**http://nginx.org/en/linux\_packages.html#mainline**

**nginx: Linux packages**

Currently, nginx packages are available for the following distributions and versions:

RHEL/CentOS:

|  |  |
| --- | --- |
| Version | Supported Platforms |
| 5.x | x86\_64, i386 |
| 6.x | x86\_64, i386 |
| 7.x | x86\_64 |

Debian:

|  |  |  |
| --- | --- | --- |
| Version | Codename | Supported Platforms |
| 7.x | wheezy | x86\_64, i386 |
| 8.x | jessie | x86\_64, i386 |

Ubuntu:

|  |  |  |
| --- | --- | --- |
| Version | Codename | Supported Platforms |
| 12.04 | precise | x86\_64, i386 |
| 14.04 | trusty | x86\_64, i386, aarch64/arm64 |
| 15.04 | vivid | x86\_64, i386 |
| 15.10 | wily | x86\_64, i386 |

SLES:

|  |  |
| --- | --- |
| Version | Supported Platforms |
| 12 | x86\_64 |

To enable automatic updates of Linux packages set up the yum repository for the RHEL/CentOS distributions, the apt repository for the Debian/Ubuntu distributions, or the zypper repository for SLES.

**Pre-Built Packages for Stable version**

To set up the yum repository for RHEL/CentOS, choose the corresponding nginx-release package from the list:

* [RHEL 5](http://nginx.org/packages/rhel/5/noarch/RPMS/nginx-release-rhel-5-0.el5.ngx.noarch.rpm)
* [RHEL 6](http://nginx.org/packages/rhel/6/noarch/RPMS/nginx-release-rhel-6-0.el6.ngx.noarch.rpm)
* [RHEL 7](http://nginx.org/packages/rhel/7/noarch/RPMS/nginx-release-rhel-7-0.el7.ngx.noarch.rpm)
* [CentOS 5](http://nginx.org/packages/centos/5/noarch/RPMS/nginx-release-centos-5-0.el5.ngx.noarch.rpm)
* [CentOS 6](http://nginx.org/packages/centos/6/noarch/RPMS/nginx-release-centos-6-0.el6.ngx.noarch.rpm)
* [CentOS 7](http://nginx.org/packages/centos/7/noarch/RPMS/nginx-release-centos-7-0.el7.ngx.noarch.rpm)

This package contains yum configuration file and a public PGP key necessary to authenticate signed RPMs. Download and install it, then run the following:

yum install nginx

Alternatively, a repository configuration can be added manually without installing the nginx-releasepackage. Create the file named /etc/yum.repos.d/nginx.repo with the following contents:

[nginx]

name=nginx repo

baseurl=http://nginx.org/packages/OS/OSRELEASE/$basearch/

gpgcheck=0

enabled=1

Replace “OS” with “rhel” or “centos”, depending on the distribution used, and “OSRELEASE” with “5”, “6”, or “7”, for 5.x, 6.x, or 7.x versions, respectively.

For Debian/Ubuntu, in order to authenticate the nginx repository signature and to eliminate warnings about missing PGP key during installation of the nginx package, it is necessary to add the key used to sign the nginx packages and repository to the apt program keyring. Please download[this key](http://nginx.org/keys/nginx_signing.key) from our web site, and add it to the apt program keyring with the following command:

sudo apt-key add nginx\_signing.key

For Debian replace *codename* with Debian distribution [codename](http://nginx.org/en/linux_packages.html#distributions), and append the following to the end of the /etc/apt/sources.list file:

deb http://nginx.org/packages/debian/ *codename* nginx

deb-src http://nginx.org/packages/debian/ *codename* nginx

For Ubuntu replace *codename* with Ubuntu distribution [codename](http://nginx.org/en/linux_packages.html#distributions), and append the following to the end of the /etc/apt/sources.list file:

deb http://nginx.org/packages/ubuntu/ *codename* nginx

deb-src http://nginx.org/packages/ubuntu/ *codename* nginx

For Debian/Ubuntu then run the following commands:

apt-get update

apt-get install nginx

For SLES run the following command:

zypper addrepo -G -t yum -c 'http://nginx.org/packages/sles/12' nginx

**Pre-Built Packages for Mainline version**

To set up the yum repository for RHEL/CentOS, create the file named /etc/yum.repos.d/nginx.repo with the following contents:

[nginx]

name=nginx repo

baseurl=http://nginx.org/packages/mainline/OS/OSRELEASE/$basearch/

gpgcheck=0

enabled=1

Replace “OS” with “rhel” or “centos”, depending on the distribution used, and “OSRELEASE” with “5”, “6”, or “7”, for 5.x, 6.x, or 7.x versions, respectively.

For Debian/Ubuntu, in order to authenticate the nginx repository signature and to eliminate warnings about missing PGP key during installation of the nginx package, it is necessary to add the key used to sign the nginx packages and repository to the apt program keyring. Please download[this key](http://nginx.org/keys/nginx_signing.key) from our web site, and add it to the apt program keyring with the following command:

sudo apt-key add nginx\_signing.key

For Debian replace *codename* with Debian distribution [codename](http://nginx.org/en/linux_packages.html#distributions), and append the following to the end of the /etc/apt/sources.list file:

deb http://nginx.org/packages/mainline/debian/ *codename* nginx

deb-src http://nginx.org/packages/mainline/debian/ *codename* nginx

For Ubuntu replace *codename* with Ubuntu distribution [codename](http://nginx.org/en/linux_packages.html#distributions), and append the following to the end of the /etc/apt/sources.list file:

deb http://nginx.org/packages/mainline/ubuntu/ *codename* nginx

deb-src http://nginx.org/packages/mainline/ubuntu/ *codename* nginx

For Debian/Ubuntu then run the following commands:

apt-get update

apt-get install nginx

For SLES run the following command:

zypper addrepo -G -t yum -c 'http://nginx.org/packages/mainline/sles/12' nginx

**Configure Arguments**

Configure arguments common for nginx binaries from pre-built packages for stable version:

--prefix=/etc/nginx

--sbin-path=/usr/sbin/nginx

--conf-path=/etc/nginx/nginx.conf

--error-log-path=/var/log/nginx/error.log

--http-log-path=/var/log/nginx/access.log

--pid-path=/var/run/nginx.pid

--lock-path=/var/run/nginx.lock

--http-client-body-temp-path=/var/cache/nginx/client\_temp

--http-proxy-temp-path=/var/cache/nginx/proxy\_temp

--http-fastcgi-temp-path=/var/cache/nginx/fastcgi\_temp

--http-uwsgi-temp-path=/var/cache/nginx/uwsgi\_temp

--http-scgi-temp-path=/var/cache/nginx/scgi\_temp

--user=nginx

--group=nginx

--with-http\_ssl\_module

--with-http\_realip\_module

--with-http\_addition\_module

--with-http\_sub\_module

--with-http\_dav\_module

--with-http\_flv\_module

--with-http\_mp4\_module

--with-http\_gunzip\_module

--with-http\_gzip\_static\_module

--with-http\_random\_index\_module

--with-http\_secure\_link\_module

--with-http\_stub\_status\_module

--with-http\_auth\_request\_module

--with-mail

--with-mail\_ssl\_module

--with-file-aio

--with-http\_spdy\_module

--with-ipv6

Packages for mainline version also have the following arguments:

--with-threads

--with-stream

--with-stream\_ssl\_module

and

--with-http\_spdy\_module

replaced with

--with-http\_v2\_module

Package are built with all modules that do not require additional libraries to avoid extra dependencies.

**Signatures**

Both RPM packages and Debian/Ubuntu repositories use digital signatures to verify the integrity and origin of the downloaded package. In order to check a signature it is necessary to download[nginx signing key](http://nginx.org/keys/nginx_signing.key) and import it to the rpm or apt program’s keyring:

* On Debian/Ubuntu:

sudo apt-key add nginx\_signing.key

* On RHEL/CentOS:

sudo rpm --import nginx\_signing.key

* On SLES:

sudo rpm --import nginx\_signing.key

On Debian/Ubuntu/SLES signatures are checked by default, but on RHEL/CentOS it is necessary to set

gpgcheck=1

in the /etc/yum.repos.d/nginx.repo file.

Since our [PGP keys](http://nginx.org/en/pgp_keys.html) and packages are located on the same server, they are equally trusted. It is highly advised to additionally verify the authenticity of the downloaded PGP key. PGP has the “Web of Trust” concept, when a key is signed by someone else’s key, that in turn is signed by another key and so on. It often makes possible to build a chain from an arbitrary key to someone’s key who you know and trust personally, thus verify the authenticity of the first key in a chain. This concept is described in details in [GPG Mini Howto](http://www.dewinter.com/gnupg_howto/english/GPGMiniHowto-1.html). Our keys have enough signatures, and their authenticity is relatively easy to check.

原文  [http://www.phodal.com/blog/nginx-194-with-http2-install/](http://www.phodal.com/blog/nginx-194-with-http2-install/?utm_source=tuicool&utm_medium=referral)

主题 [Nginx](http://www.tuicool.com/topics/11090014)[HTTP2](http://www.tuicool.com/topics/11090148)

看到了一些关于HTTP2的传闻，于是就想着升级网站的Nginx，让他支持HTTP2.0，顺便也编译一下新的ngx\_pagespeed，也是有近一年没有更新nginx了。

**前提:**

1. 需要https证书
2. 需要有 OpenSSL 1.0.2+

**安装**

以下步骤适合于LNMP安装。

1.下载Nginx

wget http://nginx.org/down**load**/nginx-1.9.4.tar.gz

2.下载和编译

tar xvfz nginx-1.9.4.tar.gz

cd nginx-1.9.4

3.打patch

wget http://nginx.org/patches/http2/patch.http2.txt

patch -p1 < patch.http2.txt

4.配置

./configure --**with**-http\_ssl\_module \

--**with**-http\_v2\_module \

--**with**-debug \

--**with**-openssl=/path/to/openssl-1.0.2

如果你和我一样有各种模块，那么配置可能是下面这样子的

./configure --user=www --group=www --add-module=../ngx\_pagespeed-release-1.9.32.6-beta --prefix=/usr/local/nginx --**with**-pcre --**with**-http\_ssl\_module --**with**-http\_realip\_module --**with**-http\_addition\_module --**with**-http\_sub\_module --**with**-http\_dav\_module --**with**-http\_flv\_module --**with**-http\_mp4\_module --**with**-http\_gunzip\_module --**with**-http\_gzip\_static\_module --**with**-http\_random\_index\_module --**with**-http\_secure\_link\_module --**with**-http\_stub\_status\_module --**with**-mail --**with**-mail\_ssl\_module --**with**-ipv6

5.编译

make

6.修改配置如下

server {

**listen** 443 default\_server ssl http2;

ssl\_certificate server.crt;

ssl\_certificate\_key server.key;

...

}

7.更新

mv /usr/**local**/nginx/sbin/nginx /usr/**local**/nginx/sbin/nginx.old

cp objs/nginx /usr/**local**/nginx/sbin/nginx

/usr/**local**/nginx/sbin/nginx -t

make upgrade

8.查看

chrome://net-internals