ShellHacks (https://www.shellhacks.com/)

Linux Hacks and Guides

BLOG (HTTPS://WWW.SHELLHACKS.COM/CAT/BLOG/)

Linux Proxy Server Settings – Set Proxy For Command Line

Posted on Tuesday December 27th, 2016 (https://www.shellhacks.com/linux-proxy-server-settings-set-proxy-command-line/) by admin (https://www.shellhacks.com/author/admin/)

(https://www.shellhacks.com/linux-proxy-server-settings-set-proxy-command-line/)

To use a proxy on the Linux command-line, you can set the environment variables `http_proxy`, `https_proxy` or `ftp_proxy`, depending on the traffic type.

These proxy server settings are used by the almost all Linux command-line utilities, e.g. `ftp`, `wget`, `curl`, `ssh`, `apt-get`, `yum` and others.

If you don't know yet which proxy server to use, you can take one from the lists of the free public proxy servers at the end of this article.

> **Cool Tip:** Need to improve security of the Linux system? Encrypt DNS traffic and get the

> protection from DNS spoofing! Read more → (/encrypt-dns-traffic-dnscrypt/)

Export Proxy Server Settings

Set these variables to configure Linux proxy server settings for the command-line tools:

```
$ export http_proxy="http://PROXY_SERVER:PORT"
$ export https_proxy="https://PROXY_SERVER:PORT"
$ export ftp_proxy="http://PROXY_SERVER:PORT"
```

If a proxy server requires authentication, set the proxy variables as follows:

```
$ export http_proxy="http://USER:PASSWORD@PROXY_SERVER:PORT"
$ export https_proxy="https://USER:PASSWORD@PROXY_SERVER:PORT"
$ export ftp_proxy="http://USER:PASSWORD@PROXY_SERVER:PORT"
```

> **Special Characters:** If your password contains special characters, you must replace them with ASCII codes (http://www.ascii-code.com/), for example the at sign `@` must be replaced by the `%40` code, e.g. `p@ssword = p%40ssword`.

Test The Proxy Server From The Linux Command-Line

As only you have configured a proxy it is time to ensure that it works as expected.

First off all it is required to check that the proxy server settings are set in the corresponding proxy variables.

Than it is required to ensure that your public IP address has changed.

Also it would be interesting to measure and compare response time of the remote resources and the Internet speed with and without proxy.

Check the current proxy server settings:

```
$ env | grep -i proxy
```

Check your public IP address from the Linux command-line:

```
$ wget -q -O - checkip.dyndns.org \
| sed -e 's/.*Current IP Address: //' -e 's/<.*$//'
```

Compare the difference in the response time with the configured proxy and without it:

```
$ time wget -q -O - checkip.dyndns.org \
| sed -e 's/.*Current IP Address: //' -e 's/<.*$//'
```

Check the Internet download speed through the proxy:

```
$ wget --output-document=\
/dev/null http://speedtest.wdc01.softlayer.com/downloads/test500.zip
```

Unset Linux Proxy Variables

Use the following commands to disable proxy:

```
$ unset http_proxy
$ unset https_proxy
$ unset ftp_proxy
```

> **Cool Tip:** Stay anonymous during port scanning! Use `Nmap + Tor + ProxyChains` ! Safe and easy penetration testing! Read more → (/anonymous-port-scanning-nmap-tor-proxychains/)

Automate Proxy Server Settings In Linux

If you use the same proxy server settings for the `https`, `http` and `ftp` traffic, you can use the following commands to set and unset the proxy settings:

```
$ export {http,https,ftp}_proxy="http://PROXY_SERVER:PORT"
$ unset {http,https,ftp}_proxy
```

If you use a proxy server often, you can create Bash functions as follows (add to your `~/.bashrc` file):

```
# Set Proxy
function setproxy() {
    export {http,https,ftp}_proxy="http://PROXY_SERVER:PORT"
}

# Unset Proxy
function unsetproxy() {
    unset {http,https,ftp}_proxy
}
```

Reload your `~/.bashrc` file.

```
$ source ~/.bashrc
```

Now use the `setproxy` and `unsetproxy` commands to set and unset Linux proxy server settings.

Lists of Free Public Proxy Servers

> **WARNING:** Free public proxy servers can insert your IP address into the headers of requests or sniff your traffic! Don't use them to transfer sensitive data and do not expect anonymity!

- Hide My Ass (http://www.hidemyass.com/proxy-list/)
- Proxy Server List (http://www.proxynova.com/proxy-server-list/)
- Anonymous Public Proxy Servers (http://spys.ru/en/)

- Daily HTTP Proxies (http://public-proxy.blogspot.com/)

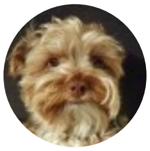
> **Cool Tip:** Even if you use proxy server, all your DNS queries still go to the name servers of your ISP (Internet Service Provider)! Improve anonymity, by using free public name servers! Read more → (/free-fast-public-dns-servers/)

Comment (1) (https://www.shellhacks.com/linux-proxy-server-settings-set-proxy-command-line/#comments)

ANONYMITY (HTTPS://WWW.SHELLHACKS.COM/TAG/ANONYMITY/)

PROXY (HTTPS://WWW.SHELLHACKS.COM/TAG/PROXY/)

ONE REPLY TO “LINUX PROXY SERVER SETTINGS – SET PROXY FOR COMMAND LINE”



CURTIS REPLY

Thursday November 9th, 2017 at 09:08 PM (https://www.shellhacks.com/linux-proxy-server-settings-set-proxy-command-line/#comment-3006)

You can use no_proxy or NO_PROXY that includes a comma delimited list of domains, subdomains, hostnames, and/or IP addresses that are exempt from the {http{,s},ftp,rsync}_proxy variables.

So something like
export no_proxy='localhost,127.0.0.1,.example.com,.shellhacks.com'
would exempt localhost, 127.0.0.1, *.example.com, and *.shellhacks.com from the other proxy variables.

LEAVE A REPLY

Comment

Name

Email

POST REPLY

‹ INSTALLING THE OCS INVENTORY AGENT 1.X ON CENTOS/RHEL (HTTPS://WWW.SHELLHACKS.COM/INSTALL-OCS-INVENTORY-AGENT-1X-CENTOS-RHEL/)

HOWTO: INSTALL TSM CLIENT ON CENTOS/RHEL › (HTTPS://WWW.SHELLHACKS.COM/INSTALL-TSM-CLIENT-CENTOS-RHEL/)

^

CATEGORIES

Blog (https://www.shellhacks.com/cat/blog/)

Databases (https://www.shellhacks.com/cat/databases/)

Version control (https://www.shellhacks.com/cat/version-control/)

TAGS

ACCESS-CONTROL (HTTPS://WWW.SHELLHACKS.COM/TAG/ACCESS-CONTROL/)

AIRCRACK-NG (HTTPS://WWW.SHELLHACKS.COM/TAG/AIRCRACK-NG/)

ANONYMITY (HTTPS://WWW.SHELLHACKS.COM/TAG/ANONYMITY/)

APACHE (HTTPS://WWW.SHELLHACKS.COM/TAG/APACHE/)

ARCHIVE (HTTPS://WWW.SHELLHACKS.COM/TAG/ARCHIVE/) BASH (HTTPS://WWW.SHELLHACKS.COM/TAG/BASH/)

BOOT (HTTPS://WWW.SHELLHACKS.COM/TAG/BOOT/) CISCO (HTTPS://WWW.SHELLHACKS.COM/TAG/CISCO/)

COMMAND-LINE (HTTPS://WWW.SHELLHACKS.COM/TAG/COMMAND-LINE/)

CURL (HTTPS://WWW.SHELLHACKS.COM/TAG/CURL/) DNS (HTTPS://WWW.SHELLHACKS.COM/TAG/DNS/)

DOCKER (HTTPS://WWW.SHELLHACKS.COM/TAG/DOCKER/)

ENCODING (HTTPS://WWW.SHELLHACKS.COM/TAG/ENCODING/)

ENCRYPTION (HTTPS://WWW.SHELLHACKS.COM/TAG/ENCRYPTION/)

FTP (HTTPS://WWW.SHELLHACKS.COM/TAG/FTP/) GIT (HTTPS://WWW.SHELLHACKS.COM/TAG/GIT/)

HASH (HTTPS://WWW.SHELLHACKS.COM/TAG/HASH/) HISTORY (HTTPS://WWW.SHELLHACKS.COM/TAG/HISTORY/)

ISO (HTTPS://WWW.SHELLHACKS.COM/TAG/ISO/)

JOHN-THE-RIPPER (HTTPS://WWW.SHELLHACKS.COM/TAG/JOHN-THE-RIPPER/)

MAIL (HTTPS://WWW.SHELLHACKS.COM/TAG/MAIL/)

MOD-WSGI (HTTPS://WWW.SHELLHACKS.COM/TAG/MOD-WSGI/)

MONITORING (HTTPS://WWW.SHELLHACKS.COM/TAG/MONITORING/)

MOUNT (HTTPS://WWW.SHELLHACKS.COM/TAG/MOUNT/) MYSQL (HTTPS://WWW.SHELLHACKS.COM/TAG/MYSQL/)

NETWORK (HTTPS://WWW.SHELLHACKS.COM/TAG/NETWORK/)

NMAP (HTTPS://WWW.SHELLHACKS.COM/TAG/NMAP/) OPENSSL (HTTPS://WWW.SHELLHACKS.COM/TAG/OPENSSL/)

PASSWORD (HTTPS://WWW.SHELLHACKS.COM/TAG/PASSWORD/) PDF (HTTPS://WWW.SHELLHACKS.COM/TAG/PDF/)

PERFORMANCE (HTTPS://WWW.SHELLHACKS.COM/TAG/PERFORMANCE/)

PROXY (HTTPS://WWW.SHELLHACKS.COM/TAG/PROXY/) PYTHON (HTTPS://WWW.SHELLHACKS.COM/TAG/PYTHON/)

REGEX (HTTPS://WWW.SHELLHACKS.COM/TAG/REGEX/)

REPOSITORY (HTTPS://WWW.SHELLHACKS.COM/TAG/REPOSITORY/)

SALT-STACK (HTTPS://WWW.SHELLHACKS.COM/TAG/SALT-STACK/) SSH (HTTPS://WWW.SHELLHACKS.COM/TAG/SSH/)

TELNET (HTTPS://WWW.SHELLHACKS.COM/TAG/TELNET/)

TEXT-PROCESSING (HTTPS://WWW.SHELLHACKS.COM/TAG/TEXT-PROCESSING/)

TOR (HTTPS://WWW.SHELLHACKS.COM/TAG/TOR/) TSM (HTTPS://WWW.SHELLHACKS.COM/TAG/TSM/)

VSFTPD (HTTPS://WWW.SHELLHACKS.COM/TAG/VSFTPD/) WGET (HTTPS://WWW.SHELLHACKS.COM/TAG/WGET/)

WINDOWS (HTTPS://WWW.SHELLHACKS.COM/TAG/WINDOWS/) YUM (HTTPS://WWW.SHELLHACKS.COM/TAG/YUM/)