Universidad ORT Uruguay

Facultad de Ingeniería

Taller de servidores Linux

Noguera, Aaron - 265834

Profesor: Enrique Manuel Verdes Míguez

2024

Declaración de auditoria

Se declara que el trabajo que se presenta en esta obra es de mi propia autoría. Puedo asegurar que:

- La obra fue producida en su totalidad mientras realice el trabajo final del Taller de servidores Linux
- Cuando he citado obras de otros, he indicado las fuentes. Con excepción de estas citas, la obra es enteramente mía.
- Cuando la obra se basa en trabajo realizado conjuntamente con otros, he explicado claramente qué fue contribuido por otros, y qué fue contribuido por mí.

Índice

Declaración de auditoria 2
Introducción 4
Instalación de Ansible Controller 5
Instalación APP Server 8
Instalación BD Server 11
Preparación del entorno para Ansible 14
Ejecución de los playbooks 14
Creación de los playbooks 18
Pruebas de funcionamiento de la aplicación 21
Bibliografía 22

Introducción

Se plantea instalar 3 servidores, cada uno con características y propósitos diferentes, para luego poder desplegar mediante la herramienta Ansible, todos los servicios necesarios para alojar una aplicación de tomcat.

Se solicita implementar LVM en los servidores APP Server y BD Server con las siguientes dimensiones:

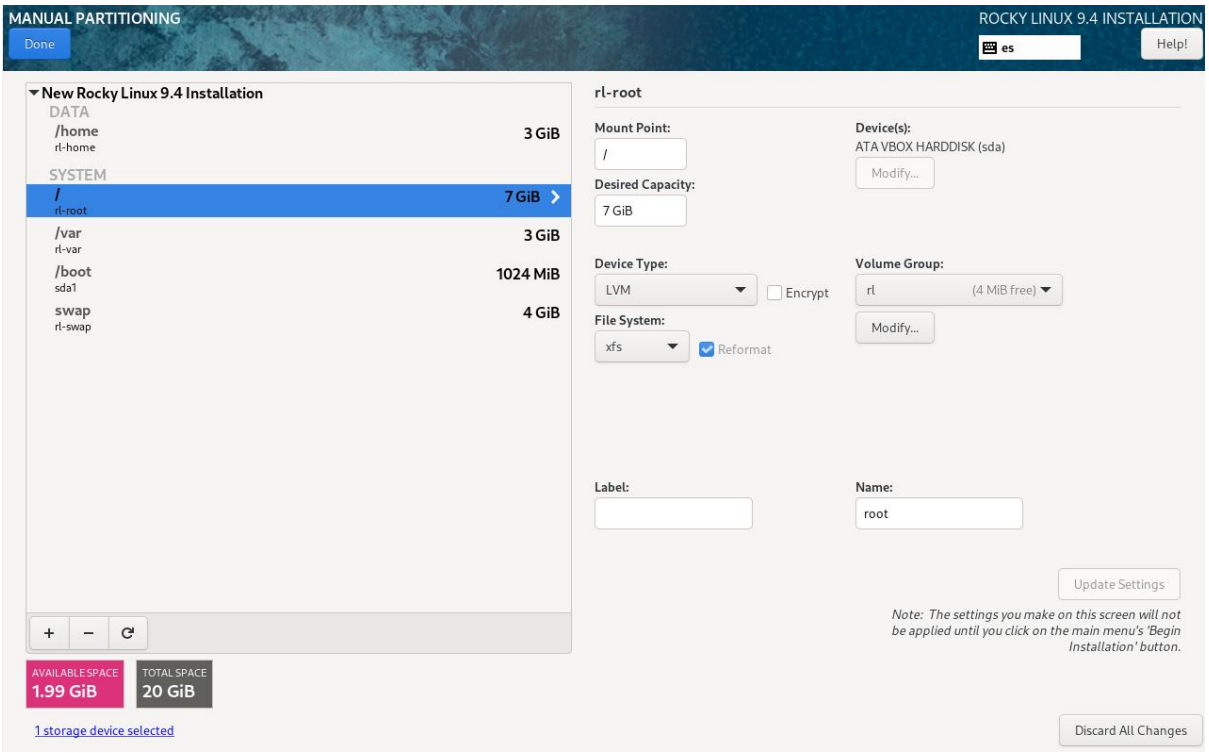
- Partición de 1GB para /boot
- LVM de 7GB para /
- LVM de 3GB para /var
- LVM de 2GB para SWAP

Las características de los servidores son las siguientes:

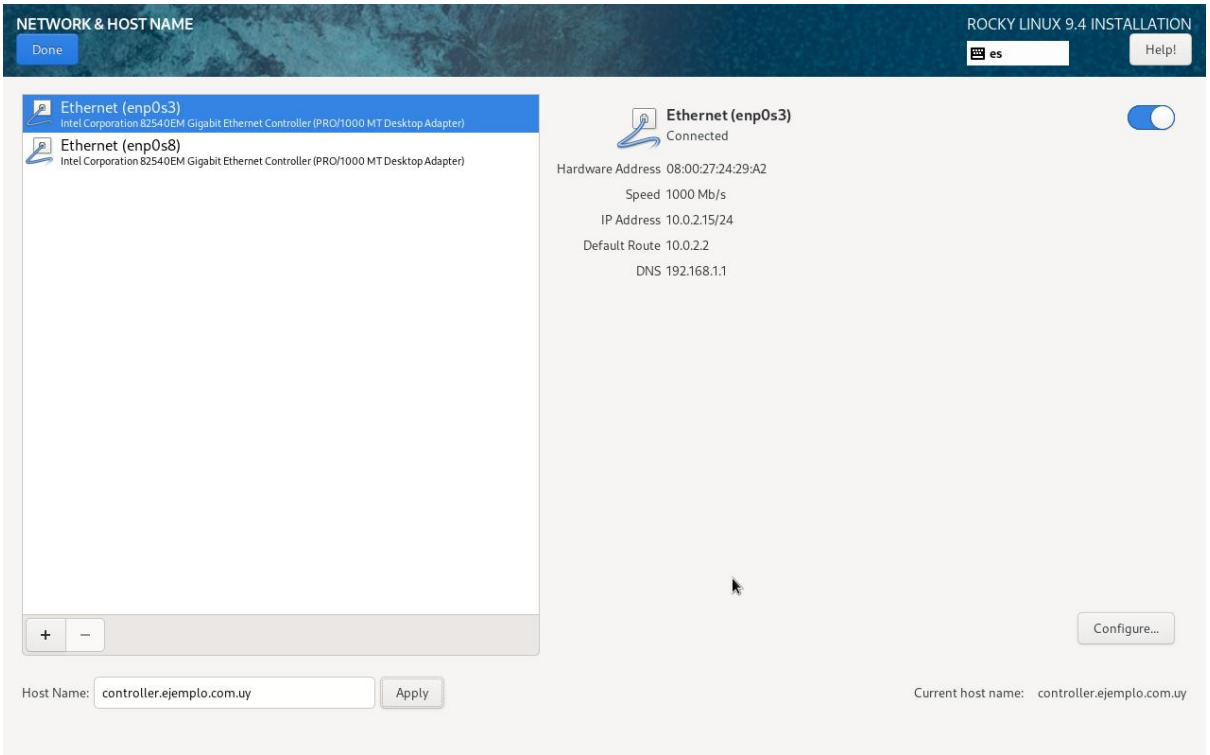
- Ansible Controller:
    - SO: distribución de la familia de Red Hat.
    - Tipo: Workstation.
    - Software instalado: Ansible, Git.
- APP Server:
    - SO: distribución de la familia de Red Hat.
    - Tipo: Minimal server
    - Software instalado: JDK, Tomcat.
- BD Server
    - SO: Ubuntu Server 24.04.
    - Tipo: Ubuntu Server.
    - Software instalado: MariaDB

Instalación de Ansible Controller

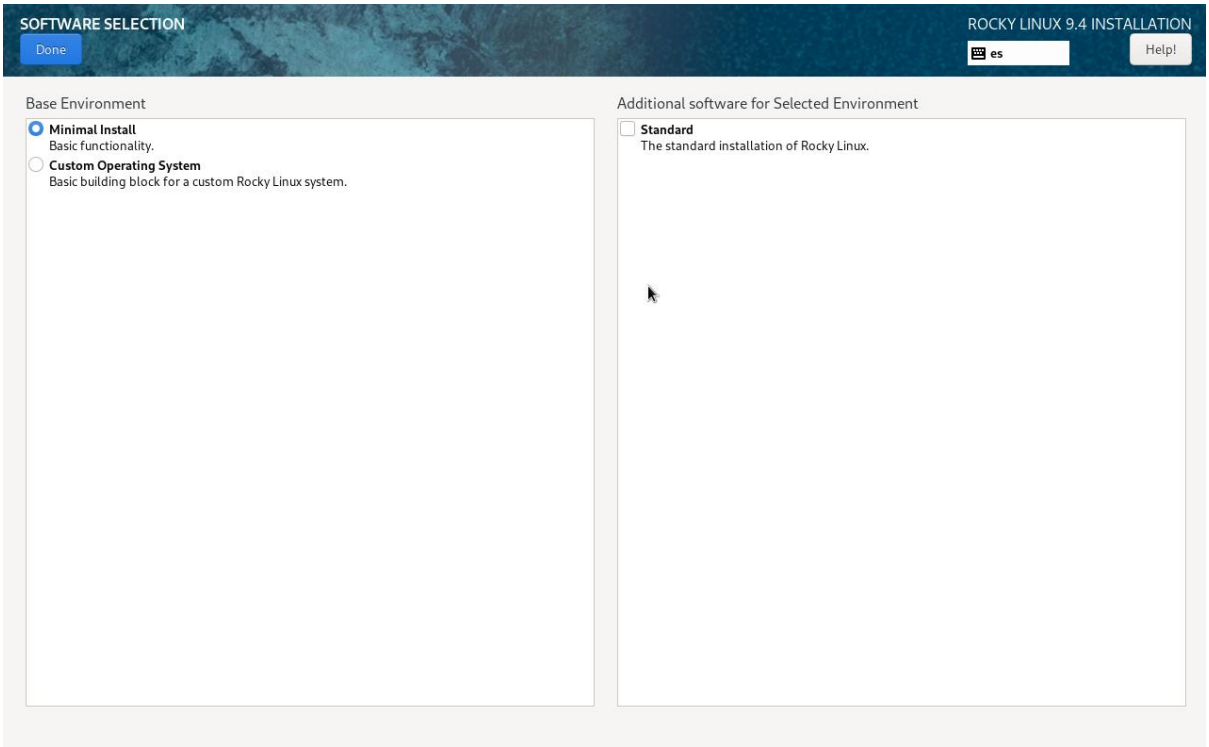
Se configura LVM.



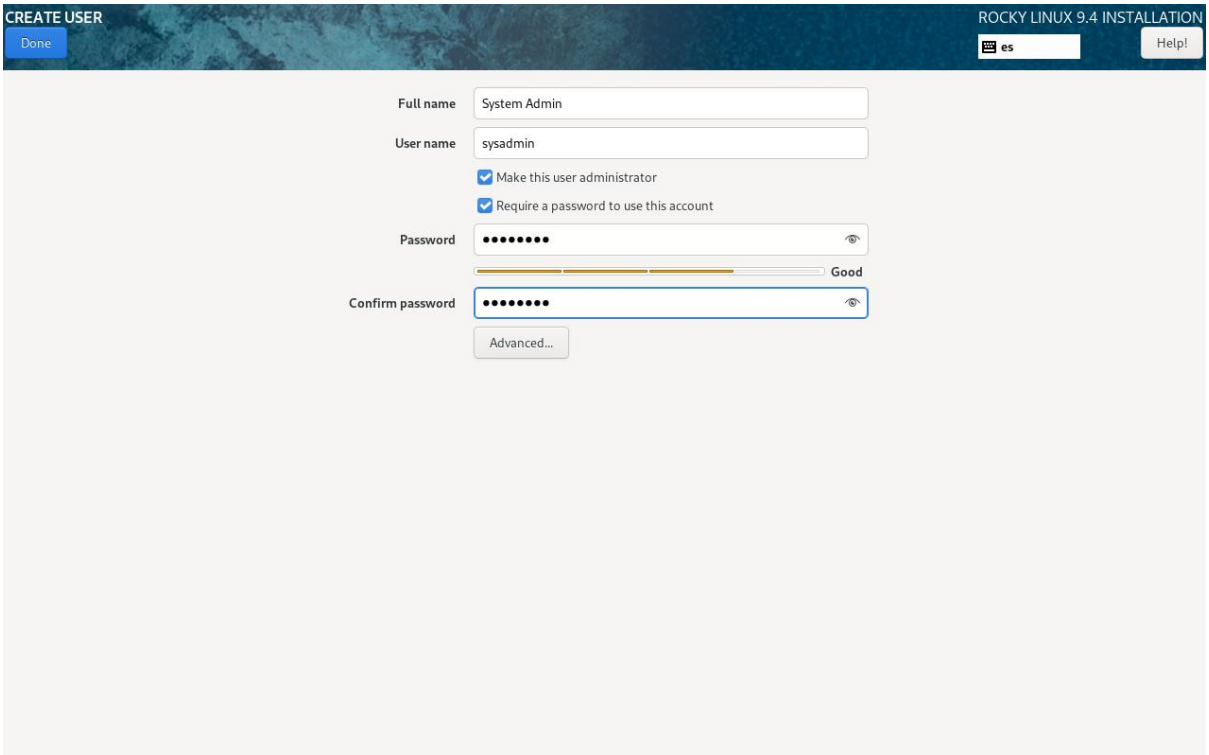
Configuración de red.



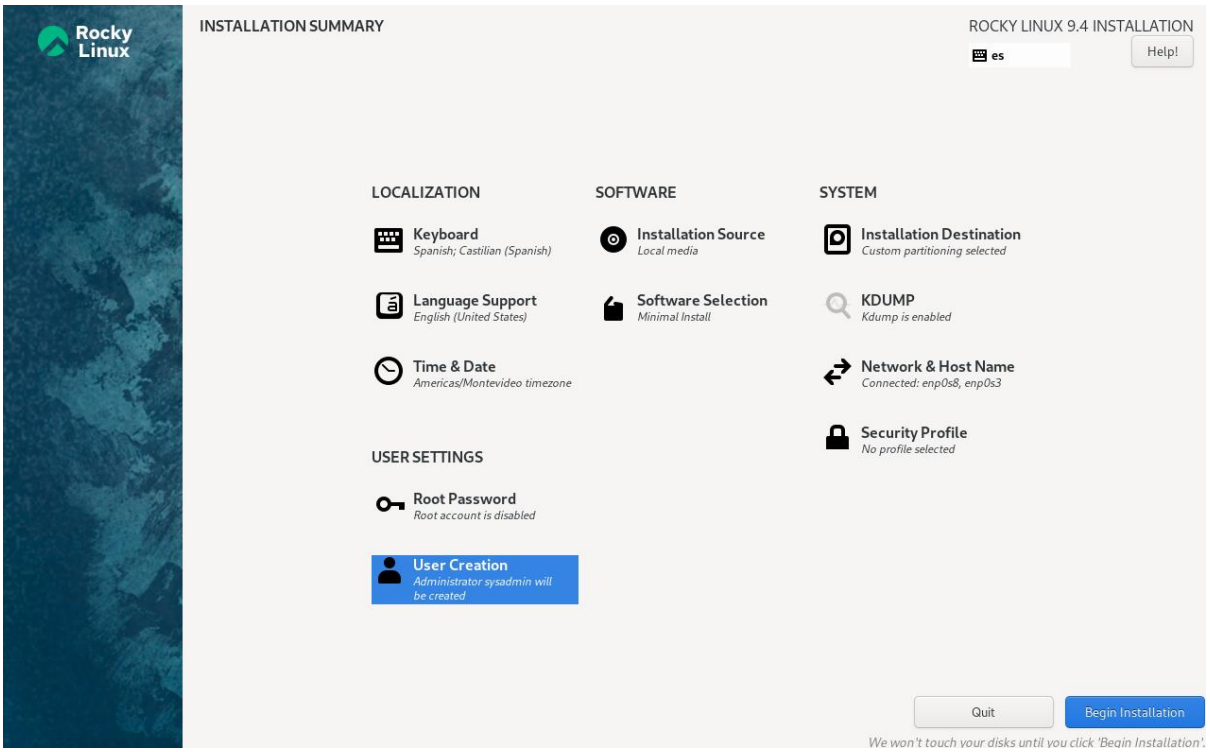
Selección de software. Se selecciona minimal install.



Configuración de usuario con permisos de administrador.



Resumen de instalación

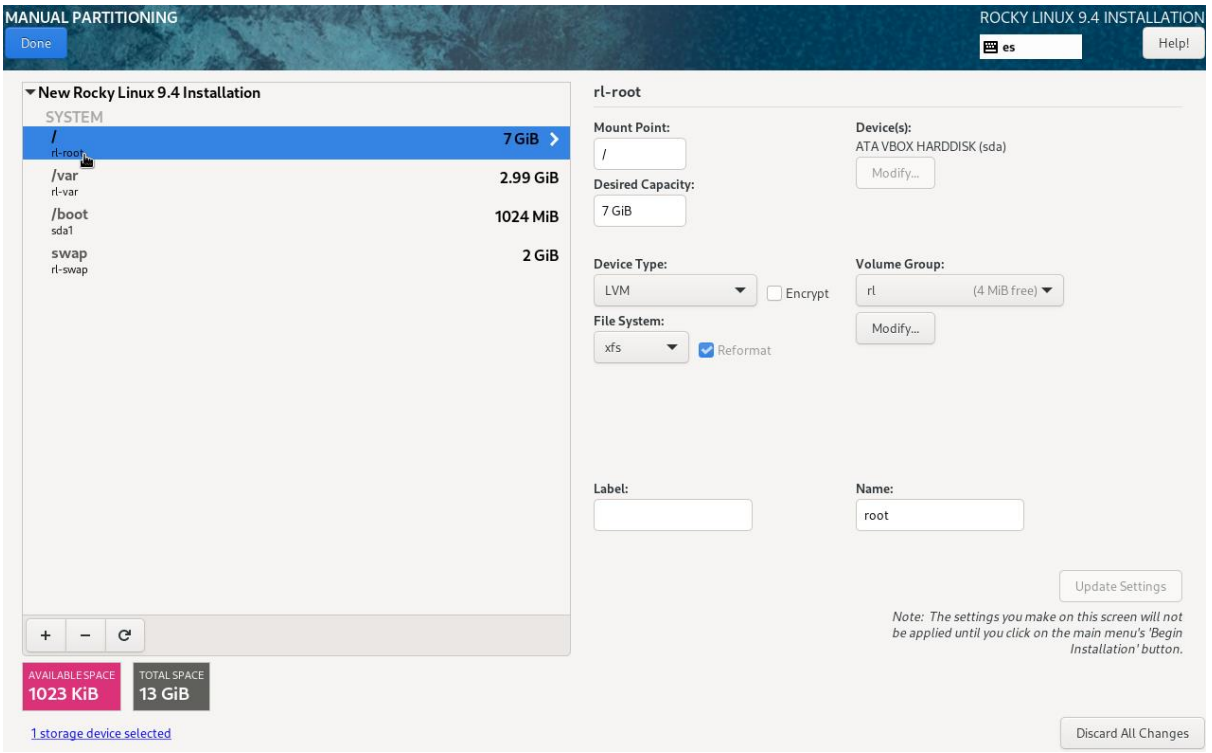


Para convertir el servidor en tipo Workstation se ejecutan los siguientes comandos:

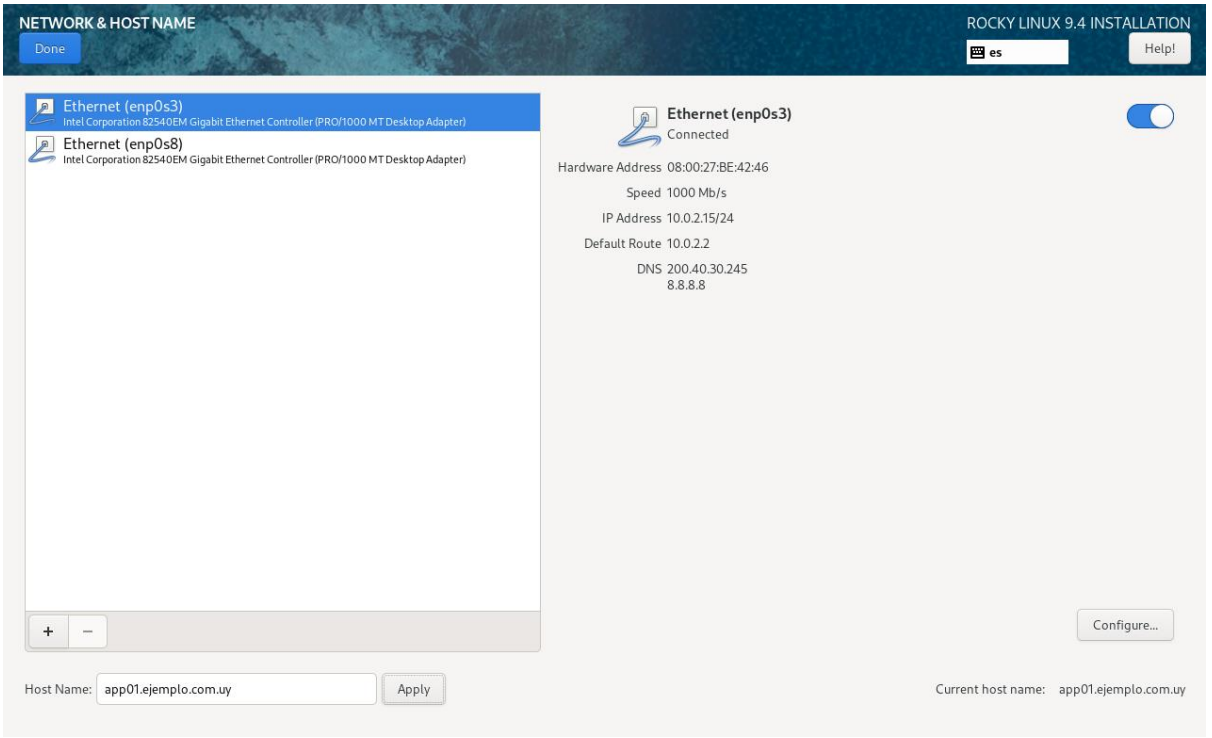
- sudo dnf groupinstall Workstation
- sudo systemctl set-default graphical.target
- sudo systemctl isolate graphical.target

Instalación APP Server

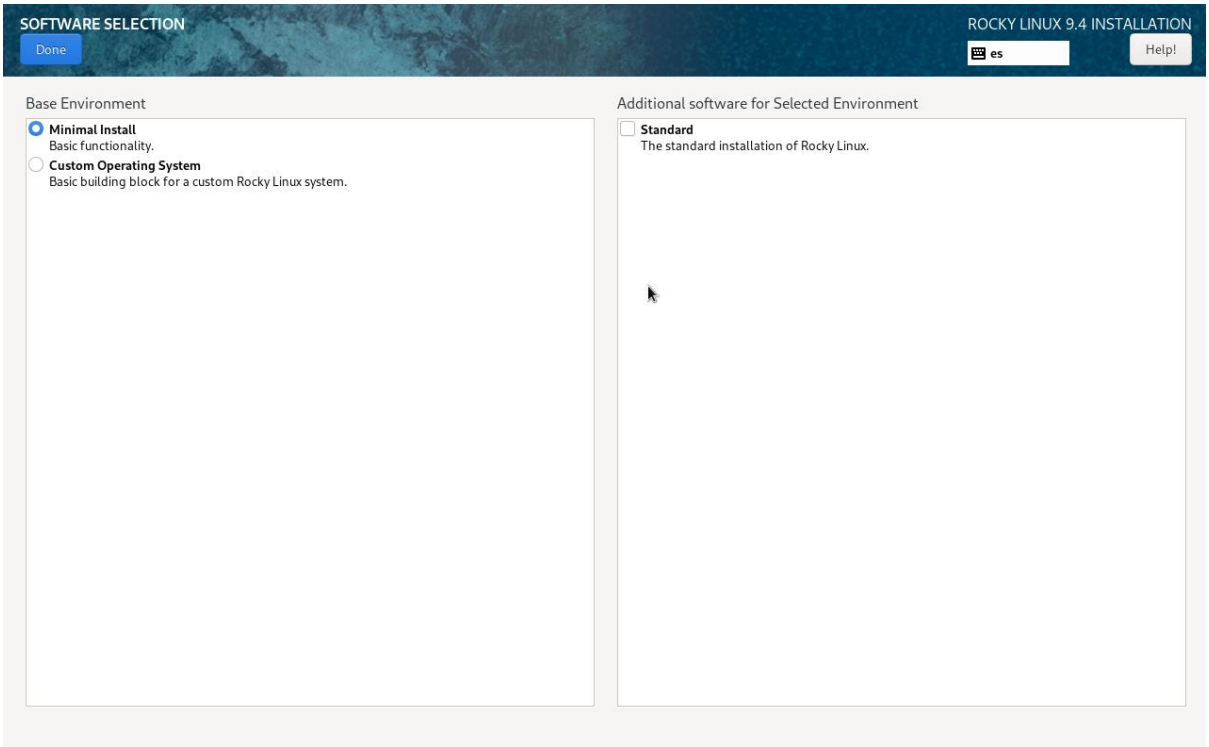
Configuración de LVM.



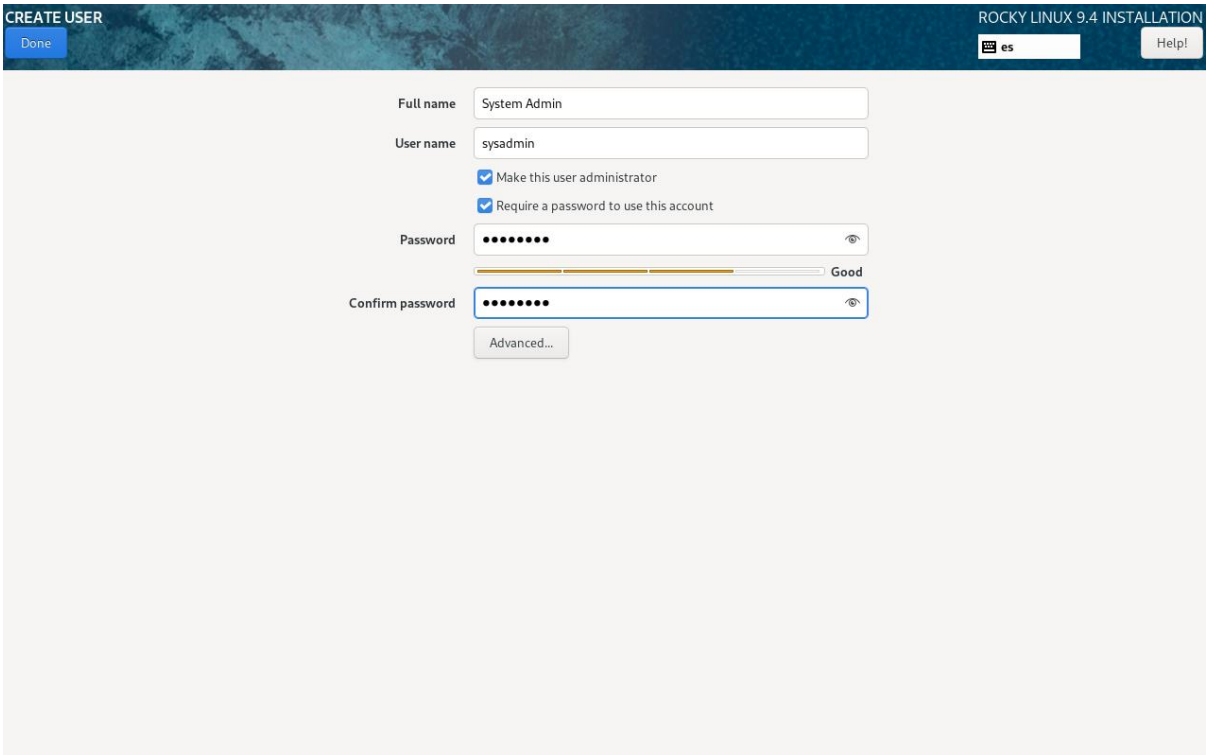
Configuración de red en la instalación.



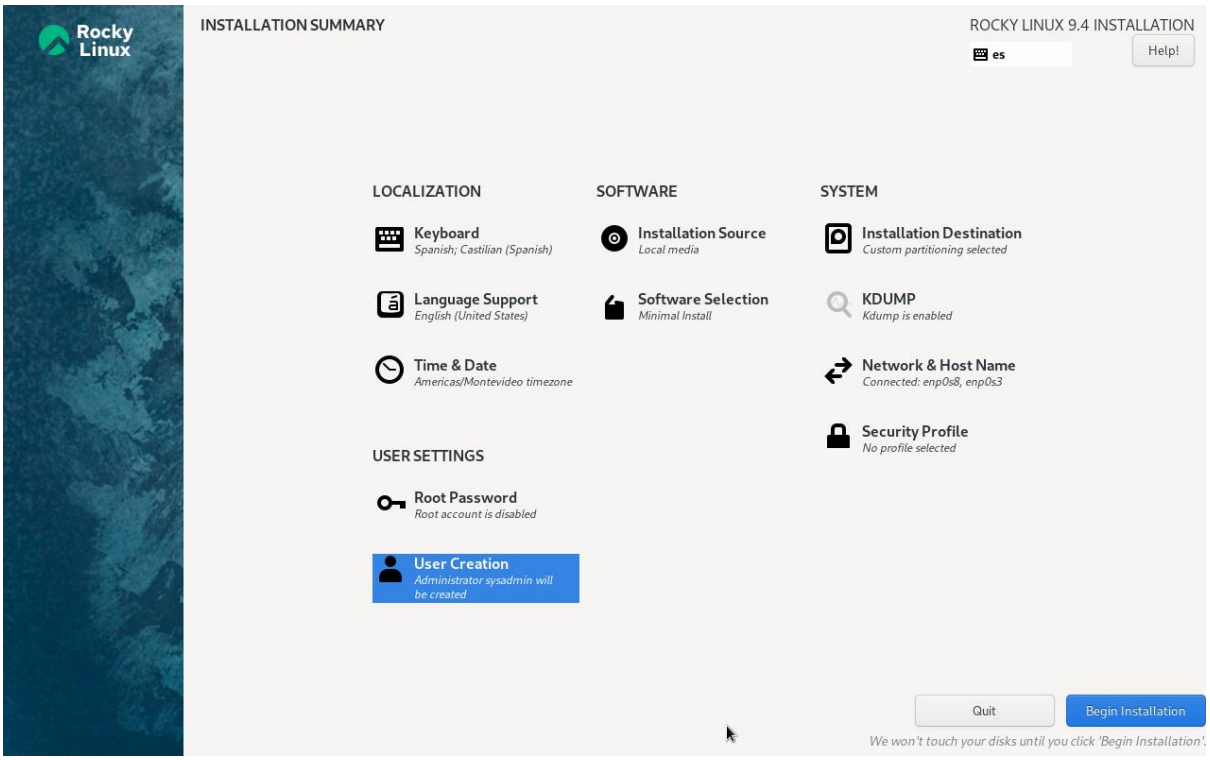
Selección de software. Se selecciona minimal install.



Configuración de usuario con permisos de administrador.



Resumen de instalación.

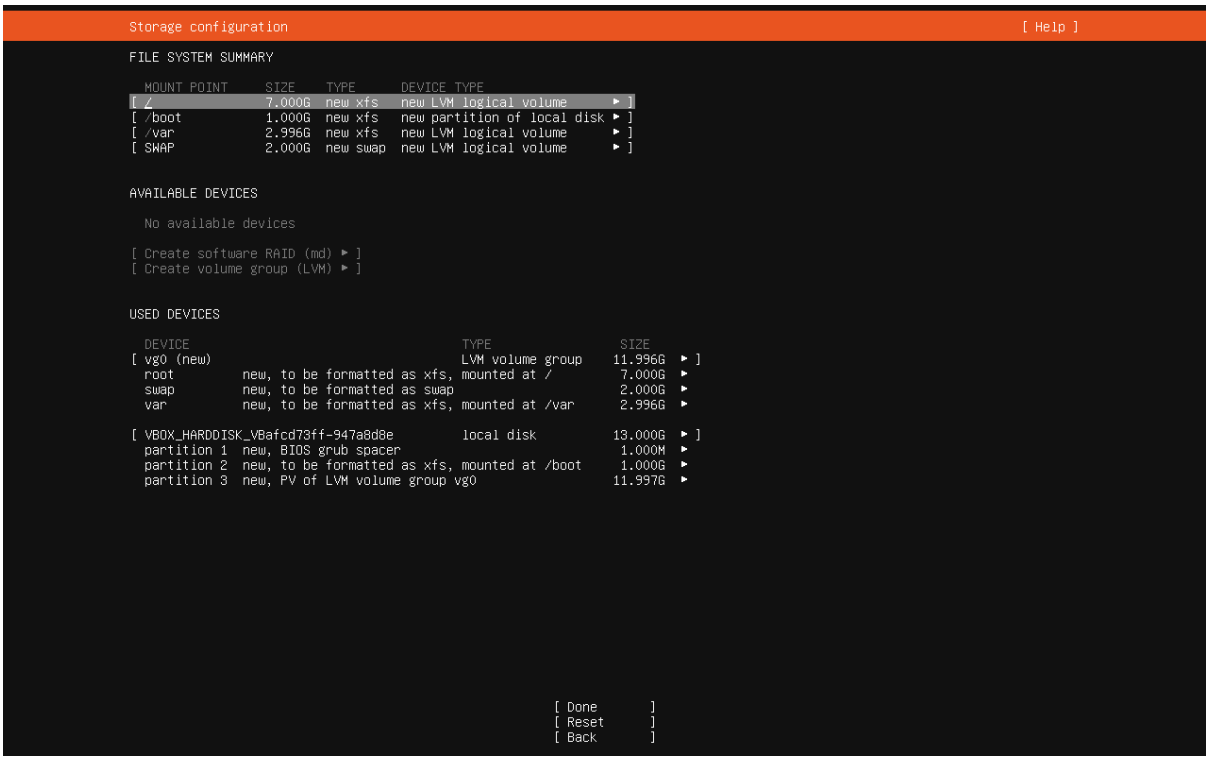


Comandos ejecutados para configurar el direccionamiento IP:

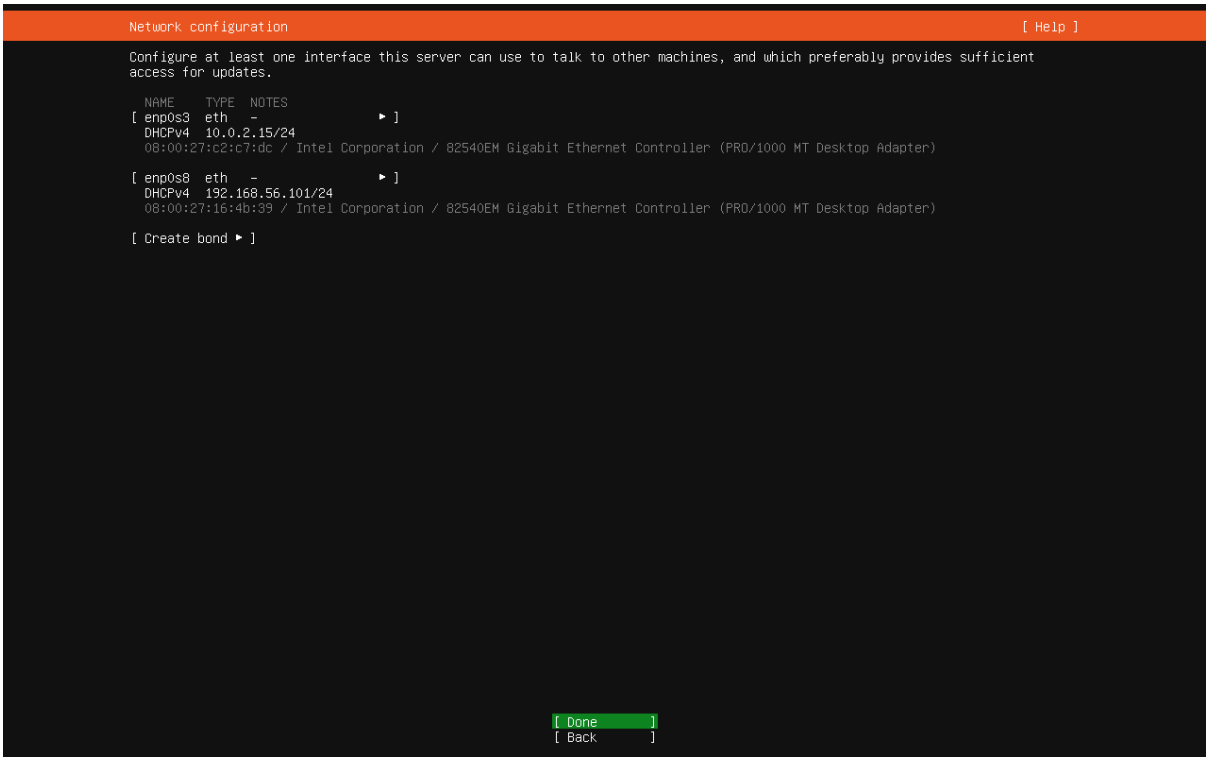
- sudo nmcli con mod enp0s8 ipv4.addresses 192.168.56.20/24
- sudo nmcli con mod enp0s8 ipv4.method manual
- sudo nmcli con up enp0s8

Instalación BD Server

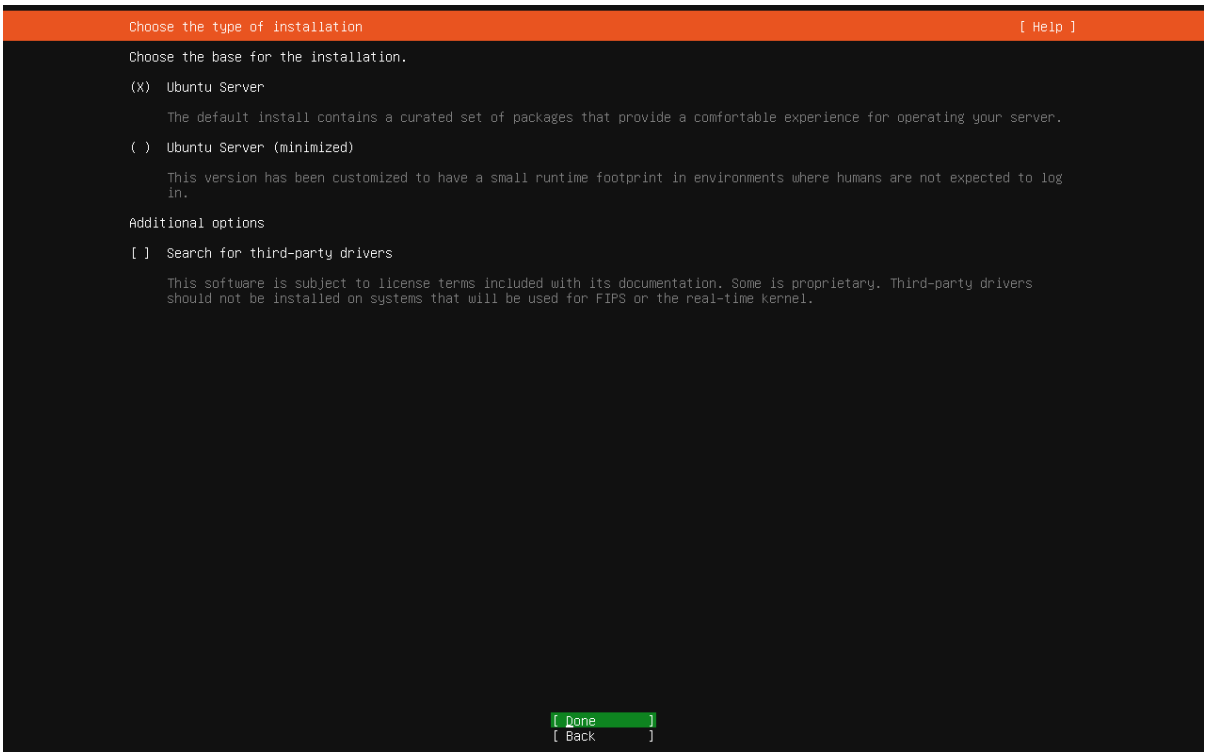
Configuración de LVM.



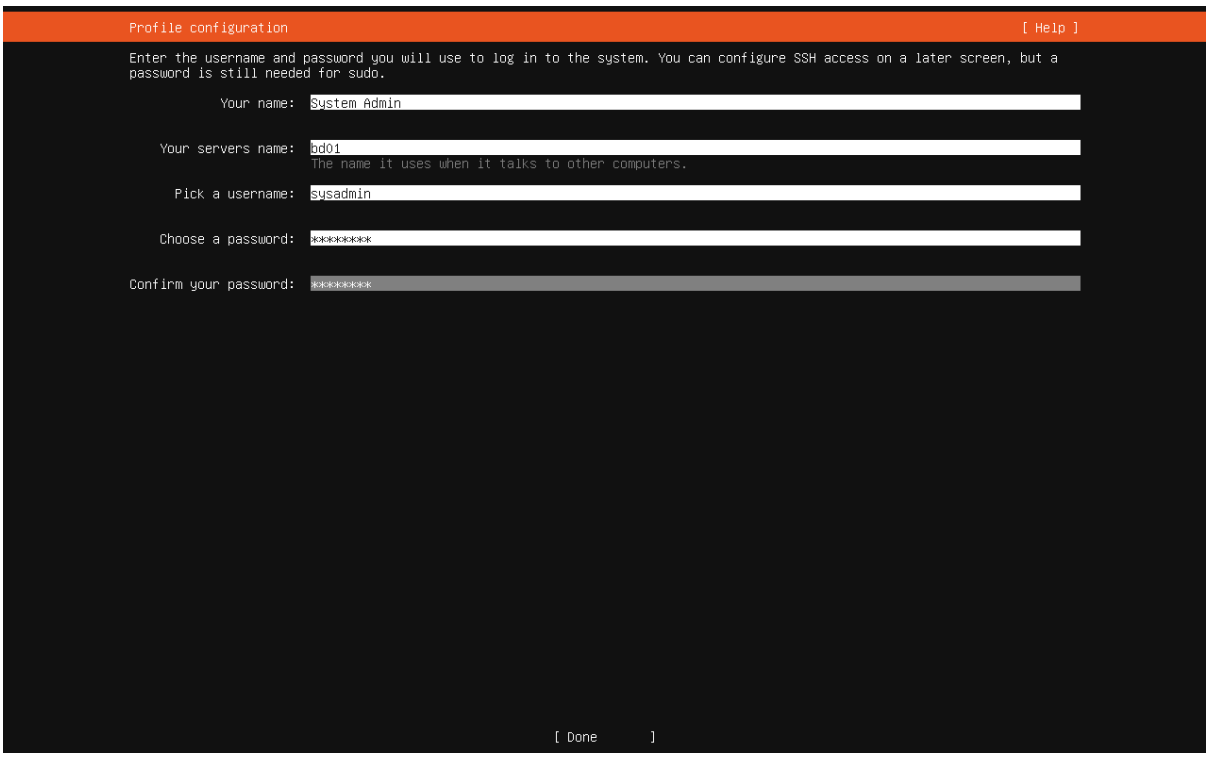
Configuración de red en instalación.



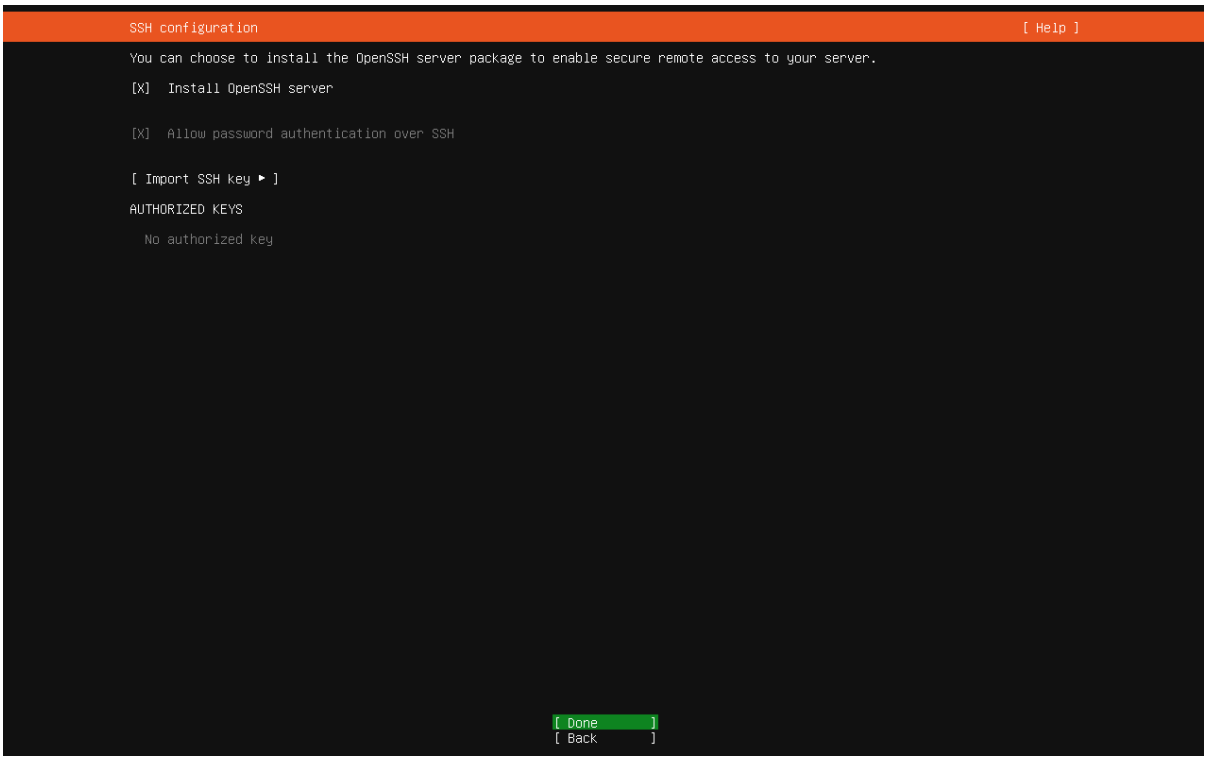
Selección de software. Se selecciona Ubuntu Server.



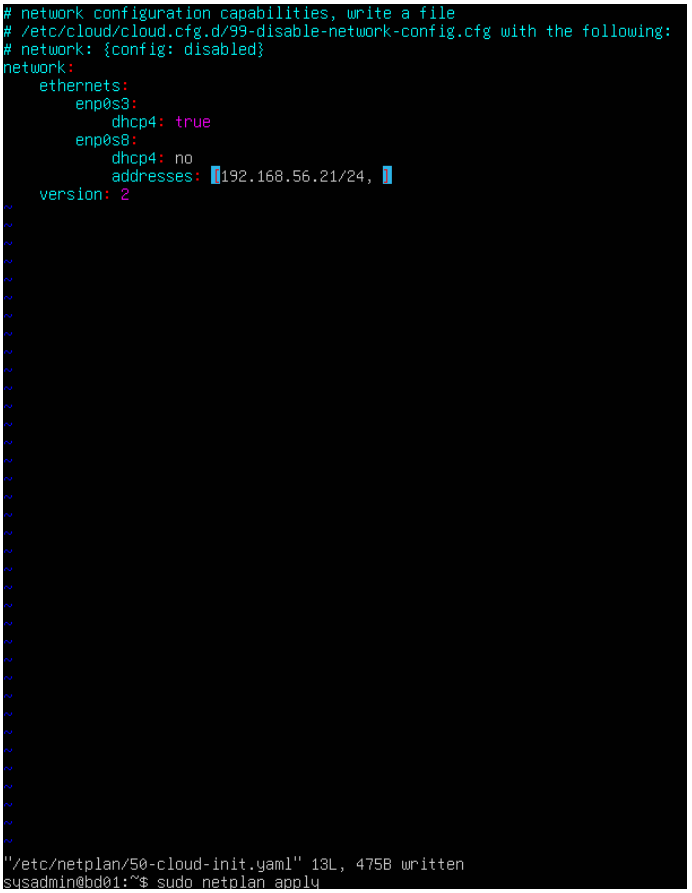
Configuración de usuario con permisos de administrador.



Instalación OpenSSH Server.



Configuración de direccionamiento IP.



Preparación del entorno para Ansible

Se instala Ansible y complementos utilizando pipx:

- pip install pipx
- pipx ensurepath
- pipx install ansible-core
- pipx inject ansible-core argcomplete
- pipx inject ansible-core ansible-lint
- activate-global-python-argcomplete –user

Se ejecuta .bash_completion con nuestro usuario:

- source /home/sysadmin/.bash_completion

Se crean par de claves ssh para poder conectarnos desde nuestro controlador de Ansible hacia los hosts:

- ssh-keygen

Se copia la clave pública en los hosts:

- ssh-copy-id 192.168.50.20
- ssh-copy-id 192.168.50.21

Se instala git y se clona el repositorio:

- sudo dnf install git
- git clone git@github.com:AforGaming/Obl-TallerLinux.git

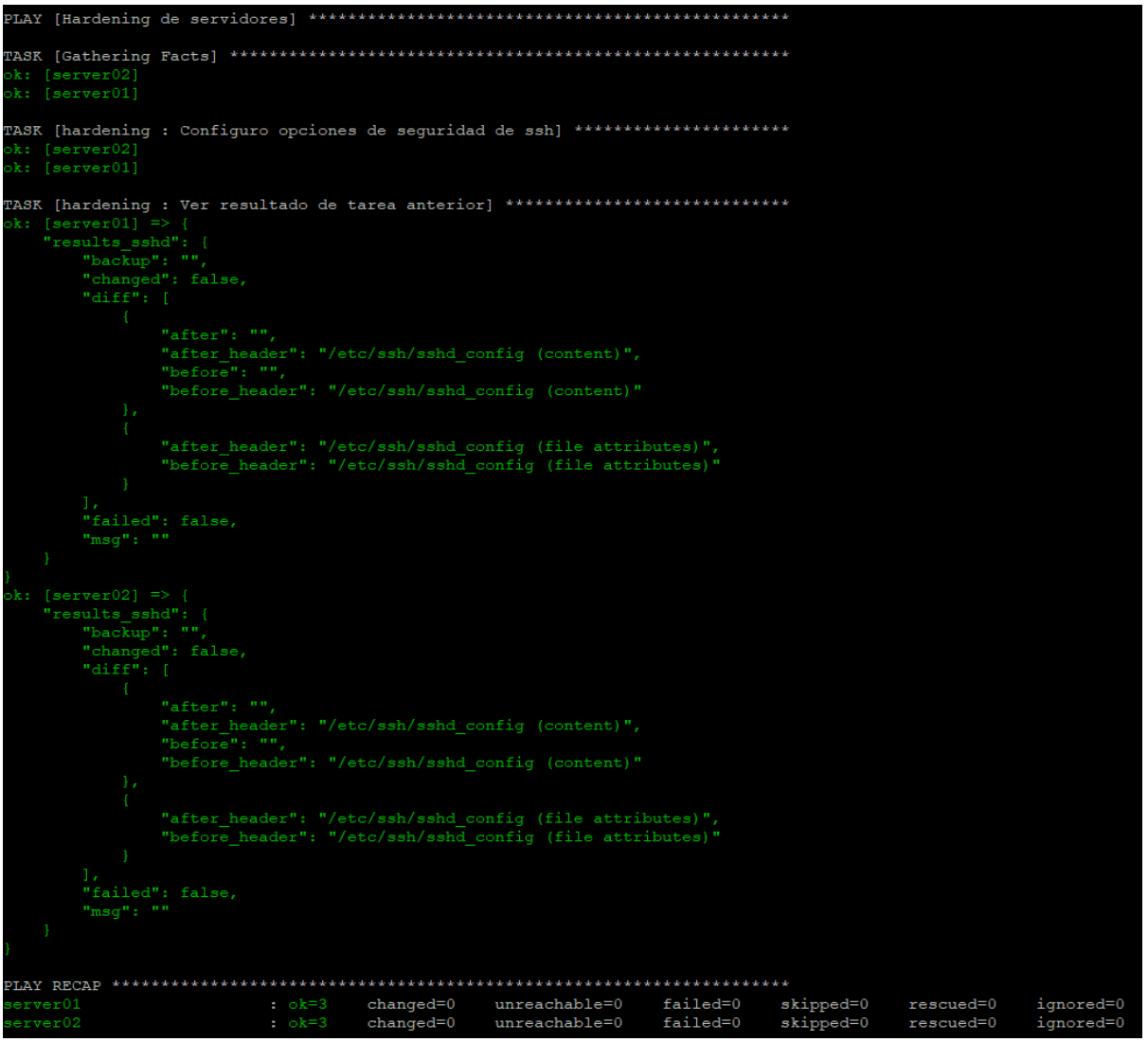
Se instalan los modulos necesarios:

- ansible-galaxy collection install -r collections/requirements.yml

Ejecución de los playbooks

Hardening de SSH.

- ansible-playbook hardening.yml -i inventory/servidores.yml --ask-become-pass



WebServer.

- ansible-playbook webserver.yml -i inventory/servidores.yml --ask-become-pass

```
PLAY [Instalacion de httpd] ***************************************************************************************************

TASK [Gathering Facts] ********************************************************************************************************
ok: [server01]

TASK [webserver : Instalar apache] ********************************************************************************************
ok: [server01] => (item=httpd)
ok: [server01] => (item=mod_ssl)

TASK [webserver : Configurar virtualhost] *************************************************************************************
changed: [server01]

TASK [webserver : Permito http y https] ***************************************************************************************
ok: [server01] => (item=http)
ok: [server01] => (item=https)

TASK [webserver : Apache levantado y habilitado] ******************************************************************************
ok: [server01]

RUNNING HANDLER [webserver : Reiniciar apache] ********************************************************************************
changed: [server01]

PLAY RECAP ********************************************************************************************************************
server01                   : ok=6    changed=2    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Database.

- ansible-playbook database.yml -i inventory/servidores.yml --ask-become-pass

```
PLAY [Instalacion de mariadb] *************************************************************************************************

TASK [Gathering Facts] ********************************************************************************************************
ok: [server02]

TASK [database : UFW instalado] ***********************************************************************************************
ok: [server02]

TASK [database : Permitir puerto 22 en ufw] ***********************************************************************************
ok: [server02]

TASK [database : Defino politicas de tráfico entrante] ************************************************************************
ok: [server02]

TASK [database : Defino politicas de tráfico entrante] ************************************************************************
ok: [server02]

TASK [database : servicio UFW levantado y activo] *****************************************************************************
ok: [server02]

TASK [database : MariaDB instalado] *******************************************************************************************
ok: [server02] => (item=mariadb-server)
ok: [server02] => (item=mariadb-client)
ok: [server02] => (item=python3-pymysql)

TASK [database : Cambiar la configuracion para escuchar en todas las interfaces] **********************************************
ok: [server02]

TASK [database : Ejecuto el handler si cambió la configuración] ***************************************************************

TASK [database : Servidor Mariadb levantado] **********************************************************************************
ok: [server02]

TASK [database : Habilitamos en ufw la conexión a mariadb] ********************************************************************
ok: [server02]

TASK [database : Copio el dump de la base de datos] ***************************************************************************
ok: [server02]
```

```
TASK [database : Cambiar password de root] *************************************************************************************************************************
[WARNING]: Option column_case_sensitive is not provided. The default is now false, so the column's name will be uppercased. The default will be changed to true in community.mysql
4.0.0.
ok: [server02]

TASK [database : Cambiar password de root IPV6 localhost (::1)] ****************************************************************************************************
ok: [server02]

TASK [database : Cambiar password de root IPV4 localhost (127.0.0.1)] **********************************************************************************************
ok: [server02]

TASK [database : Cambiar password de root localhost domain] ********************************************************************************************************
ok: [server02]

TASK [database : Eliminar usuarios anonimos] ***********************************************************************************************************************
ok: [server02]

TASK [database : Eliminar la base de datos de prueba y su acceso] **************************************************************************************************
ok: [server02]

TASK [database : Verifico si la bd esta creada] ********************************************************************************************************************
ok: [server02]

TASK [database : Creo la base de datos todo] ***********************************************************************************************************************
skipping: [server02]

TASK [database : Crear usuario mysql para bd todo] *****************************************************************************************************************
ok: [server02]

PLAY RECAP *********************************************************************************************************************************************************
server02                   : ok=19   changed=0    unreachable=0    failed=0    skipped=1    rescued=0    ignored=0
```

Tomcat.

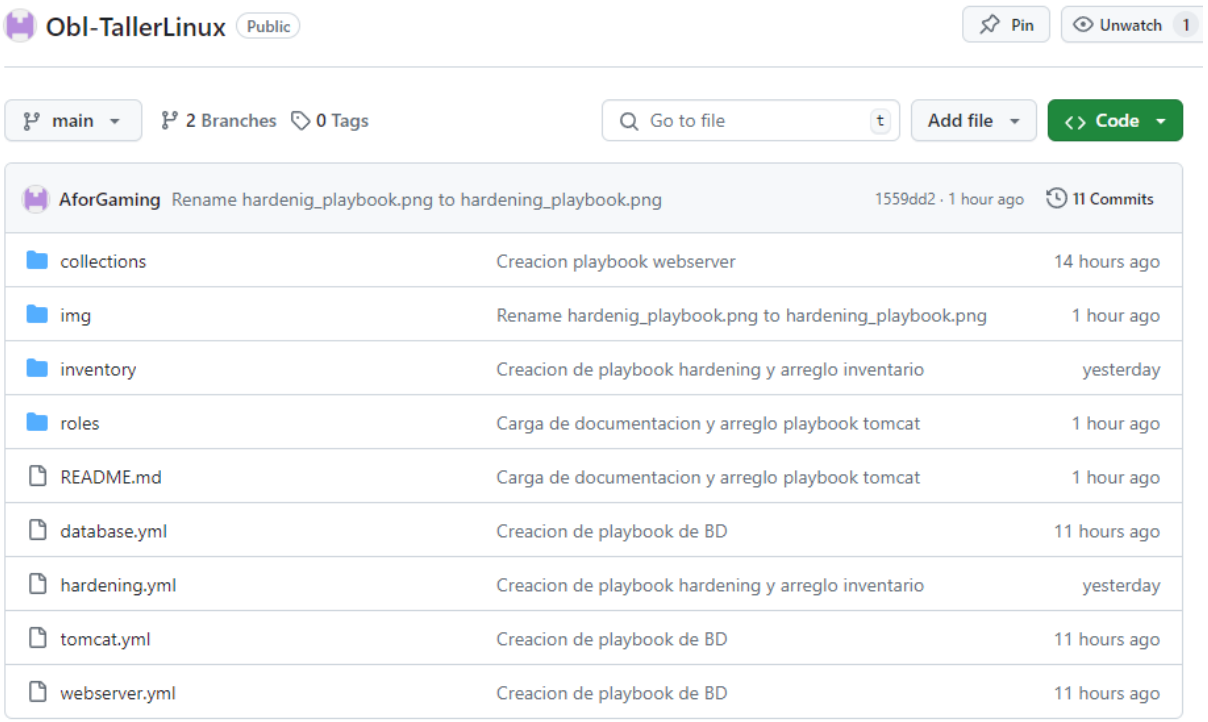
- ansible-playbook tomcat.yml -i inventory/servidores.yml --ask-become-pass

```
PLAY [Instalacion de tomcat] ***************************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************
ok: [server01]

TASK [tomcat : Instalar openjdk] ***********************************************************************************************************************************
ok: [server01]

TASK [tomcat : Instalar tar] ***************************************************************************************************************************************
ok: [server01]

TASK [tomcat : Instalar unzip] *************************************************************************************************************************************
ok: [server01]

TASK [tomcat : Configurar SELinux para que scripts y modulos HTTPD se conecten a la red] ***************************************************************************
changed: [server01]

TASK [tomcat : Crear directorio /opt/tomcat] ***********************************************************************************************************************
ok: [server01]

TASK [tomcat : Descargar Tomcat] ***********************************************************************************************************************************
ok: [server01]

TASK [tomcat : Extraer tar.gz] *************************************************************************************************************************************
changed: [server01]

TASK [tomcat : Crear usuario para servicio tomcat] *****************************************************************************************************************
ok: [server01]

TASK [tomcat : Crear directorio tomcat] ****************************************************************************************************************************
ok: [server01]

TASK [tomcat : Cambiar owner de carpeta tomcat] ********************************************************************************************************************
changed: [server01]
```

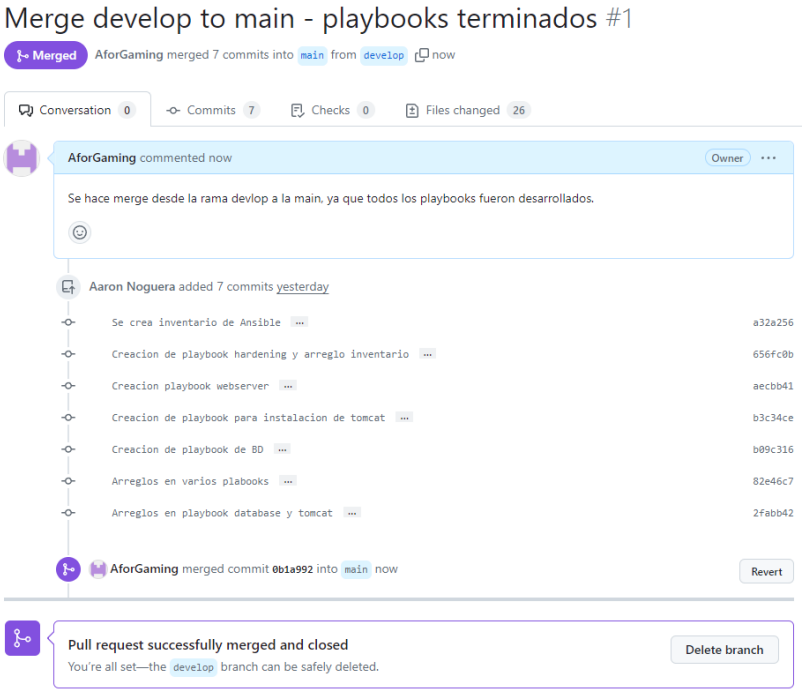
```
TASK [tomcat : Copiar archivos tomcat a /usr/local/tomcat] *********************************************************************************************************
changed: [server01]

TASK [tomcat : Crear servicio tomcat] ******************************************************************************************************************************
ok: [server01]

TASK [tomcat : Copiar app en carpeta tomcat] ***********************************************************************************************************************
ok: [server01]

TASK [tomcat : Extraer todo.war] ***********************************************************************************************************************************
changed: [server01]

TASK [tomcat : Cambiar owner de carpeta todo] **********************************************************************************************************************
changed: [server01]

TASK [tomcat : Cambiar owner de carpeta tomcat] ********************************************************************************************************************
changed: [server01]

TASK [tomcat : Sustituir app properties] ***************************************************************************************************************************
changed: [server01]

TASK [tomcat : Editar .bash_profile] *******************************************************************************************************************************
ok: [server01] => (item=JAVA_HOME=/usr/lib/jvm/jre-17)
ok: [server01] => (item=export JAVA_HOME)
ok: [server01] => (item=PATH=$PATH:$JAVA_HOME/bin)
ok: [server01] => (item=export PATH)

TASK [tomcat : Tomcat levantado y habilitado] **********************************************************************************************************************
ok: [server01]

RUNNING HANDLER [tomcat : Reiniciar tomcat] ************************************************************************************************************************
changed: [server01]

PLAY RECAP *********************************************************************************************************************************************************
server01                   : ok=21   changed=9    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Creación de los playbooks

Para alojar y trabajar en el código de los playbooks de manera eficiente se utilizó GitHub.
El código se encuentra alojado en el siguiente repositorio:
https://github.com/AforGaming/Obl-TallerLinux



Se creó una rama “develop”, para hacer commit de todos los cambios sobre ella. Luego se realizó un pull-request para luego hacer un merge hacia la rama “main”.



Todos los commit tienen su asunto y comentarios correspondientes, los cuales describen la funcionalidad agregada.

En el repositorio se encuentran 4 playbooks:

- **hardening**: Realiza configuración básica de seguridad sobre el servicio ssh para todos los hosts del inventario de Ansible.
- **webserver**: Instala el servicio httpd y mod_ssl y los configura, agregando un virtualhost y permitiendo los servicios http y https en el firewall.
- **database**: Instala el servicio de mariadb-server, realiza el secure installation y crea la base de datos y el usuario para la aplicación. El playbook verifica que la base de datos no esta creada antes de ejecutar la tarea de creación.
- **tomcat**: Instala y configura jdk y java, para luego desplegar la aplicación “todo”.

Estructura de playbooks

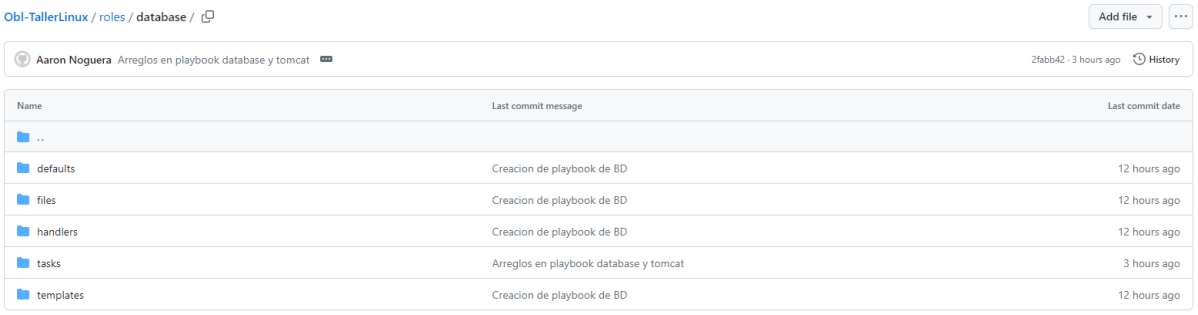
Cada playbook cuenta con un archivo main, el cual es el inicializador, donde se especifica nombre del mismo, hosts donde se ejecutará, usuario con el que lo hará en el host, si se permite ejecutar como sudo y el rol que utilizará.

Ejemplo:

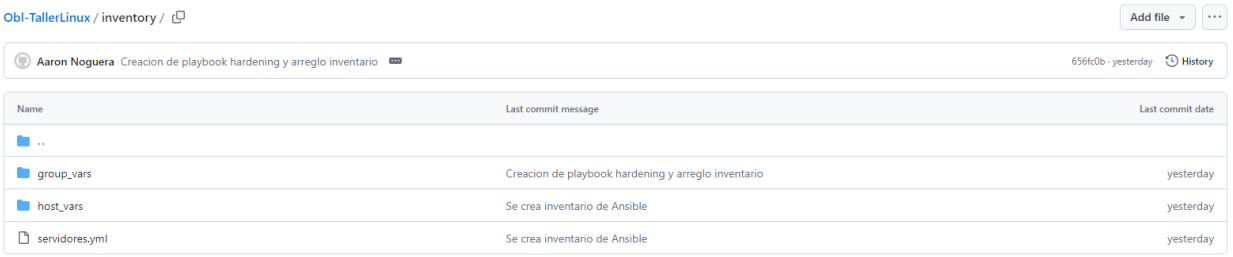
En la carpeta roles, se encuentra la carpeta específica del playbook, la cual contiene 3 directorios más:

- **tasks**: Contiene los archivos yml con las tareas definidas.
- **handlers**: Contiene el archivo yml con tareas de handlers definidas.
- **files**: Contiene archivos utilizados por el playbook.
- **templates**: Contiene archivos personalizados para el playbook.
- **defaults**: Contiene la definición y valores de las variables.

Ejemplo:

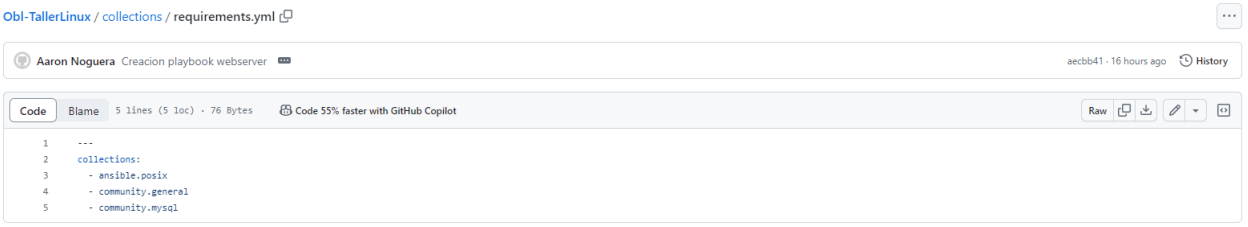


Inventario

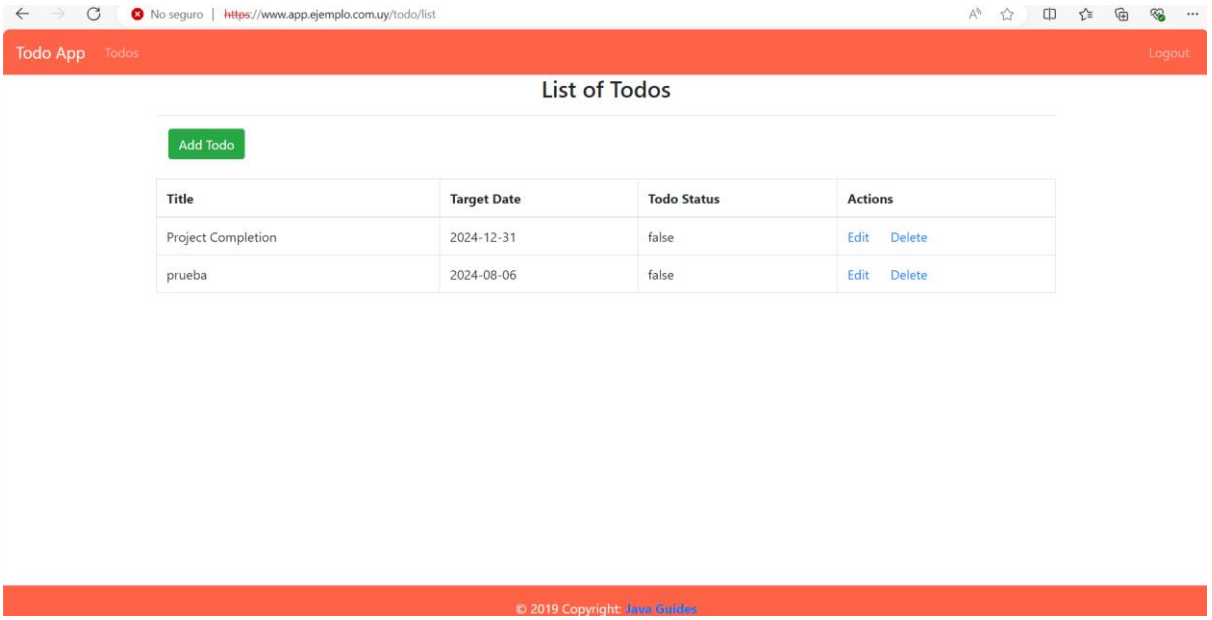


Módulos

- ansible.posix
- community.general
- community.mysql



Pruebas de funcionamiento de la aplicación



Bibliografía

- https://docs.ansible.com/
- https://stackoverflow.com/questions/27606119/make-ansible-check-if-database-is-present-on-a-remote-host
- https://stackoverflow.com/questions/25136498/ansible-answers-to-mysql-secure-installation