sudo apt install openjdk-11-jre
(JRE (java runtime environment) je potreban za pokretanje Java aplikacija i Java-based servera, kao što je Jenkins u ovom slučaju.)

/potreban ključ koji će se koristiti za kriptografsko zaštitu podataka koji će se razmjenjivati između uređaja./
JENKINS REPOSITORY KEY:
wget -q -O - https://pkg.jenkins.io/debian-stable/jenkins.io.key | sudo apt-key add -
(public/private key combination - verifies the packages and that's how apt works)

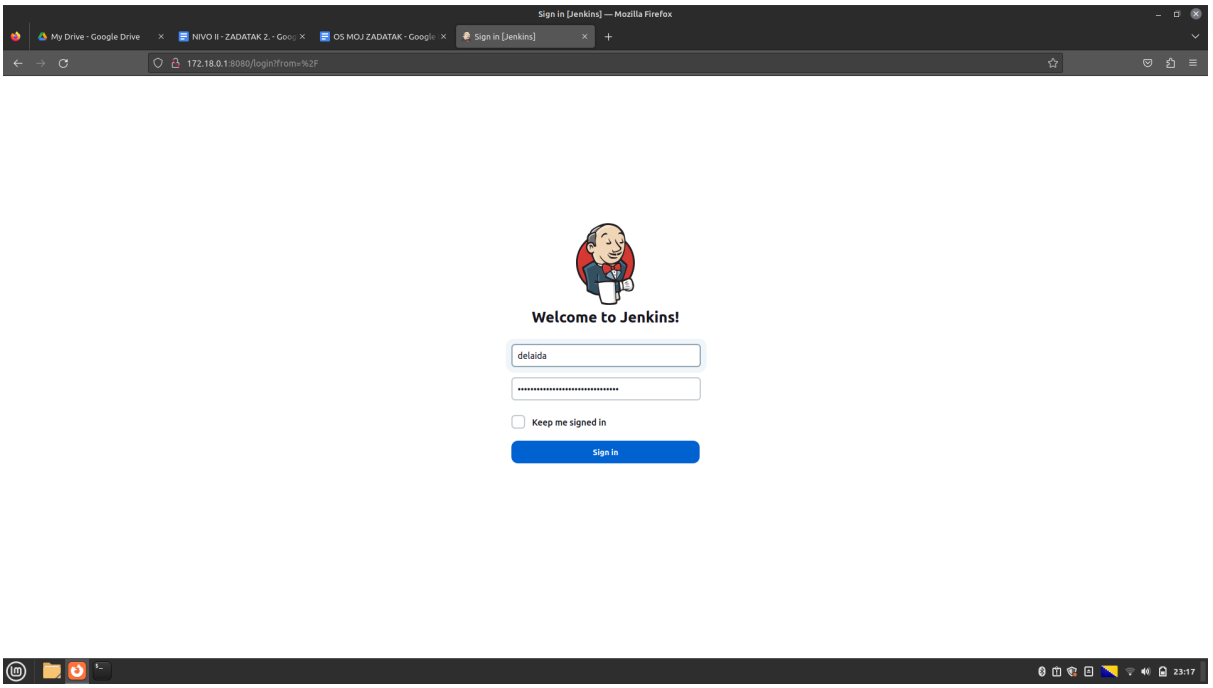
UPDATE THE REPOSITORY SOURCE LIST
sudo sh -c 'echo deb http://pkg.jenkins.io/debian-stable binary/ > /etc/apt/sources.list.d/jenkins.list'
(ECHOES THE PATH INTO THE FILE)

sudo apt install jenkins
sudo systemctl status jenkins
(aktivira se automatski)

Enable the file for security

sudo ufw allow ssh
sudo ufw allow 8080 (standardni port za jenkins)
sudo ufw enable
sudo ufw status (da provjerimo da je sve aktivirano)

Ifconfig (tražimo našu ip adresu)
Kada je pretražimo sa 172.18.1.0:8080 otvara se jenkins sučelje (not secure connection)

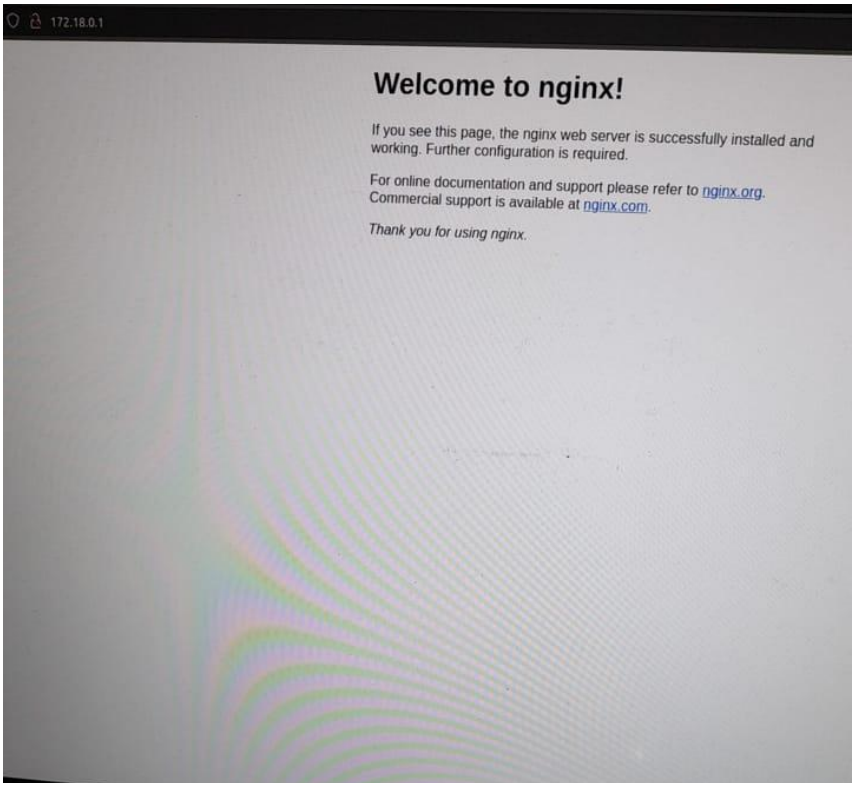


Installing a web server (koristimo nginx):
sudo apt install nginx

Adding firewalls for nginx:
sudo ufw app list
sudo ufw allow “Nging Full”
sudo ufw status (da provjerimo da je ovaj servis dodan)

systemctl status nginx

Nakon ovoga, kada idemo na: 172.18.1.0 dobijamo nginx
Sada imamo jenkins na portu 8080 i nginx, što treba da povežemo (da zaštitimo, kreiran je self-signed certificate):



*slika kao dokaz da je ovo u jednom momentu postojalo

wget ovog fajla (sa githuba):
[req]
default_bits   = 2048
default_keyfile   = localhost.key
distinguished_name = req_distinguished_name
req_extensions   = req_ext
x509_extensions   = v3_ca

[req_distinguished_name]
countryName   = Country Name (2 letter code)

countryName_default = UK
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = London
localityName = Locality Name (eg, city)
localityName_default = London
organizationName = Organization Name (eg, company)
organizationName_default = Smertan Networks Ltd
organizationalUnitName = organizationalunit
organizationalUnitName_default = Development
commonName = Common Name (e.g. server FQDN or YOUR name)
commonName_default = genja.co.uk
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 64

[req_ext]
subjectAltName = @alt_names

[v3_ca]
subjectAltName = @alt_names

[alt_names]
IP.1 = 10.120.12.5 NA OVOM MJESTU DODAJEMO SVOJU IP ADRESU

Sljedeće što radimo, kreiramo certifikat, ova komanda radi sve za nas:
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/nginx-selfsigned.key -out /etc/ssl/certs/nginx-selfsigned.crt -config openssl_selfsigned.conf
(ovdje će da nas pita za neke informacije, korištene su default-ne, osim za common name gdje je unijeta IP adresa)

Diffie helman group creation command: (kriptografski algoritam koji se koristi za stvaranje zajedničkog tajnog ključa za dvije strane koje komuniciraju, a da pritom ne razmjenjuju tajni ključ između sebe.)
sudo openssl dhparam -out /etc/ssl/certs/dhparam.pem 2048

Make nginx aware of the ssl certificate location (confing file koji je iskorišten):
ssl_certificate /etc/ssl/certs/nginx-selfsigned.crt;
ssl_certificate_key /etc/ssl/private/nginx-selfsigned.key;

sudo mv self-signed.conf /etc/nginx/snippets/
(dodajemo file na pravo mjesto)

Konfigurišemo nginx sa secure podešavanjima za ssl: (kreirali sko ključeve, certifikat i private key i dali mu neke snippets)
Nginx ssl-params.conf download komanda:

sudo wget -O /etc/nginx/snippets/ssl-params.conf

Konfiguracije za server: (glavni konfiguracijski file, urađen je wget):

```
server {
	listen 80 default_server;
	listen [::]:80 default_server;
	server_name <yourServerAddress>;    # substitue with domain name or ip address
	return 301 https://$server_name$request_uri; # 301 moved permanently
}
server {
	# SSL configuration
	listen 443 ssl http2 default_server;
	listen [::]:443 ssl http2 default_server;
	access_log /var/log/nginx/jenkins.access.log;
	error_log /var/log/nginx/jenkins.error.log;

	server_name <yourServerAddress>; # substitue with domain name or ip address
	include snippets/self-signed.conf;
	include snippets/ssl-params.conf;
	location / {
		include /etc/nginx/proxy_params;
		proxy_pass          http://localhost:8080;
		proxy_read_timeout  90s;
		# Fix potential "It appears that your reverse proxy setup is broken" error.
		proxy_redirect      http://localhost:8080 https://<yourServerAddress>; # substitue
with domain name or ip address
	}
}
```

Pomoću sed -i.bak “s/<yourServerAddress>/172.18.1.0/g” jenkins
Ova komanda globalno mijenja ova dva izraza u file-u iznad

sudo mv jenkins /etc/nginx/sites-available/

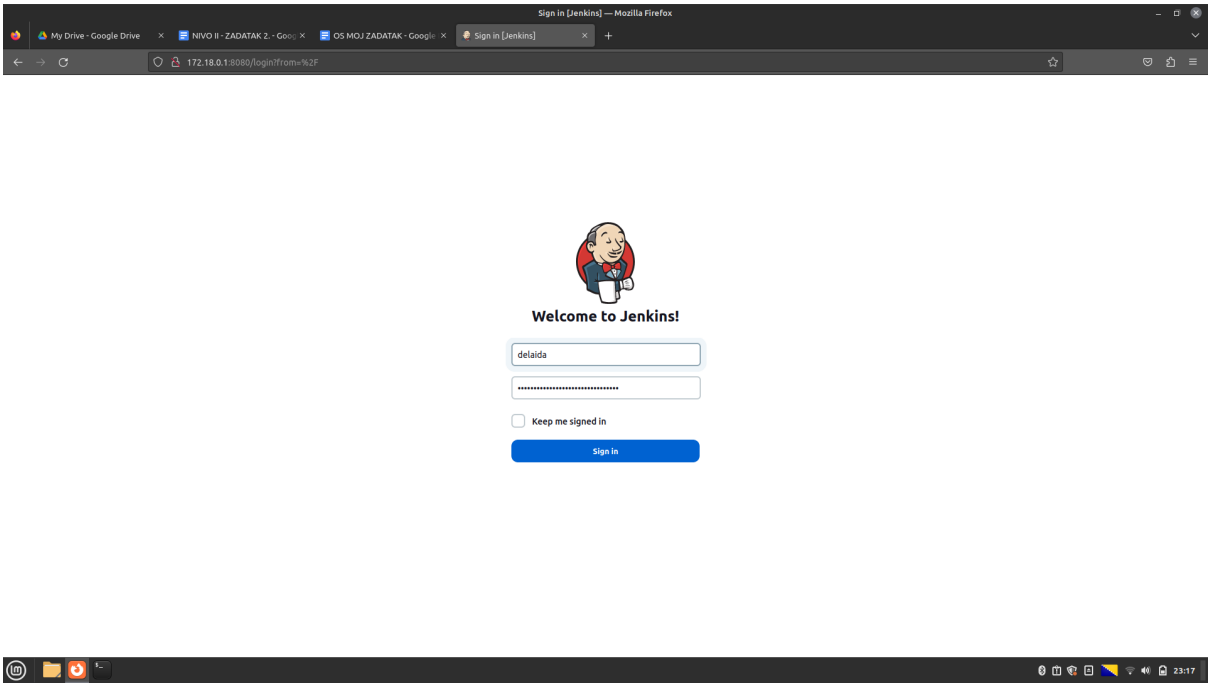
Pravimo symbolic link:
sudo ln -s /etc/nginx/sites-available/jenkins /etc/nginx/sites-enabled/jenkins
(sada je aktivirano)

Zbog greške, dodana je ova komanda:
sudo rm /etc/nginx/sites-enabled/default (jer smo imali 2 defaulta, imali svo 2 sajta u sites-enabled)

Posljednja stvar za jenkins:
sudo vim /etc/default/jenkins
Na kraju argumenata radimo (dodajemo) httpListenAddress=127.0.0.1

Restartujemo oba servisa:
sudo systemcl restart nginx jenkins

Nakon ovoga, kada odemo na našu IP adresu, te pošto imamo self signed certificate, odobrimo pristup na https://172.18.1.0, te smo ‘securely connected’ na https, što samo treba biti spremljeno u permisijama da bismo pristupili



Projekat dodan na jenkins možemo pokrenuti preko terminala:
vim "/var/lib/jenkins/workspace/Jenkins first project.txt"