HES-SO Valais Wallis

Linux WEB Server

Digital Team Academy

Dasek Joiakim

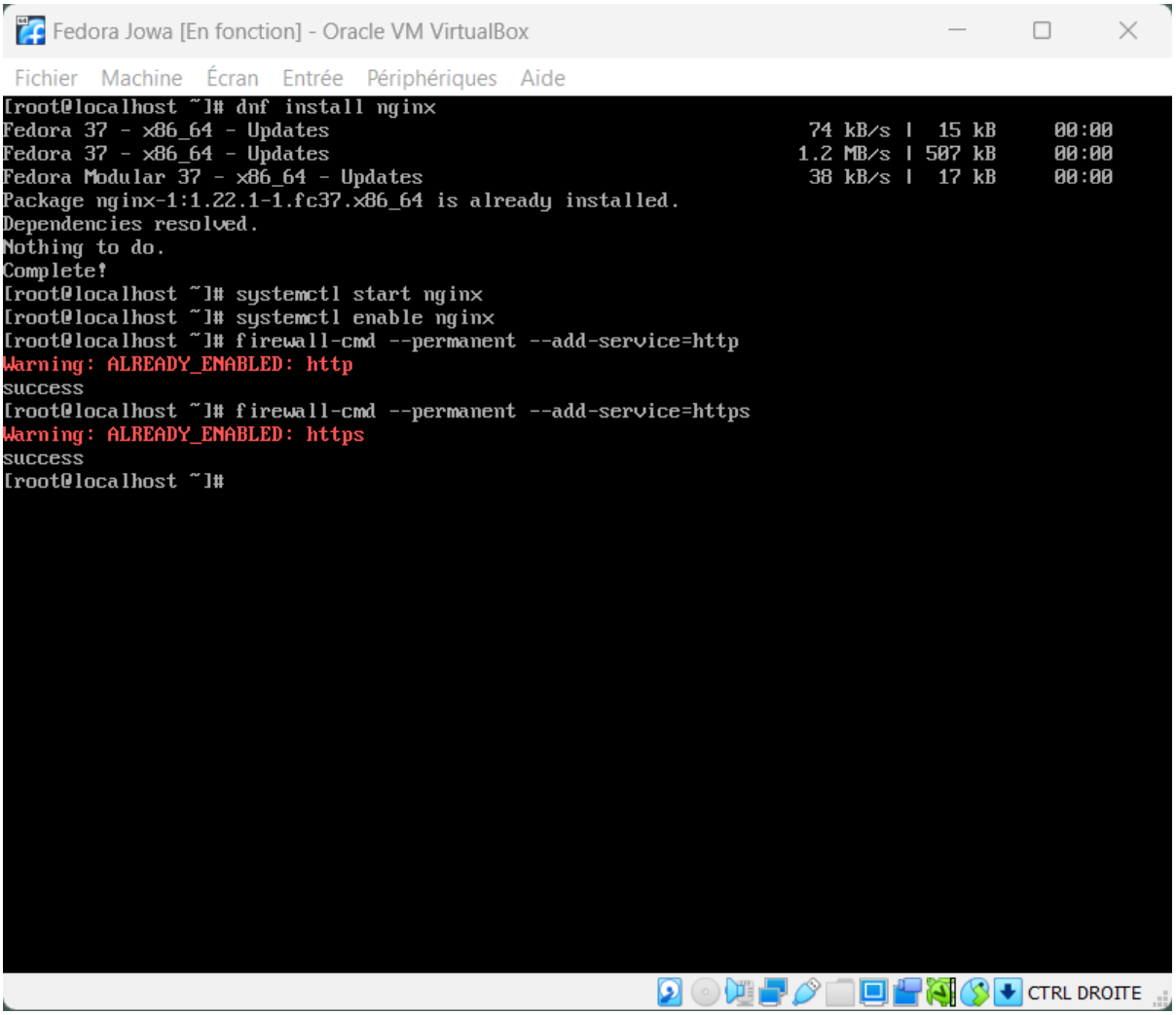
15/12/2022

Table of contents

Install

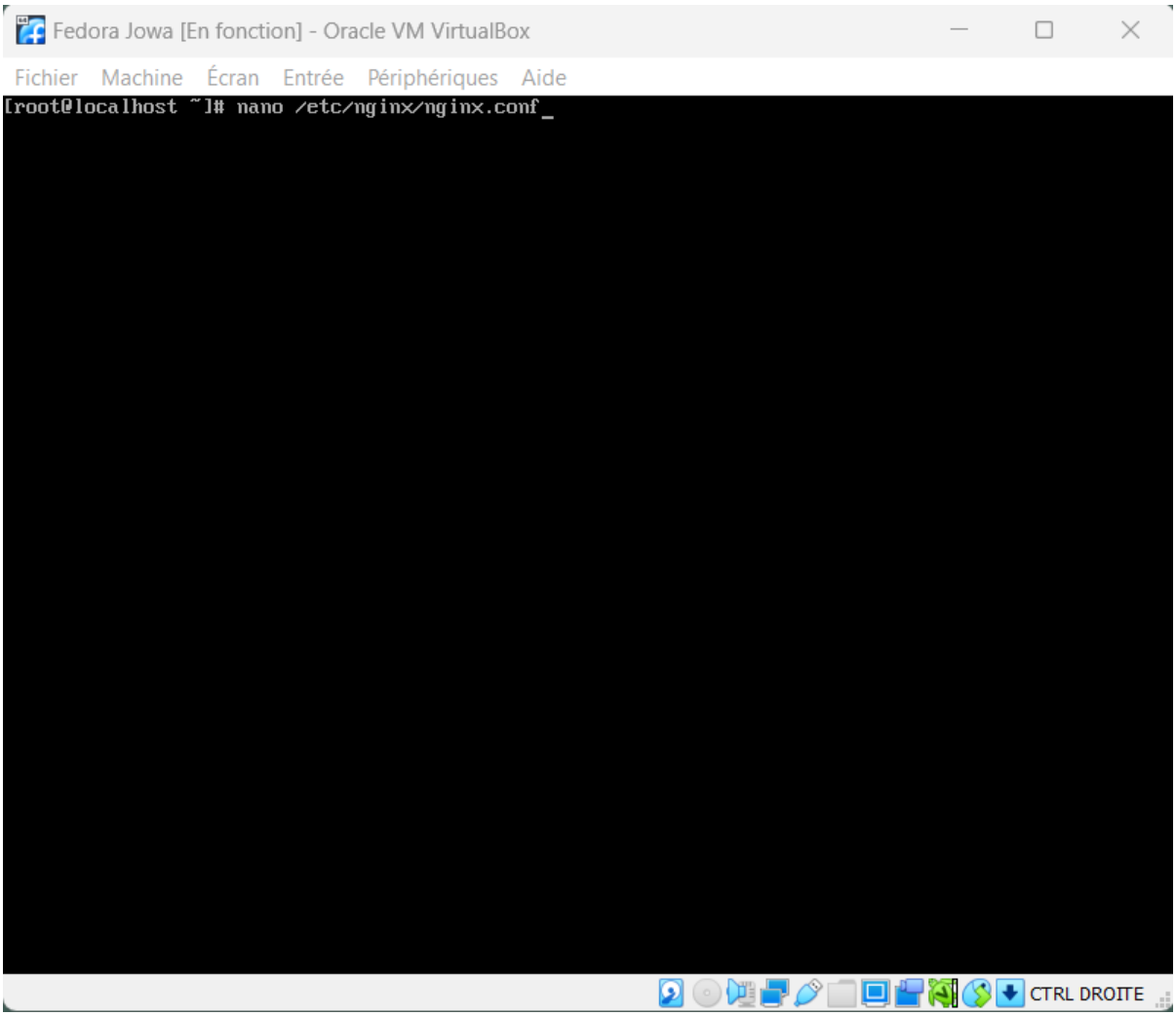
First of all we will install the "nginx" server on Fedora via the "DNF" package manager. Then we will use the "systemctl" command which is a daemon manager also called
"services. Daemons" are programmes launched as fundraising tasks for the good of the
operation of other services or programs. We will therefore launch "nginx" with the option
Click on "start" then "enable" to activate it at start-up.

Then we need to allow "http" and "https" protocol in the firewall exceptions like
in the following image:



Create site on :80

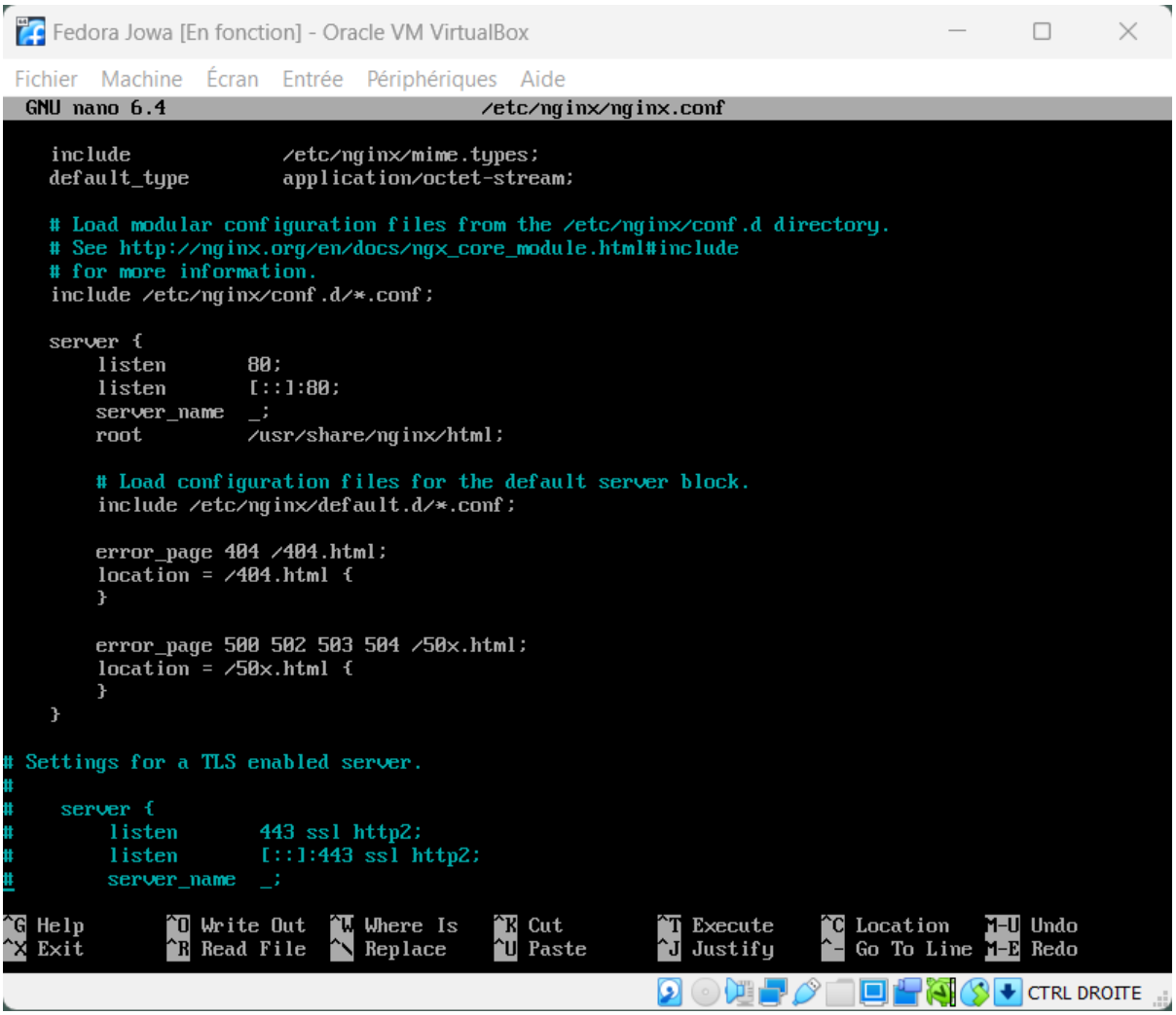
By default the server already has a configuration on port 80, this configuration can be accessed via this path:



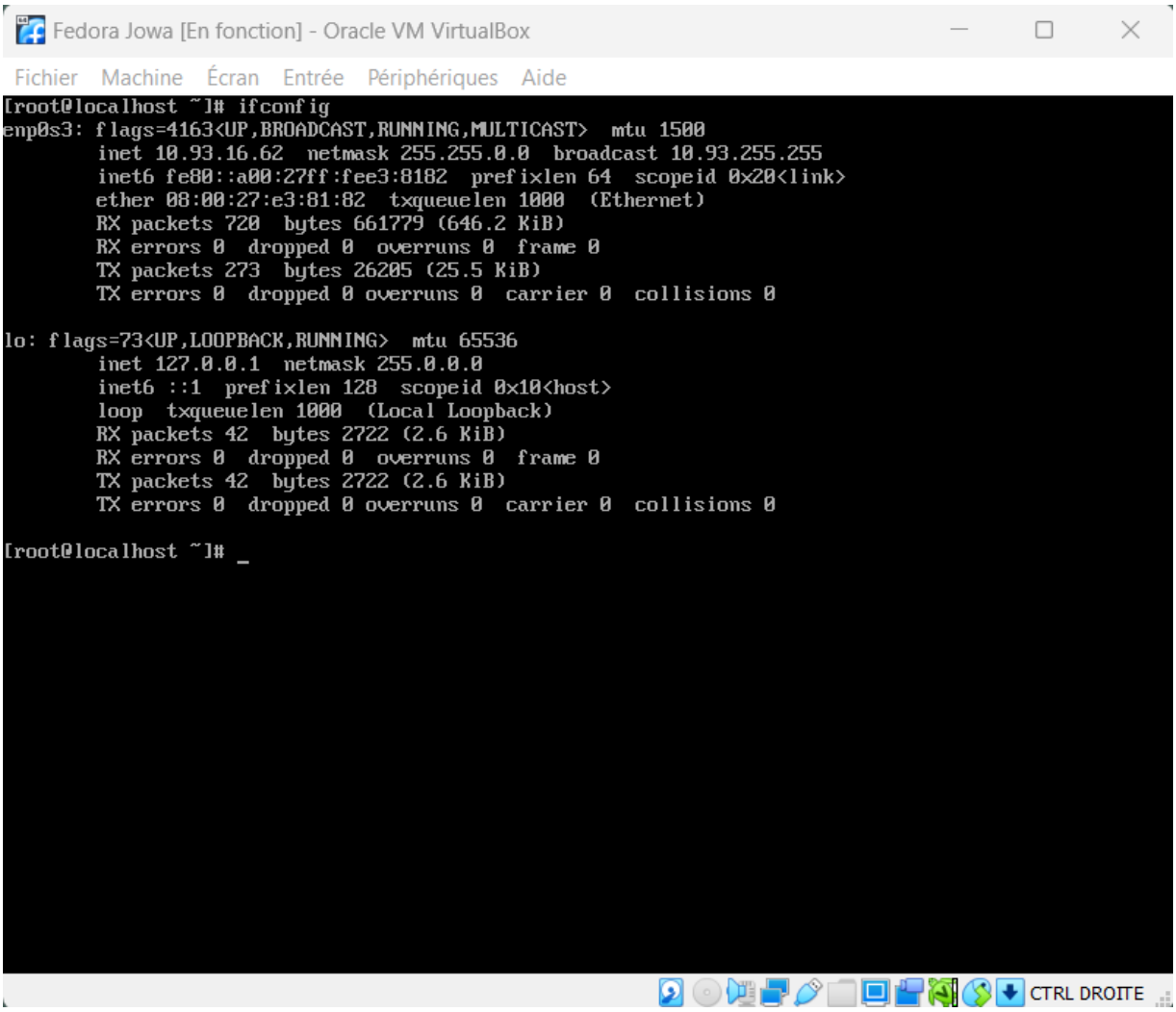
We see a block called "server" with several directives and values. The most important elements are :

- The listening port "listen 80;"
- The name of the server, in this case the ip address only: "server_name: _;".
- The root folder containing the files and dependencies of the WEB application. "root /sur/share/nginx/html "
- And some redirection routes in case of "http" error code...

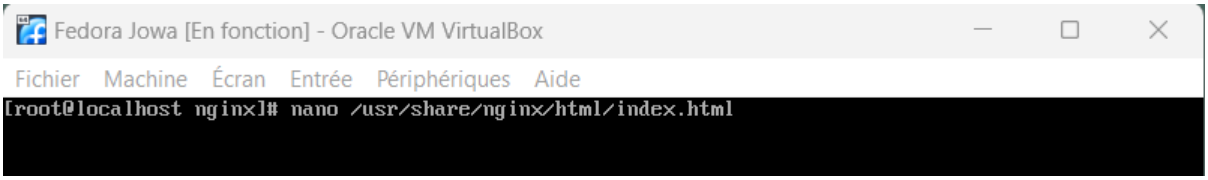
To save, press the "ctrl + x" keys, then press the "y" key and finally
"If you have not changed anything, simply press "ctrl + x":



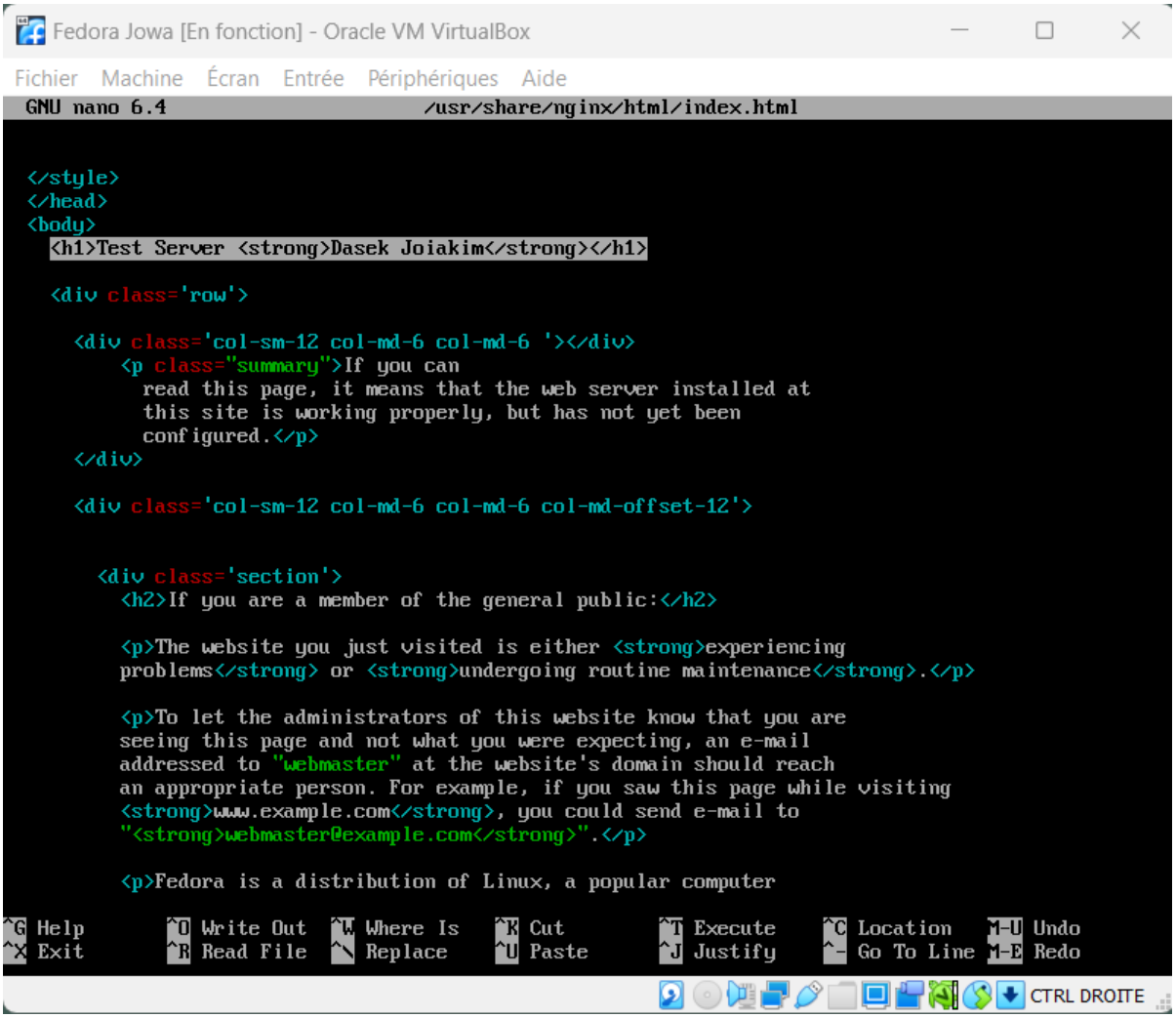
Then we want to know our IP address to access the WEB application:



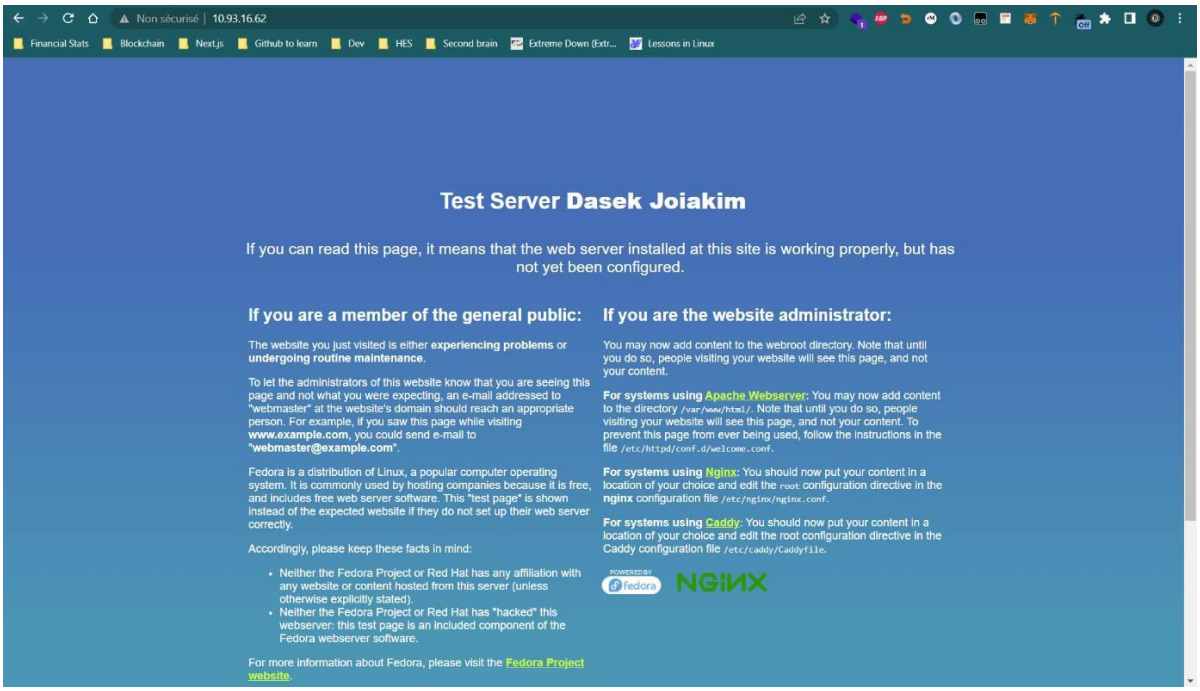
And finally we can edit the pre-existing "HTML" file via this path and the "nano" tool which allows edit files :



We will edit the HTML H1 tag, for "heading level 1" and customize the content as follows:

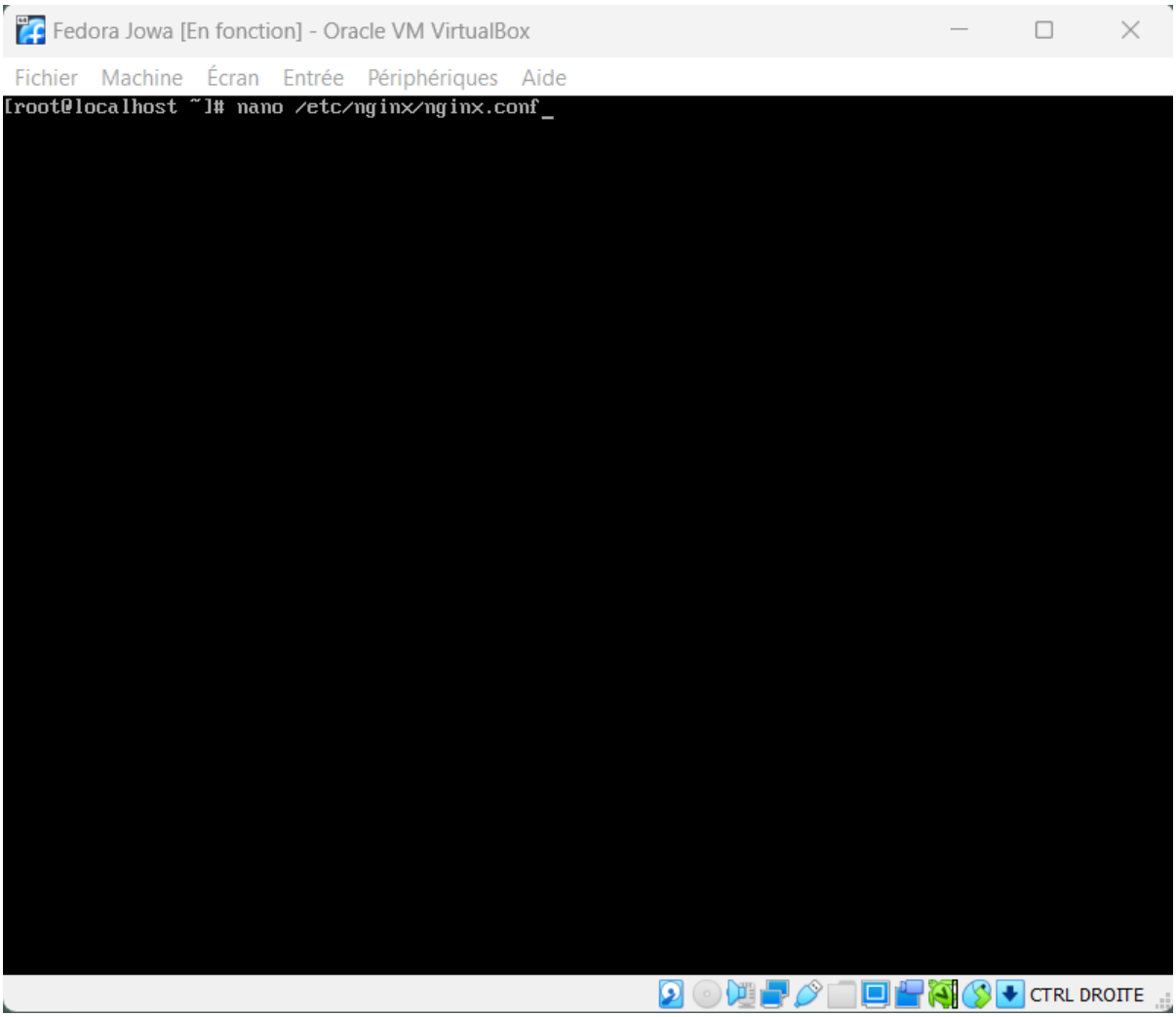


We visit the site and here we are on the index page:

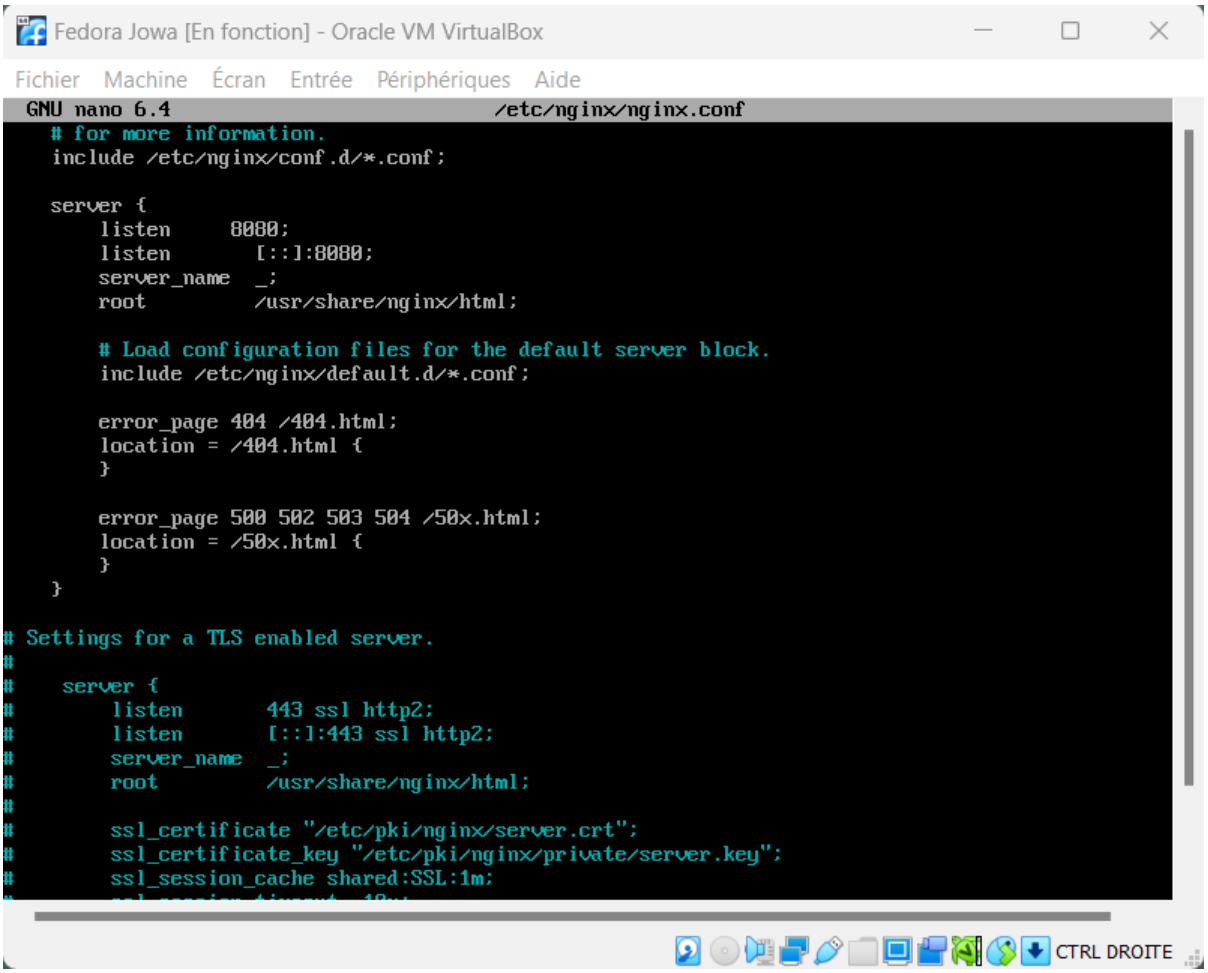


Create site on :8080

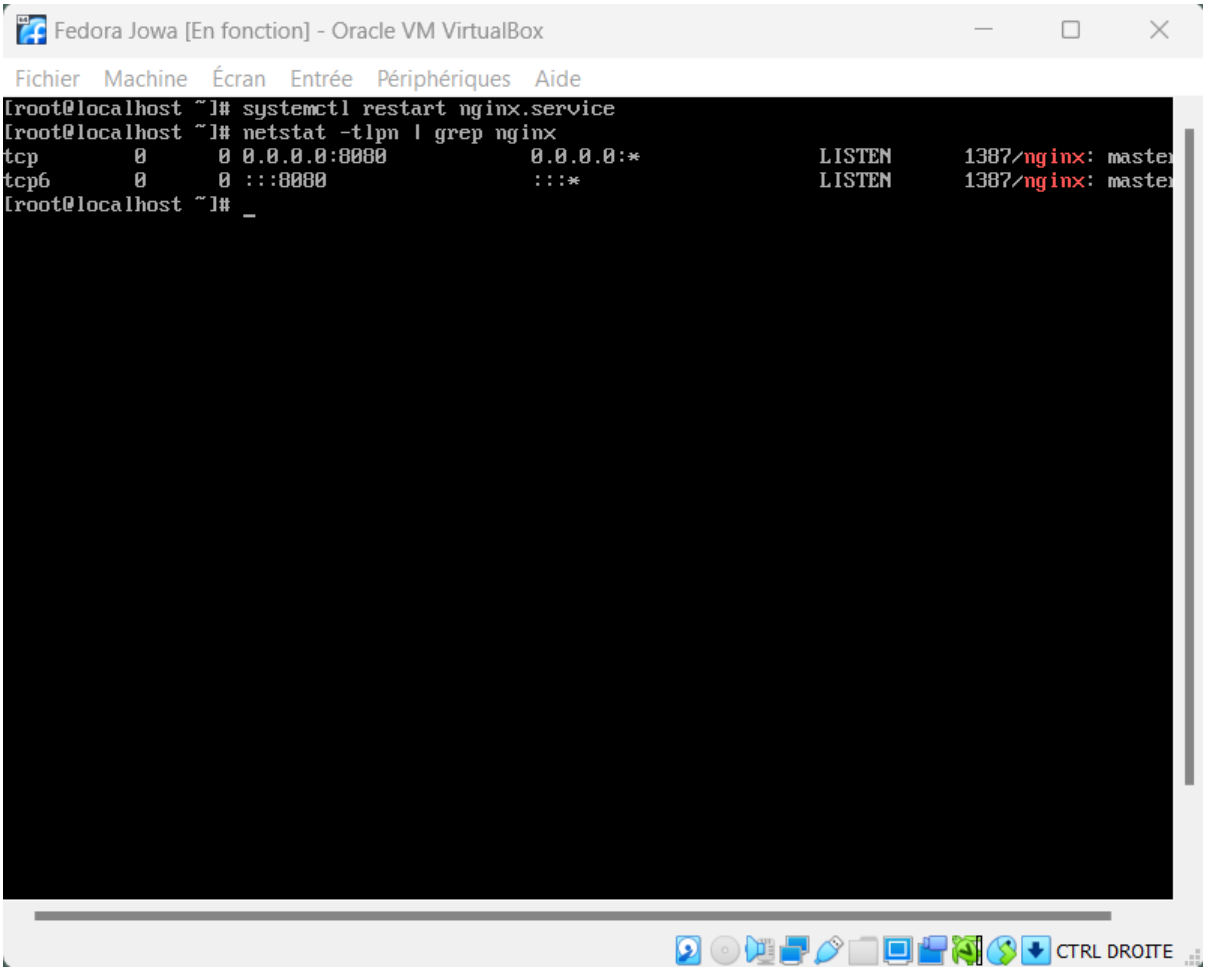
To change the port, we need to go back to the :



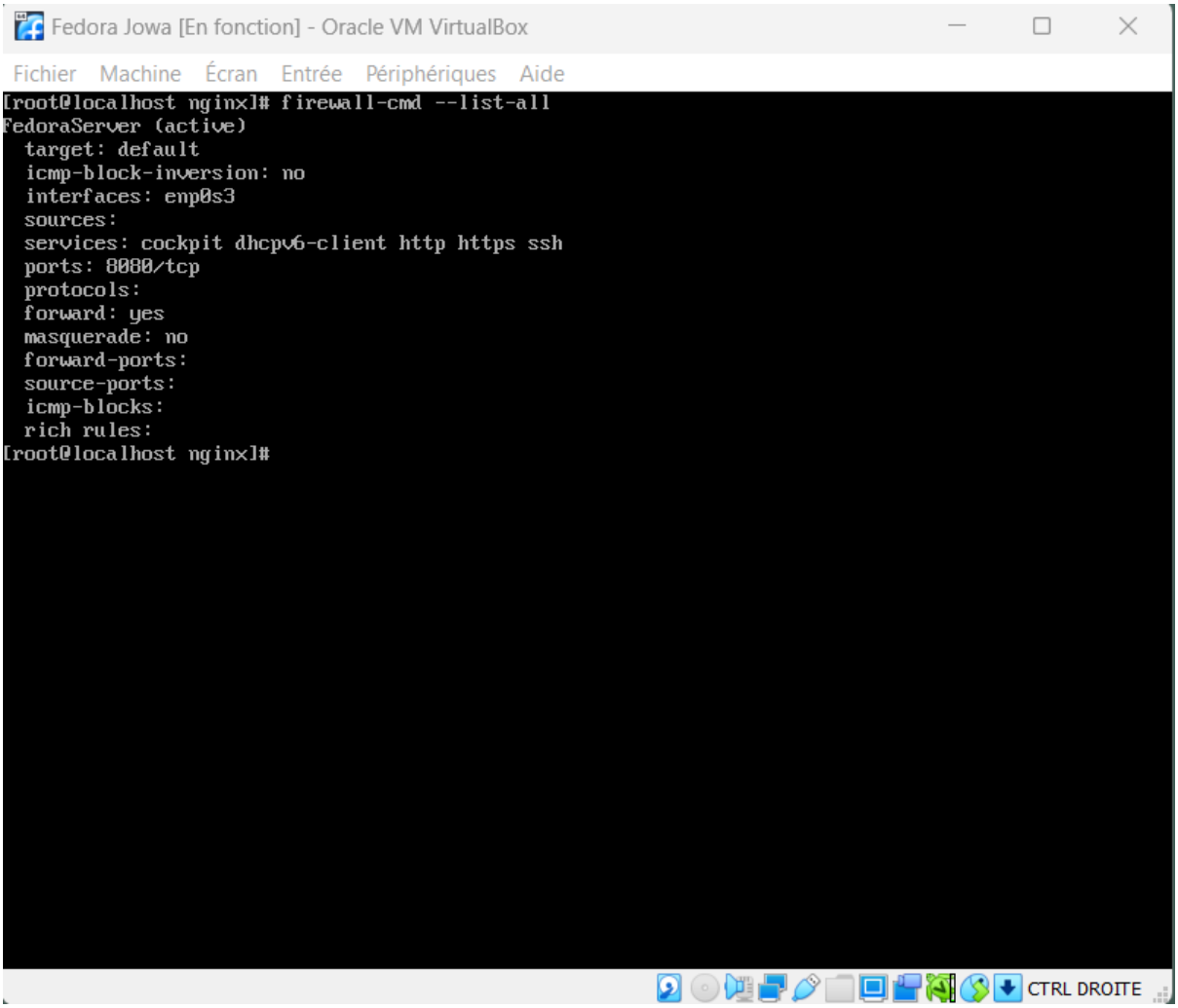
Thus, change the following port:



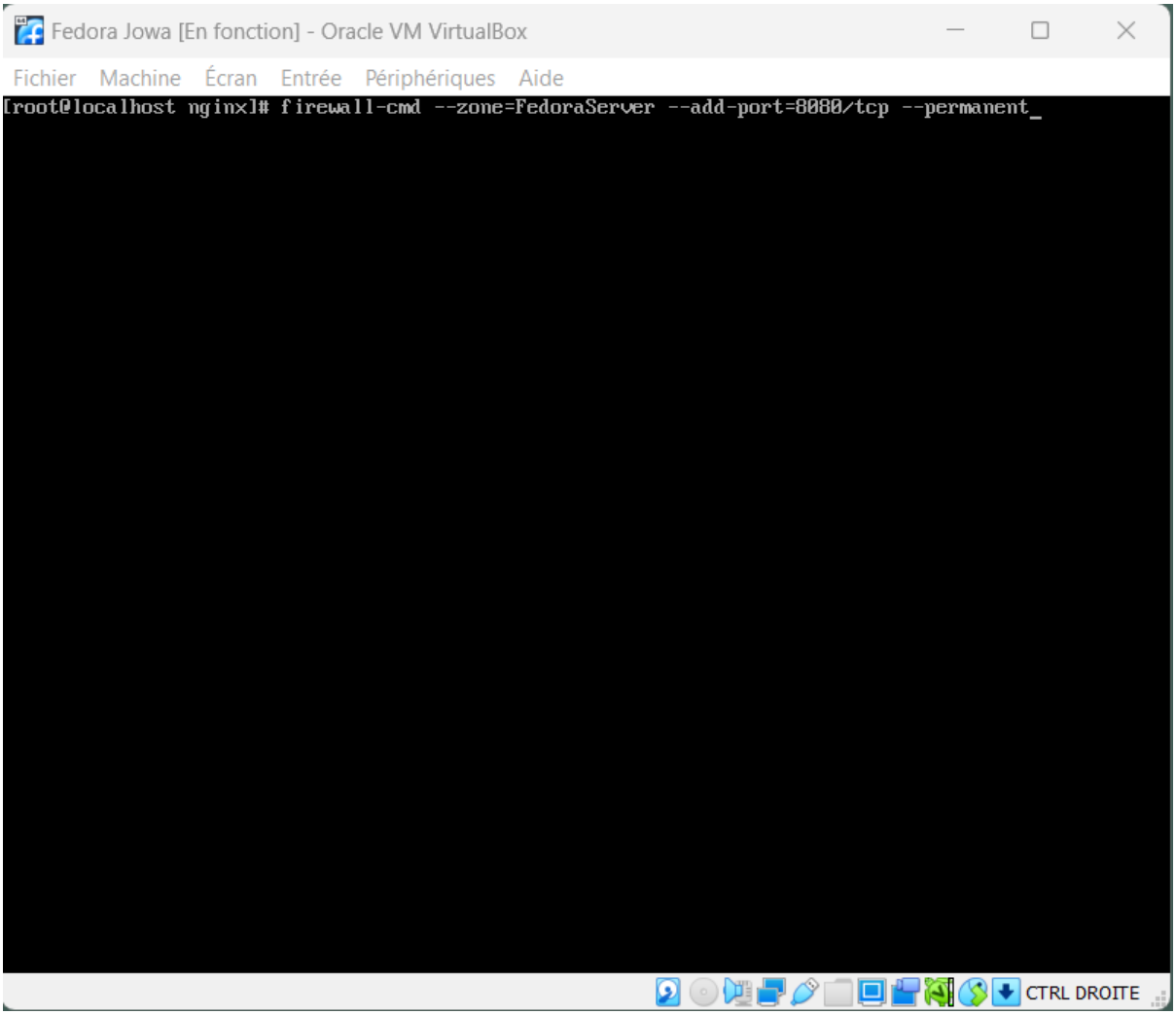
After changing the configuration, we need to restart the service to take effect and check if port "8080" is listening, "netstat" for network status and options, the "|" to retrieve the response from the "netstat" command and use the right hand side of the "|" to search this result and filter out only lines that contain the word "nginx":



Of course we need to add a port exception "8080" to the firewall. First of all we need to know the active and current area of the "Fedora" firewall which is called according to the following image "FerdoraServer:

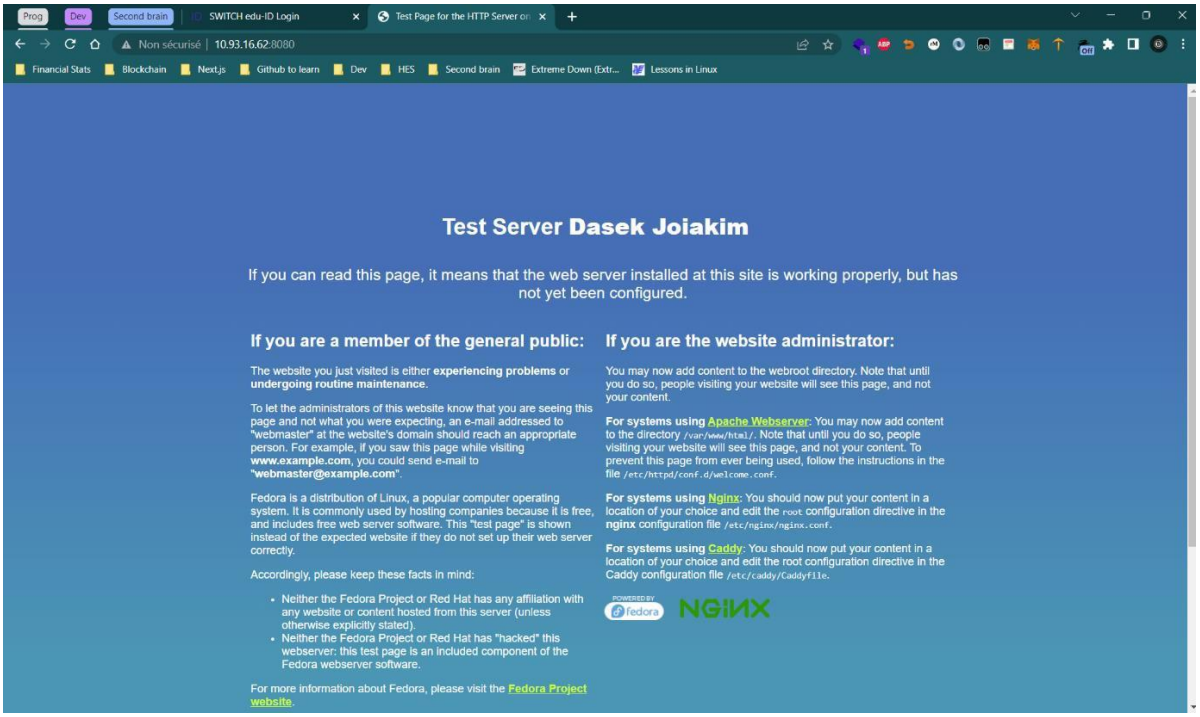


We must therefore add port "8080" to the "FedoraServer" zone permanently to that after restarting the server, everything works:



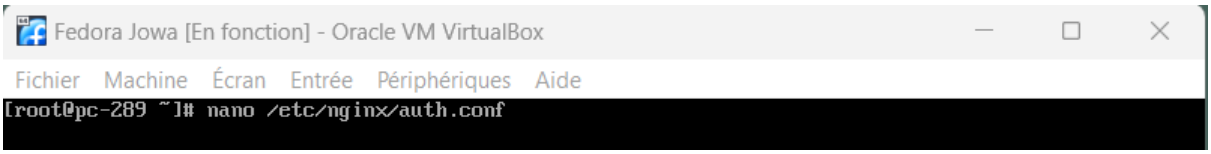
We need to restart the firewall service for the changes to take effect:

Finally we can access the website with the port "8080":

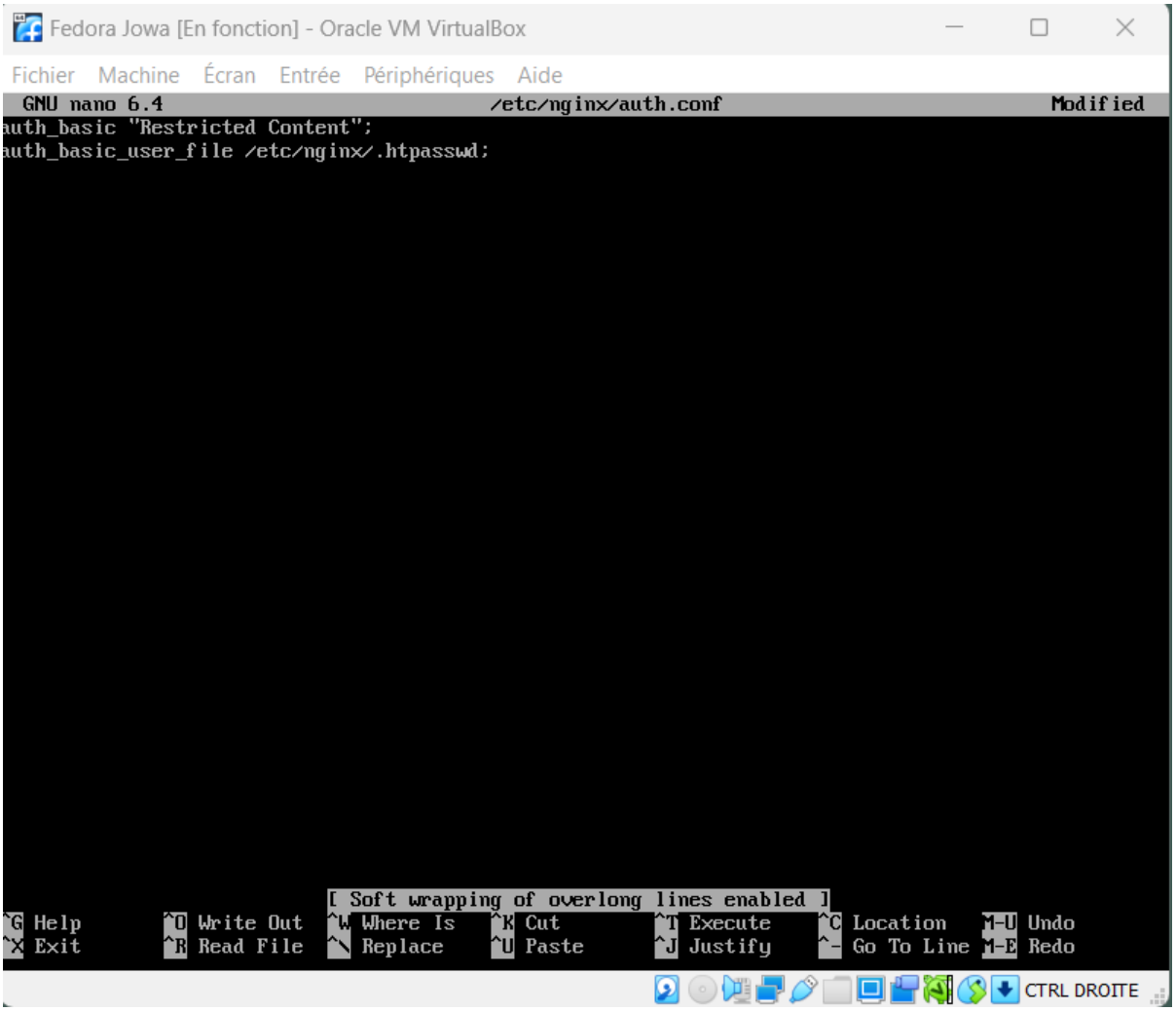


Authenticated access (optional)

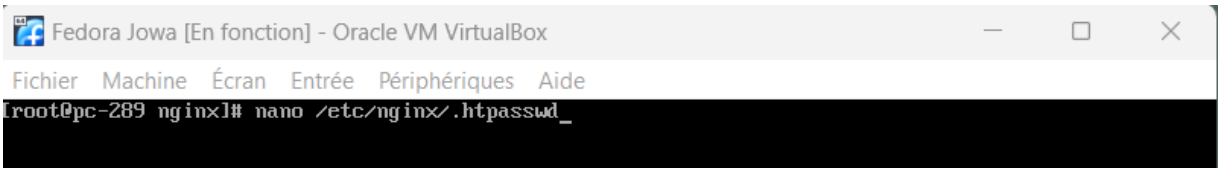
To protect a folder from its contents. You will need to perform the following steps. First, create a configuration file in the "nginx" configuration directory:



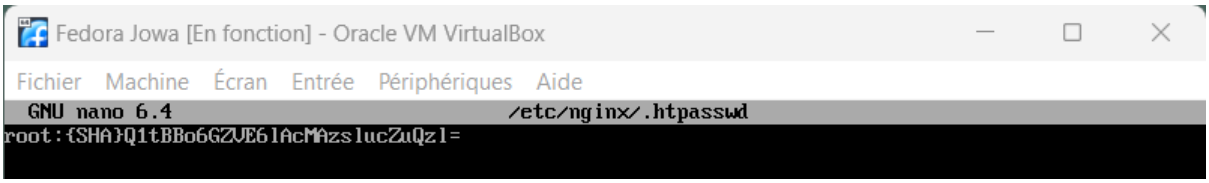
Then we will enter the data and the path to the hidden file ".htpasswd" which will contain sensitive data:



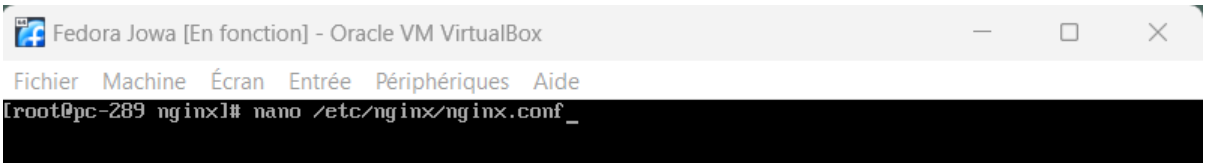
We must therefore create this file in the same way as the previous one:



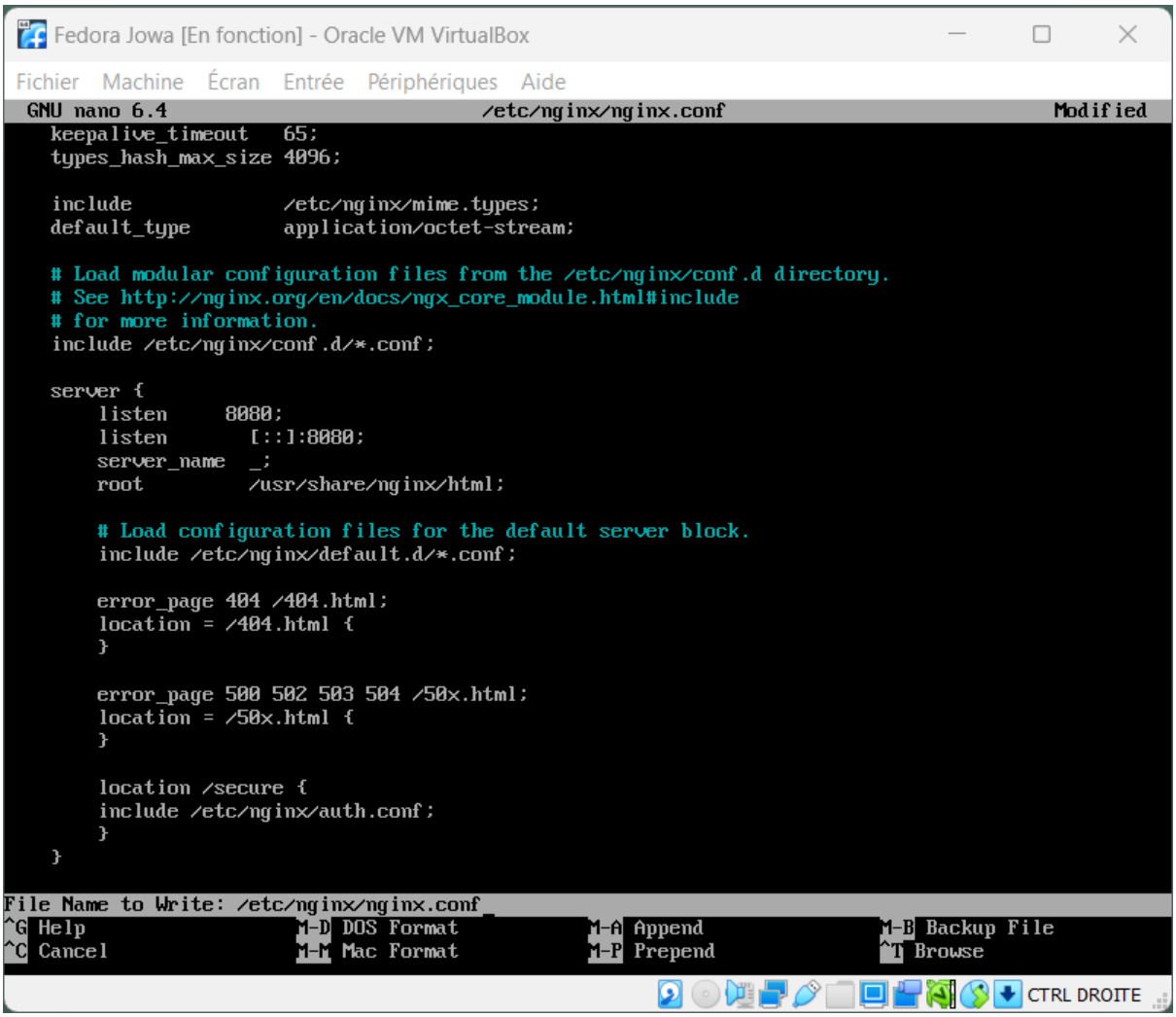
And add these lines, we can use online tools to encrypt the password, here I used the hash function "SHA-1":



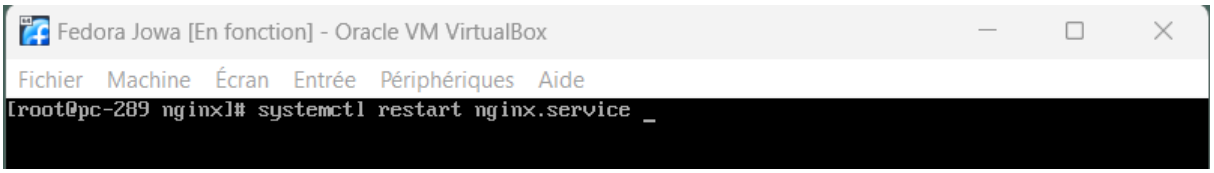
And finally we need to modify the nginx server configuration to add a route that points to a secure folder:



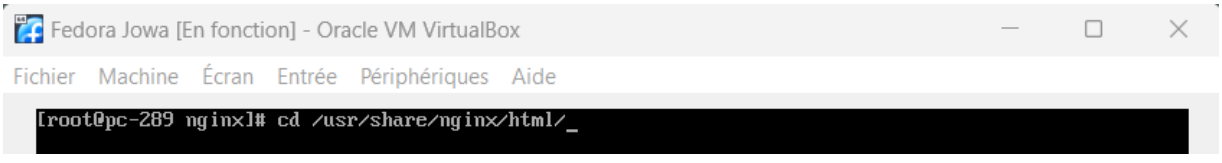
And add these lines for the 'secure' route:

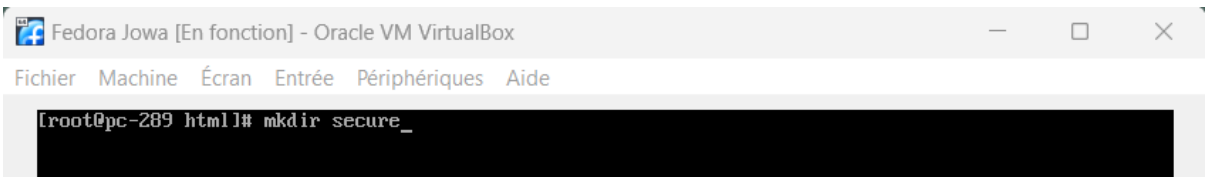


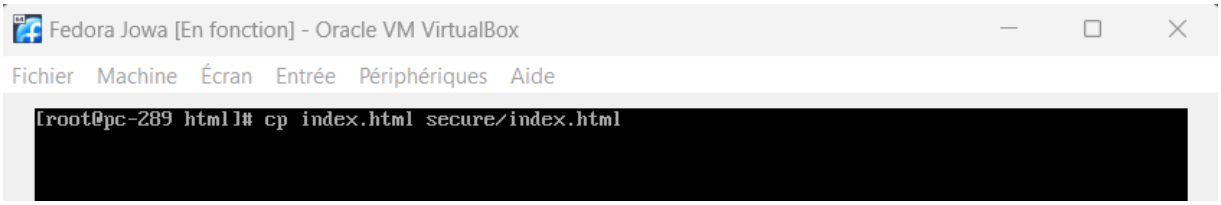
The service must be restarted for this to take effect:



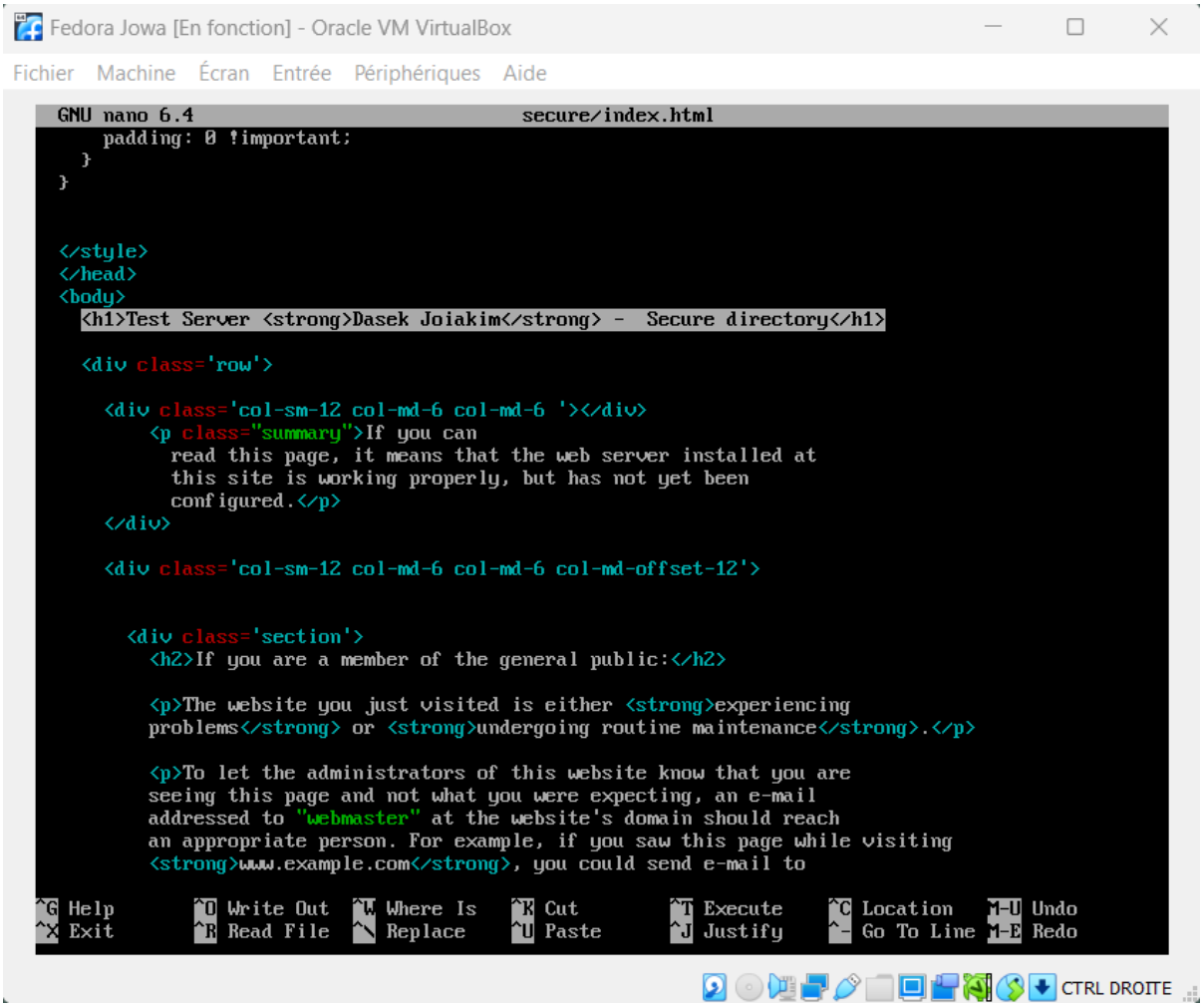
We need to move to the root of the WEB application, and add a new folder called
In the "secure" section, copy the "index.html" file and modify the "HTML" title tag:



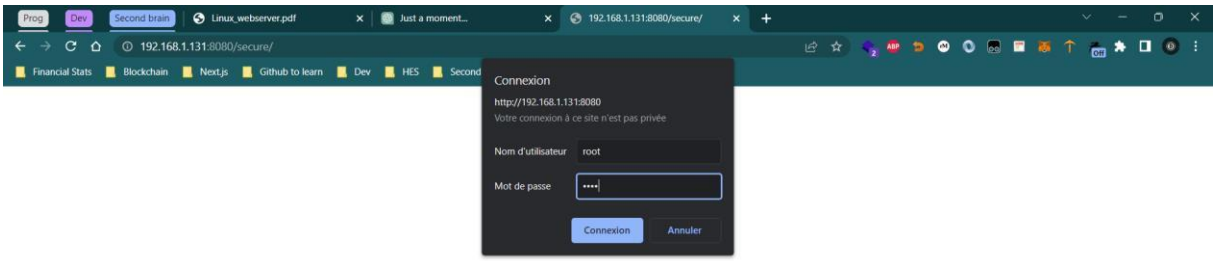




Then change the title:



This allows us to test whether the route is secure:



We have secured a file: