

Infrastructure et réseau

# Server Linux



Uka Zotrim  
18/12/2022

## 1.0 Linux Web Server

« They are more choices on Linux than on Windows to serve Web pages. • The Apache HTTP Server (apache) is a free and open-source crossplatform web server software, released under the terms of Apache License 2.0. Apache is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation. • Nginx is a web server that can also be used as a reverse proxy, load balancer, mail proxy and HTTP cache. The software was created by Igor Sysoev and publicly released in 2004. Nginx is free and open-source software, released under the terms of the 2-clause BSD license. A large fraction of web servers use NGINX, often as a load balancer. As of January 2021, Netcraft estimated that Apache served 24.63% of the million busiest websites, while Nginx served 23.21% and Microsoft is in third place at 6.85%. »

### 1.1 Install

We will install nginx. For this we will use the command: `sudo dnf install nginx`

```
[root@localhost html]# dnf install nginx
Dernière vérification de l'expiration des métadonnées effectuée il y a 1:02:50 le mer 14 déc 2022 14:08:19.
Aucune correspondance pour le paramètre: nginx
Erreur : Impossible de trouver une correspondance: nginx
[root@localhost html]# systemctl start nginx
[root@localhost html]# _
```

we will start nginx with the command: `sudo systemctl start nginx`

To check if we have activated it, we use the command: `sudo systemctl status nginx`

```
[root@localhost html]# dnf install nginx
Dernière vérification de l'expiration des métadonnées effectuée il y a 1:02:50 le mer 14 déc 2022 14:08:19.
Aucune correspondance pour le paramètre: nginx
Erreur : Impossible de trouver une correspondance: nginx
[root@localhost html]# systemctl start nginx
[root@localhost html]# systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: disabled)
   Active: active (running) since Wed 2022-12-14 14:02:16 CET; 1h 10min ago
     Main PID: 1167 (nginx)
        Tasks: 5 (limit: 2310)
       Memory: 4.7M
          CPU: 57ms
      CGroup: /system.slice/nginx.service
              └─1167 "nginx: master process /usr/sbin/nginx"
                  └─1168 "nginx: worker process"
                      └─1169 "nginx: worker process"
                          └─1170 "nginx: worker process"
                              └─1171 "nginx: worker process"

déc 14 14:02:16 localhost.localdomain systemd[1]: Starting nginx.service - The nginx HTTP and reverse proxy server: [main]
déc 14 14:02:16 localhost.localdomain nginx[1164]: nginx: the configuration file /etc/nginx/nginx.conf is not open (yet)
déc 14 14:02:16 localhost.localdomain nginx[1164]: nginx: configuration file /etc/nginx/nginx.conf test is successful
déc 14 14:02:16 localhost.localdomain systemd[1]: Started nginx.service - The nginx HTTP and reverse proxy server: [main]
lines 1-18/18 (END)
```

The `firewall-cmd --add-service=http` command adds the HTTP service to the list of services allowed by the system firewall. This means that the firewall will allow incoming connections to the HTTP service on the server.

```
[root@localhost html]# firewall-cmd --add-service=http
Warning: ALREADY_ENABLED: 'http' already in 'FedoraServer'
success
[root@localhost html]# firewall-cmd --add-service=https
Warning: ALREADY_ENABLED: 'https' already in 'FedoraServer'
success
[root@localhost html]# _
```

## 1.2 Create site on :80

To modify my index.html file, we enter the following command:  
nano/usr/share/nginx/html/index.html

```
[root@pc-315 html]# nano /usr/share/nginx/html/index.html_
```

We modify the file including the text.

```
GNU nano 6.4 index.html
.col-sm-12 {
  width: 100%;
}
h1 {
  padding: 0 !important;
}
}

</style>
</head>
<body>
  <h1>Bienvenue Zotrim Uka</h1>

  <div class='row'>

    <div class='col-sm-12 col-md-6 col-md-6 '></div>
      <p class="summary">Nous changeons le contenu de la page internet.</p>
    </div>

    <div class='col-sm-12 col-md-6 col-md-6 col-md-offset-12'>

      <div class='section'>
        <h2>If you are a member of the general public:</h2>

        <p>The website you just visited is either <strong>experiencing
        problems</strong> or <strong>undergoing routine maintenance</strong>.</p>

        <p>To let the administrators of this website know that you are
        seeing this page and not what you were expecting, an e-mail
        addressed to "webmaster" at the website's domain should reach
        an appropriate person. For example, if you saw this page while visiting
```

```
[root@localhost html]# nano index.html
```

To be able to access our site through our IP address, we must enter the following command: ifconfig

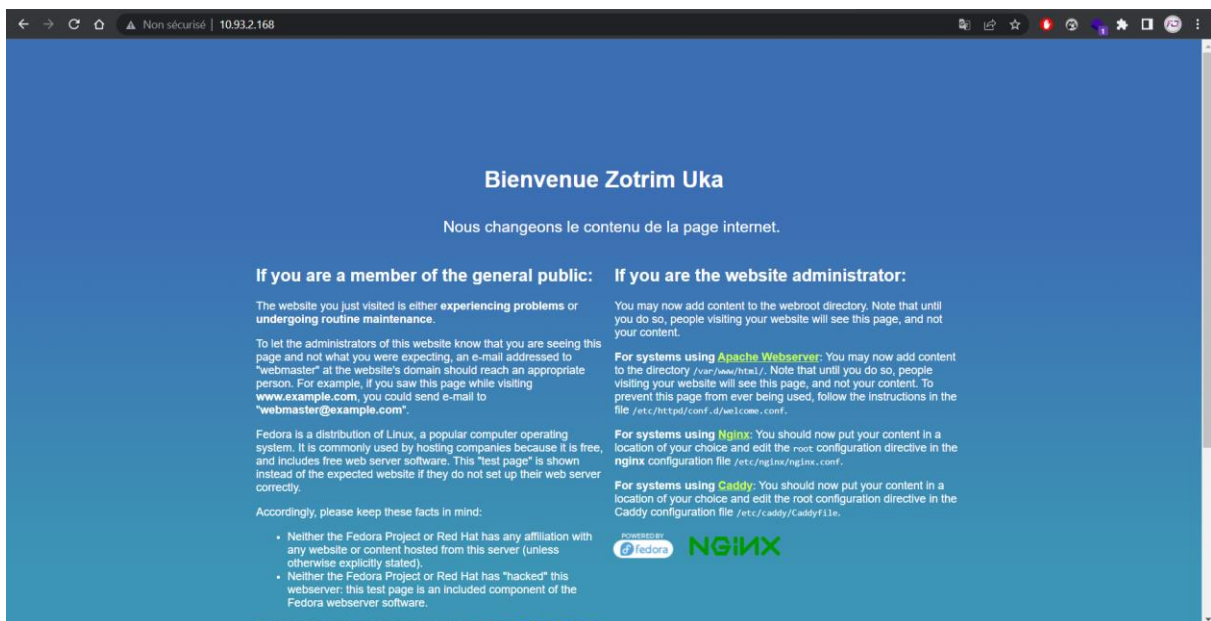
```
Main PID: 1167 (nginx)
Tasks: 5 (limit: 2310)
Memory: 4.7M
CPU: 57ms
CGroup: /system.slice/nginx.service
├─1167 "nginx: master process /usr/sbin/nginx"
├─1168 "nginx: worker process"
├─1169 "nginx: worker process"
├─1170 "nginx: worker process"
└─1171 "nginx: worker process"

déc 14 14:02:16 localhost.localdomain systemd[1]: Starting nginx.service - The nginx HTTP and reverse proxy
déc 14 14:02:16 localhost.localdomain nginx[11641]: nginx: the configuration file /etc/nginx/nginx.conf
déc 14 14:02:16 localhost.localdomain nginx[11641]: nginx: configuration file /etc/nginx/nginx.conf
déc 14 14:02:16 localhost.localdomain systemd[1]: Started nginx.service - The nginx HTTP and reverse proxy

[root@localhost html]# systemctl enable nginx.service
[root@localhost html]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.93.2.168 netmask 255.255.0.0 broadcast 10.93.255.255
    inet6 fe80::a00:27ff:fe1f:5b02 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:1f:5b:02 txqueuelen 1000 (Ethernet)
    RX packets 6632 bytes 7866585 (7.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2318 bytes 689654 (673.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Boucle locale)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@localhost html]# _
```



## 1.3 Create a site on :8080

To start, I duplicated the HTML file with the command: `cp -r file copyNameFile`

```
[root@pc-315 nginx]# cp -r html htmlPort8080_
```

Then I went to the nginx server configuration file and changed the port 80 to port 8080. I also changed the name of the folder in the root.

```
GNU nano 6.4 /etc/nginx/nginx.conf
default_type application/octet-stream;

# Load modular configuration files from the /etc/nginx/conf.d directory.
# See http://nginx.org/en/docs/nginx_core_module.html#include
# for more information.
include /etc/nginx/conf.d/*.conf;

server {
    listen 8080;
    listen [::]:8080;
    server_name _;
    root /usr/share/nginx/html8080;

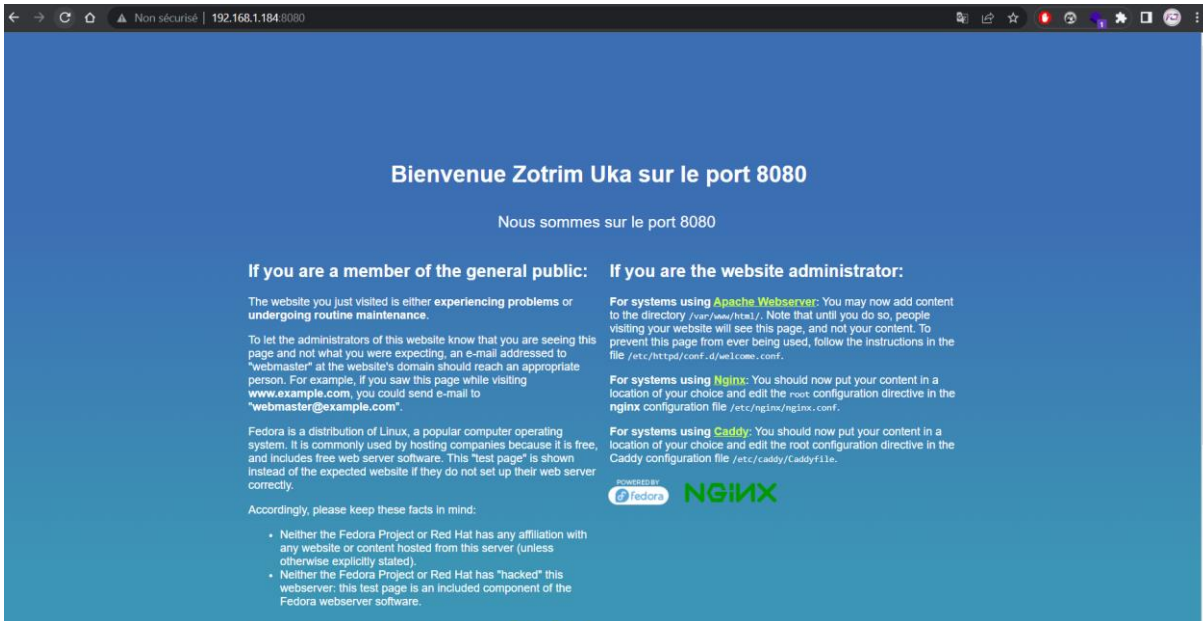
    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    error_page 404 /404.html;
    location = /404.html {
    }

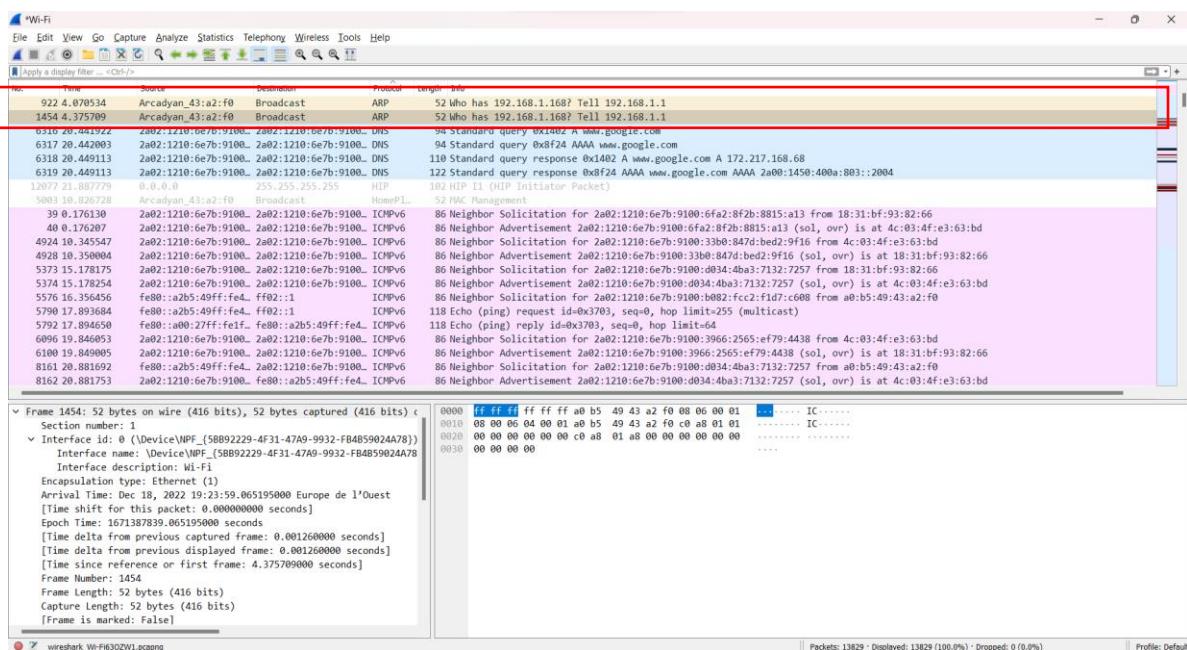
    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
    }
}

# Settings for a TLS enabled server.
#
# server {
#     listen 443 ssl http2;
#     listen [::]:443 ssl http2;
#     server_name _;
#     root /usr/share/nginx/html;
# }

[root@pc-315 etc]# nano /etc/nginx/nginx.conf_
```



2. From your workstation, test the availability of your site with putty and/or a browser, capturing or not with Wireshark.



## 2.0 Authenticated access (optional)

To protect a folder from its contents. You must perform the following steps. First, create a configuration file in the "nginx" configuration directory:

```
[root@localhost ~]# nano /etc/nginx/auth.conf_
```

Then we will enter the data and the path to the hidden file ".htpasswd" which will contain sensitive data:

```
GNU nano 6.4 /etc/nginx/auth.conf Modifié
auth_basic "Restricted Content";
auth_basic_user_file /etc/nginx/.htpasswd;_
```

Using online tools, we can encrypt the password by adding these lines of code. I chose to use the SHA-1 hash function for this

```
GNU nano 6.4 /etc/nginx/.htpasswd Modifié
root:{SHA}+GWNi00xIf007LQQmx5Llwzr4wic=
```

Pour terminer, nous devons apporter une modification à la configuration du serveur nginx afin de créer une route qui mène à un dossier protégé.

```
[root@localhost ~]# nano /etc/nginx/nginx.conf_
```



And add these lines for the 'secure' route

```
GNU nano 6.4 /etc/nginx/nginx.conf Modifié
# See http://nginx.org/en/docs/nginx_core_module.html#include
# for more information.
include /etc/nginx/conf.d/*.conf;

server {
    listen      8080;
    listen     [::]:8080;
    server_name _;
    root       /usr/share/nginx/html8080;

    # Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;

    error_page 404 /404.html;
    location = /404.html {
    }

    error_page 500 502 503 504 /50x.html;
    location = /50x.html {
    }
    location /secure{
    include /etc/nginx/auth.conf;_
    }
}

# Settings for a TLS enabled server.
#
# server {
#     listen      443 ssl http2;
#     listen     [::]:443 ssl http2;
#     server_name _;
#     root       /usr/share/nginx/html;
#
#     ssl_certificate "/etc/pki/nginx/server.crt";
#
^G Aide      ^O Écrire   ^W Chercher ^K Couper   ^T Exécuter ^C Emplacement ^U Annuler
^X Quitter  ^R Lire fich. ^_ Remplacer ^U Coller   ^J Justifier ^_ Aller ligne ^E Refaire
```

Then we need to restart the nginx service to consider the changes

```
[root@localhost ~]# systemctl restart nginx.service_
```

To make these changes, we will have to navigate to the root of the web application and add a new folder named "secure". Then we will copy the file "index.html" into this folder and change the title tag to HTML.

```
root@localhost ~]# cd /usr/share/nginx/html/_
```

```
root@localhost html]# mkdir secure
```

```
root@localhost html]# cp index.html secure/index.html
```

I changed the title of the page, so you can see the change

```
GNU nano 6.4 index.html Modifié
}
.col-sm-12 {
  width: 100%;
}
h1 {
  padding: 0 !important;
}
}

</style>
</head>
<body>
  <h1>Bienvenue Zotrim Uka site sécurisé - Secure directory </h1>

  <div class='row'>

    <div class='col-sm-12 col-md-6 col-md-6 '></div>
      <p class="summary">Nous sommes sur le port 80</p>
    </div>

    <div class='col-sm-12 col-md-6 col-md-6 col-md-offset-12'>

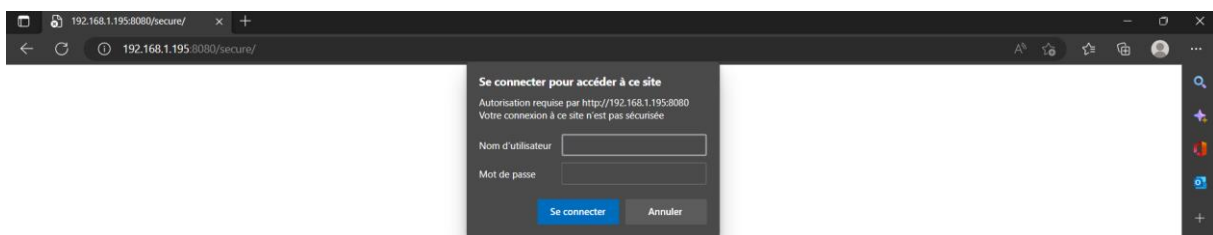
      <div class='section'>
        <h2>If you are a member of the general public:</h2>

        <ul>
          <li>Neither the Fedora Project or Red Hat has any
            affiliation with any website or content hosted from this
            server (unless otherwise explicitly stated).</li>

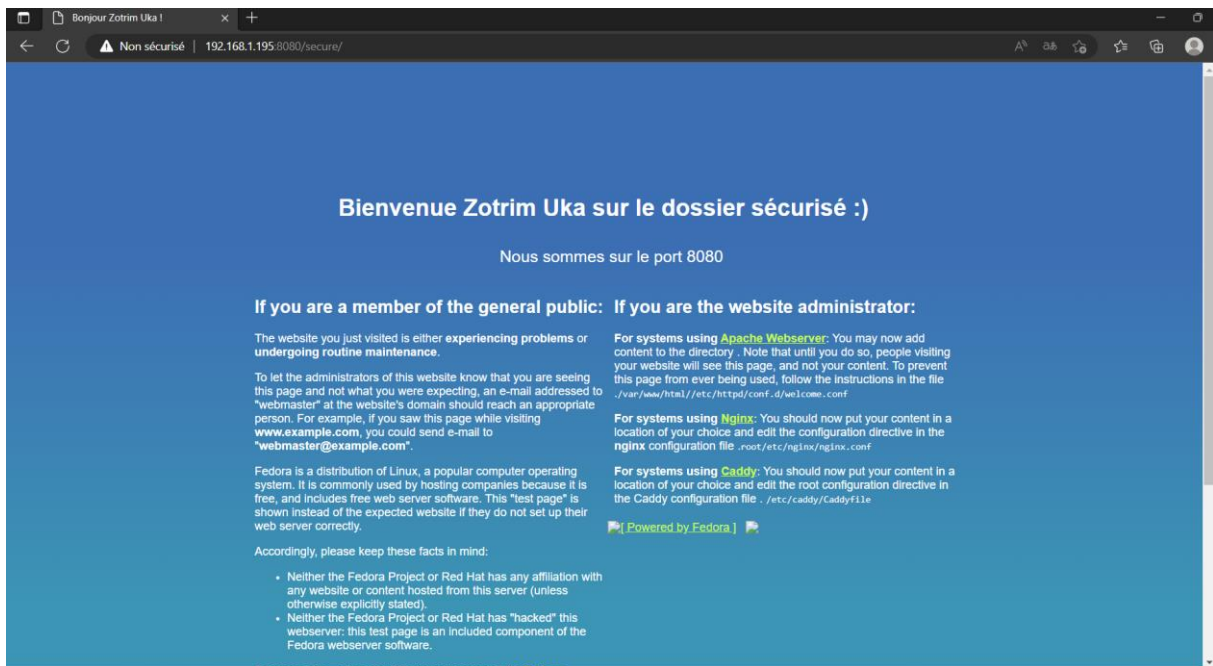
          <li>Neither the Fedora Project or Red Hat has "hacked"

Aide      Écrire  Chercher  Couper   Exécuter  Emplacement  Annuler
Quitter   Lire fich. Remplacer Coller   Justifier  Aller ligne  Refaire
```

We can use this step to check if the route is protected.



## We have secured a file



Bonjour Zotrim Uka !

Non sécurisé | 192.168.1.195:8080/secure/

### Bienvenue Zotrim Uka sur le dossier sécurisé :)

Nous sommes sur le port 8080

**If you are a member of the general public:** The website you just visited is either experiencing problems or undergoing routine maintenance.

To let the administrators of this website know that you are seeing this page and not what you were expecting, an e-mail addressed to "webmaster" at the website's domain should reach an appropriate person. For example, if you saw this page while visiting [www.example.com](http://www.example.com), you could send e-mail to "webmaster@example.com".

Fedora is a distribution of Linux, a popular computer operating system. It is commonly used by hosting companies because it is free, and includes free web server software. This "test page" is shown instead of the expected website if they do not set up their web server correctly.

Accordingly, please keep these facts in mind:

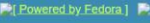
- Neither the Fedora Project or Red Hat has any affiliation with any website or content hosted from this server (unless otherwise explicitly stated).
- Neither the Fedora Project or Red Hat has "hacked" this webserver; this test page is an included component of the Fedora webserver software.

**If you are the website administrator:**

**For systems using Apache Webserver:** You may now add content to the directory. Note that until you do so, people visiting your website will see this page, and not your content. To prevent this page from ever being used, follow the instructions in the file `./var/www/html/.etc/httpd/conf.d/welcome.conf`

**For systems using Nginx:** You should now put your content in a location of your choice and edit the configuration directive in the nginx configuration file `./root/etc/nginx/nginx.conf`

**For systems using Caddy:** You should now put your content in a location of your choice and edit the root configuration directive in the Caddy configuration file `./etc/caddy/Caddyfile`

 [Powered by Fedora]

For more information about Fedora, please visit the [Fedora Project](#)