**To backup an old version of nginx before installing a new one:**

mkdir /etc/nginx-backup/

cp -r /etc/nginx/\* /etc/nginx-backup/

**Install the prerequisites:**

sudo yum install yum-utils

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

[nginx-stable]

name=nginx stable repo

baseurl=http://nginx.org/packages/centos/$releasever/$basearch/

gpgcheck=1

enabled=1

gpgkey=https://nginx.org/keys/nginx\_signing.key

module\_hotfixes=true

[nginx-mainline]

name=nginx mainline repo

baseurl=http://nginx.org/packages/mainline/centos/$releasever/$basearch/

gpgcheck=1

enabled=0

gpgkey=https://nginx.org/keys/nginx\_signing.key

module\_hotfixes=true

By default, the repository for stable nginx packages is used. If you would like to use mainline nginx packages, run the following command:

sudo yum-config-manager --enable nginx-mainline

**To install nginx**, run the following command:

sudo yum install nginx

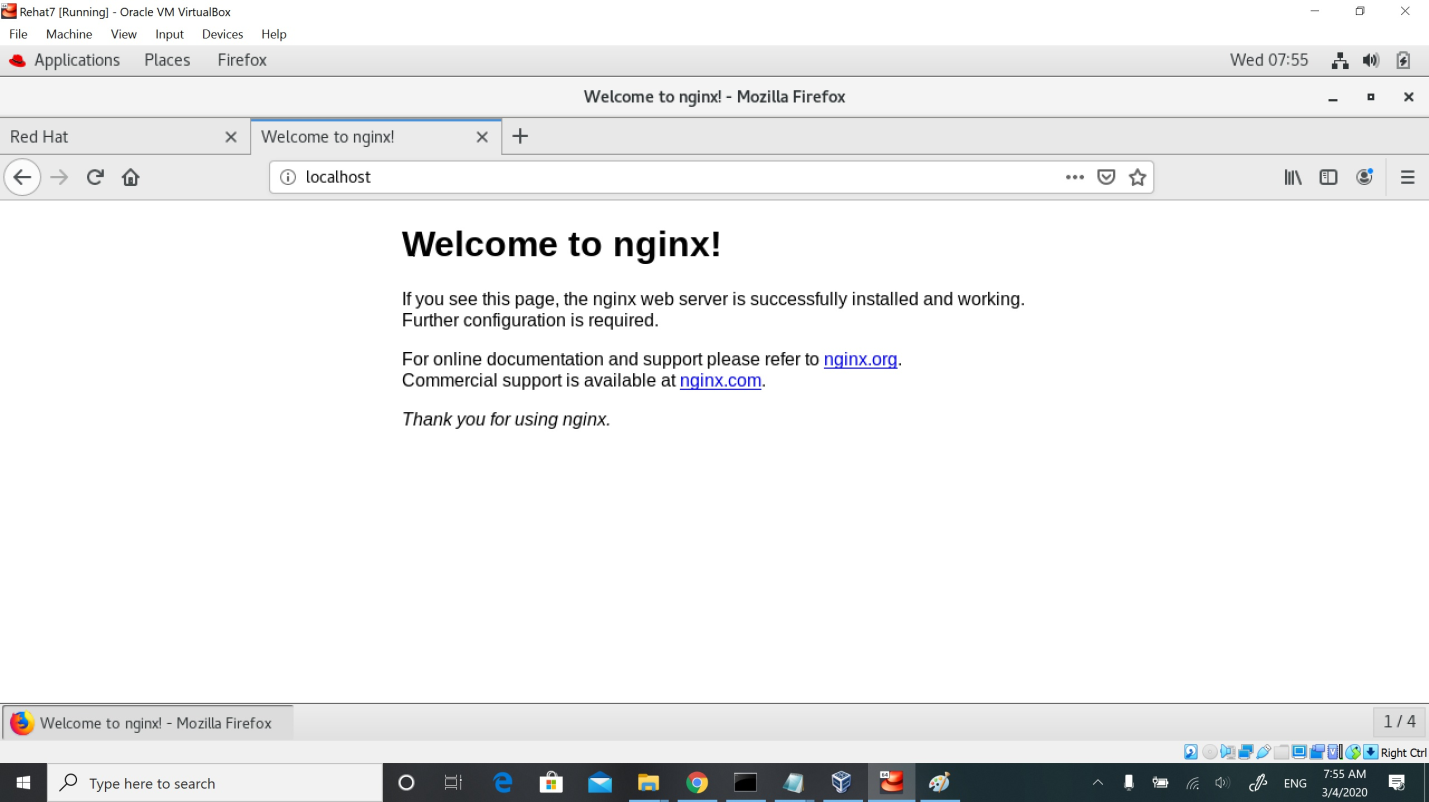
When prompted to accept the GPG key, **verify that the fingerprint matches** 573B FD6B 3D8F BC64 1079 A6AB ABF5 BD82 7BD9 BF62, and if so, accept it.

**Check the version of nginx** installed:

sudo nginx -v

**Verify, nginx is up and running** by opening the welcome page at this url:

http://127.0.0.1



**Verify that NGINX Open Source is up and running**:

$ curl -I 127.0.0.1

HTTP/1.1 200 OK

Server: nginx/1.13.8

Step 3 – **Start/stop/restart nginx server**

**First enable nginx service** by running systemctl command so that it start at server boot time:

$ sudo systemctl enable nginx

Sample outputs:

Created symlink from /etc/systemd/system/multi-user.target.wants/nginx.service to /usr/lib/systemd/system/nginx.service.

**Start Nginx** command

$ sudo systemctl start nginx

**Stop Nginx** command

$ sudo systemctl stop nginx

**Restart Nginx** command

$ sudo systemctl restart nginx

**Find status of Nginx server** command

$ sudo systemctl status nginx

Sample outputs:

\* nginx.service - nginx - high performance web server

Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; vendor preset: disabled)

Active: active (running) since Thu 2018-01-18 21:45:54 UTC; 8s ago

Docs: http://nginx.org/en/docs/

Process: 656 ExecStart=/usr/sbin/nginx -c /etc/nginx/nginx.conf (code=exited, status=0/SUCCESS)

Main PID: 657 (nginx)

CGroup: /system.slice/nginx.service

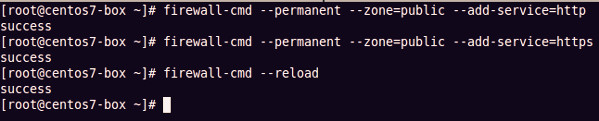
??657 nginx: master process /usr/sbin/nginx -c /etc/nginx/nginx.conf

??658 nginx: worker process

Jan 18 21:45:54 cenots7-theosin systemd[1]: Starting nginx - high performance web server...

Jan 18 21:45:54 cenots7-theosin systemd[1]: Started nginx - high performance web server.

**Step 4 – Open port 80 and 443 using firewall-cmd**

You must open and enable port 80 and 443 using the firewall-cmd command:  
$ sudo firewall-cmd --permanent --zone=public --add-service=http  
$ sudo firewall-cmd --permanent --zone=public --add-service=https  
$ sudo firewall-cmd --reload  
[](https://www.cyberciti.biz/media/new/faq/2018/01/RHEL7-CentOS7-allow-HTTP-and-HTTPS-traffic-with-firewall-cmd.jpg)

**Step 5 – Test it**

Verify that port 80 or 443 opened using ss command:  
$ sudo ss -tulpn  
Sample outputs:

|  |
| --- |
| Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port  udp UNCONN 0 0 \*:60139 \*:\* users:(("dhclient",pid**=**242,fd=20))  udp UNCONN 0 0 \*:68 \*:\* users:(("dhclient",pid**=**242,fd=6))  udp UNCONN 0 0 :::34050 :::\* users:(("dhclient",pid**=**242,fd=21))  tcp LISTEN 0 128 \*:80 \*:\* users:(("nginx",pid**=**696,fd=6),("nginx",pid**=**695,fd=6)) |

If you do not know your server IP address run the following [ip command](https://www.cyberciti.biz/faq/linux-ip-command-examples-usage-syntax/" \o "See Linux/Unix ip command examples for more info):  
$ ip a  
Sample outputs:

|  |
| --- |
| 1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN qlen 1000  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  inet 127.0.0.1/8 scope host lo  valid\_lft forever preferred\_lft forever  inet6 ::1/128 scope host  valid\_lft forever preferred\_lft forever  4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc noqueue state UP qlen 1000  link/ether 00:16:3e:ac:ba:1e brd ff:ff:ff:ff:ff:ff link-netnsid 0  inet 10.21.136.134/24 brd 10.21.136.255 scope global dynamic eth0  valid\_lft 3348sec preferred\_lft 3348sec  inet6 fe80::216:3eff:feac:ba1e/64 scope link  valid\_lft forever preferred\_lft forever |

So my IP address is 10.21.136.134. Fire a web browser and type the ip address:  
http://10.21.136.134  
[](https://www.cyberciti.biz/media/new/faq/2018/01/Welcome-to-Nginx.jpg)

In case you need **to close the previously open HTTP port 80 and HTTPS port 443** execute:

# firewall-cmd --zone=public --permanent --**remove**-service=http

# firewall-cmd --zone=public --permanent --**remove**-service=https

# firewall-cmd --reload