote status reporting to LPD clients may be unreliable.

ERRORS

Errors are sent to the system log.

FILES

/etc/inetd.conf
/etc/xinetd.d/cups-lpd
/System/Library/LaunchDaemons/org.cups.cups-lpd.plist

NOTES

PERFORMANCE

cups-lpd performs well with small numbers of clients and printers. However, since a new process is created for each connection and since each process must query the printing system before each job submission, it does not scale to larger configurations. We highly recommend that large configurations use the native IPP support provided by CUPS instead.

SECURITY

cups-lpd currently does not perform any access control based on the settings in *cupsd.conf(5)* or in the *hosts.allow(5)* or *hosts.deny(5)* files used by TCP wrappers. Therefore, running **cups-lpd** on your server will allow any computer on your network (and perhaps the entire Internet) to print to your server.

While **xinetd**(8) has built-in access control support, you should use the TCP wrappers package with **inetd**(8) to limit access to only those computers that should be able to print through your server.

cups-lpd is not enabled by the standard CUPS distribution. Please consult with your operating system vendor to determine whether it is enabled by default on your system.

EXAMPLE

If you are using **inetd**(8), add the following line to the *inetd.conf* file to enable the **cups-lpd** mini-server:

```
printer stream tcp nowait lp /usr/lib/cups/daemon/cups−lpd cups−lpd \
  −o document−format=application/octet−stream
```

Note: If you are using Solaris 10 or higher, you must run the **inetdconv**(1m) program to register the changes to the *inetd.conf* file.

CUPS includes configuration files for **launchd**(8), **systemd**(8), and **xinetd**(8). Simply enable the **cups-lpd** service using the corresponding control program.

SEE ALSO

cupsd(8), **inetd**(8), **launchd**(8), **xinetd**(8), CUPS Online Help (http://localhost:631/help), RFC 2569

COPYRIGHT