

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
Ejecución de los playbooks.....	14
Creación de los playbooks.....	18
Bibliografía	21

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

Instalación de Ansible Controller

Se configura LVM.

MANUAL PARTITIONING ROCKY LINUX 9.4 INSTALLATION

Done es Help!

▼ New Rocky Linux 9.4 Installation

DATA

- /home 3 GiB
- rt-home

SYSTEM

- / 7 GiB
- rt-root
- /var 3 GiB
- rt-var
- /boot 1024 MiB
- sda1
- swap 4 GiB
- rt-swap

+ - ↺

AVAILABLE SPACE: 1.99 GiB TOTAL SPACE: 20 GiB

1 storage device selected

rt-root

Mount Point: /

Desired Capacity: 7 GiB

Device(s): ATA VBOX HARDISK (sda)

Modify...

Device Type: LVM ☐ Encrypt

File System: xfs ☒ Reformat

Volume Group: rt (4 MiB free)

Modify...

Label:

Name: root

Update Settings

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

Discard All Changes

Configuración de red.

NETWORK & HOST NAME ROCKY LINUX 9.4 INSTALLATION

Done es Help!

Ethernet (enp0s3)
Intel Corporation 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)

Ethernet (enp0s8)
Intel Corporation 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)

Ethernet (enp0s3) Connected

Hardware Address 08:00:27:24:29:A2

Speed 1000 Mb/s

IP Address 10.0.2.15/24

Default Route 10.0.2.2

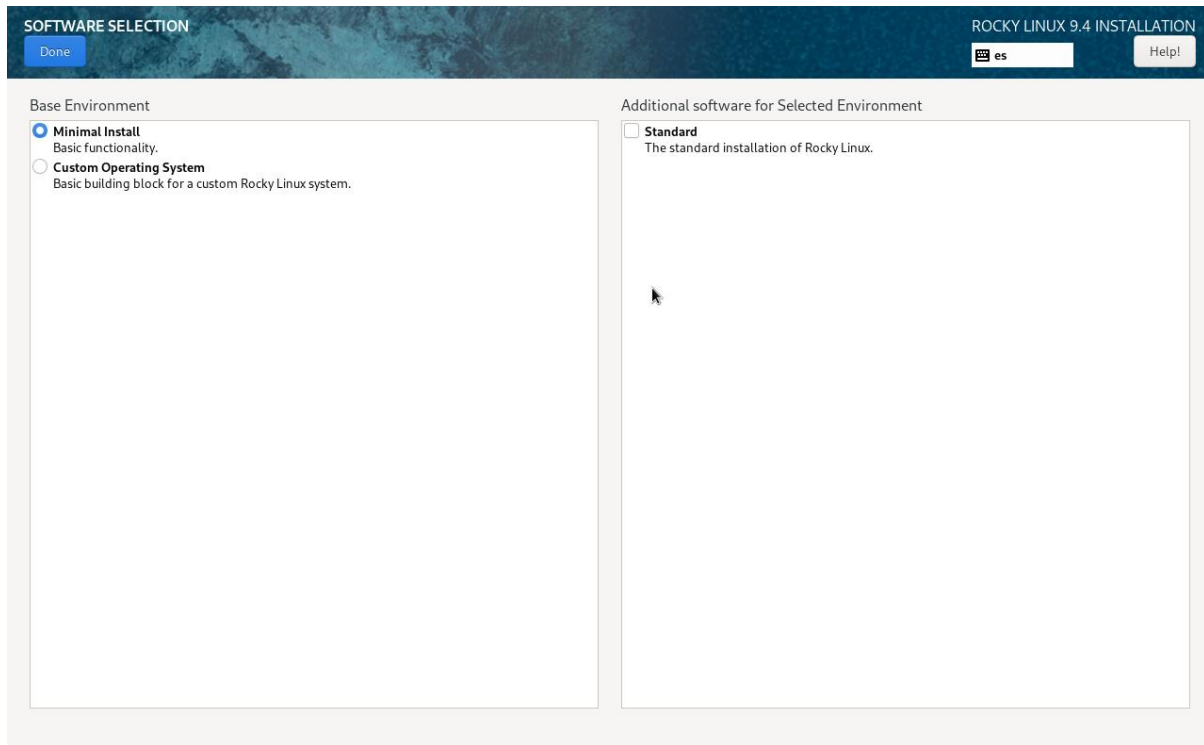
DNS 192.168.1.1

Configure...

Host Name: controller.ejemplo.com.uy Apply

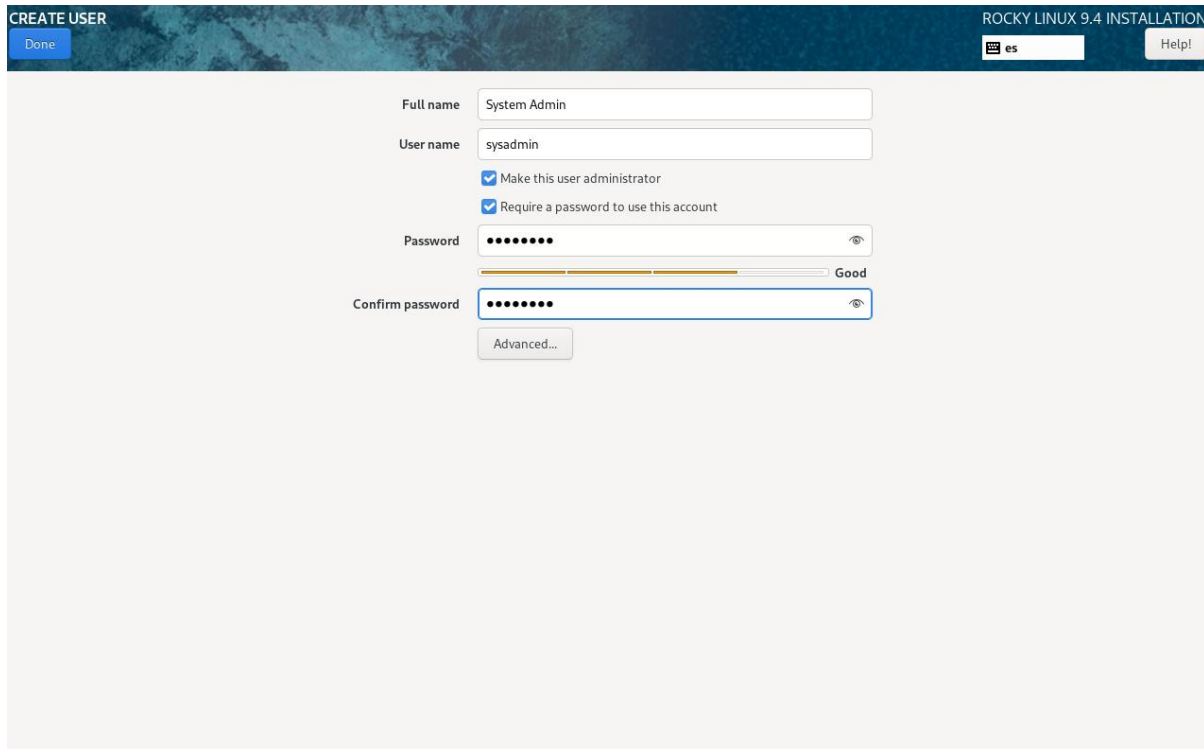
Current host name: controller.ejemplo.com.uy

Selección de software. Se selecciona minimal install.



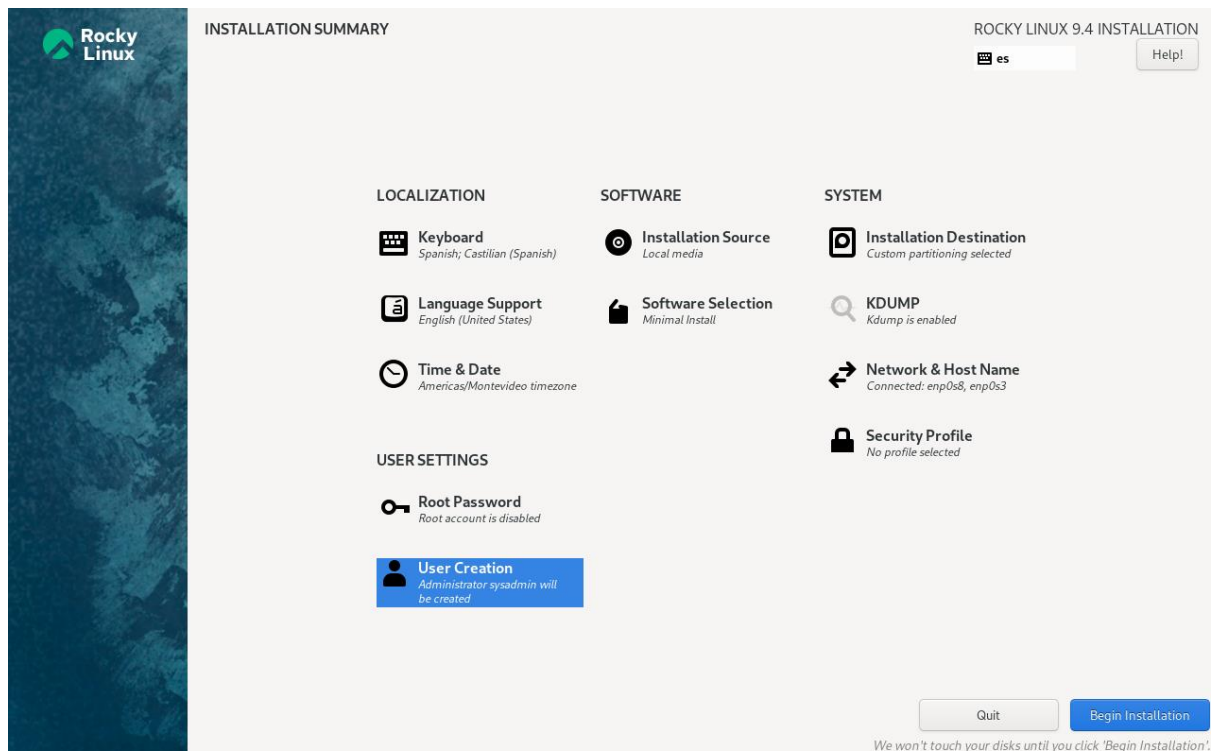
The screenshot shows the 'SOFTWARE SELECTION' window of the Rocky Linux 9.4 installer. The window has a dark blue header with the title 'SOFTWARE SELECTION' on the left and 'ROCKY LINUX 9.4 INSTALLATION' on the right, including a language dropdown set to 'es' and a 'Help!' button. The main area is divided into two panels. The left panel, titled 'Base Environment', contains two radio button options: 'Minimal Install' (selected) with the description 'Basic functionality.', and 'Custom Operating System' with the description 'Basic building block for a custom Rocky Linux system.'. The right panel, titled 'Additional software for Selected Environment', contains one checkbox option: 'Standard' (unchecked) with the description 'The standard installation of Rocky Linux.'.

Configuración de usuario con permisos de administrador.



The screenshot shows the 'CREATE USER' window of the Rocky Linux 9.4 installer. The window has a dark blue header with the title 'CREATE USER' on the left and 'ROCKY LINUX 9.4 INSTALLATION' on the right, including a language dropdown set to 'es' and a 'Help!' button. The main area contains a form for creating a user. It includes input fields for 'Full name' (containing 'System Admin') and 'User name' (containing 'sysadmin'). Below these are two checked checkboxes: 'Make this user administrator' and 'Require a password to use this account'. There are two password input fields, both masked with dots. The first password field has a strength indicator bar below it that is mostly orange and labeled 'Good'. To the right of each password field is an eye icon for toggling visibility. At the bottom of the form is an 'Advanced...' button.

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.

MANUAL PARTITIONING ROCKY LINUX 9.4 INSTALLATION

Done es Help!

▼ New Rocky Linux 9.4 Installation

SYSTEM

/	7 GiB
rl-root	
/var	2.99 GiB
rl-var	
/boot	1024 MiB
sda1	
swap	2 GiB
rl-swap	

+ - ↺

AVAILABLE SPACE: 1023 KiB TOTAL SPACE: 13 GiB

1 storage device selected

rl-root

Mount Point: /

Desired Capacity: 7 GiB

Device Type: LVM ☐ Encrypt

File System: xfs ☒ Reformat

Device(s): ATA VBOX HARDDISK (sda) Modify...

Volume Group: rl (4 MiB free) Modify...

Label:

Name: root

Update Settings

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

Discard All Changes

Configuración de red en la instalación.

NETWORK & HOST NAME ROCKY LINUX 9.4 INSTALLATION

Done es Help!

Ethernet (enp0s3)
Intel Corporation 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)

Ethernet (enp0s8)
Intel Corporation 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)

Ethernet (enp0s3)
Connected

Hardware Address 08:00:27:BE:42:46

Speed 1000 Mb/s

IP Address 10.0.2.15/24

Default Route 10.0.2.2

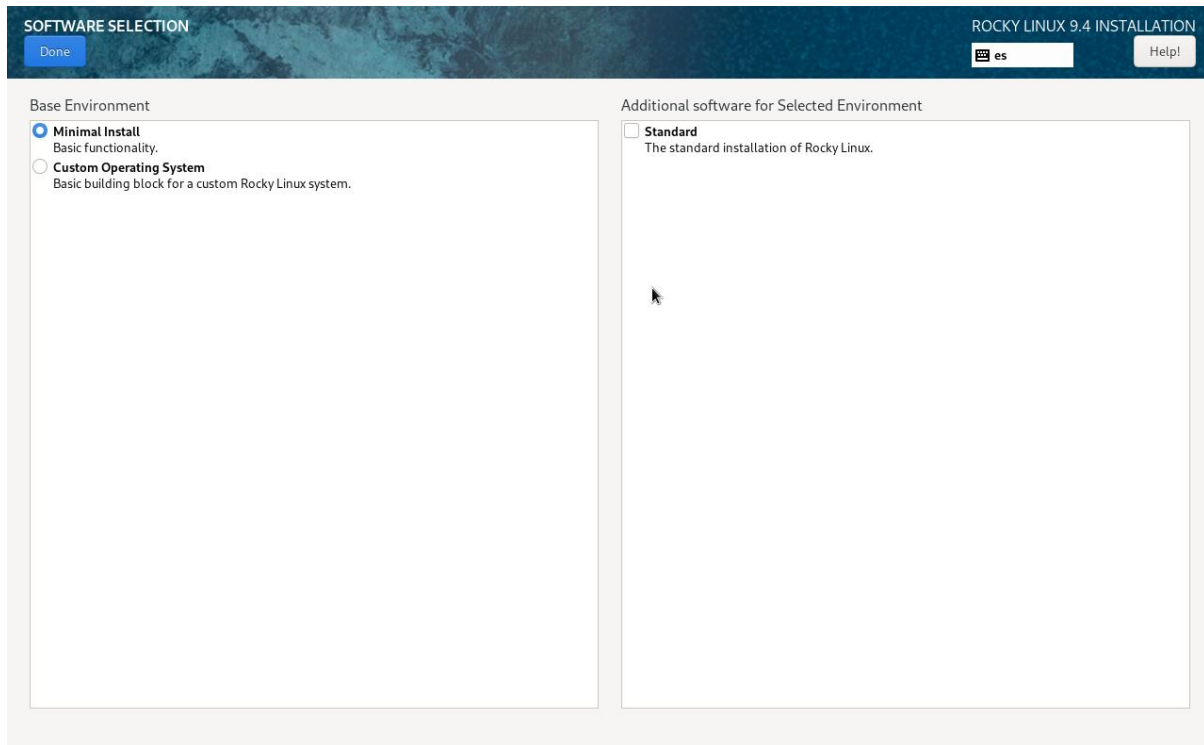
DNS 200.40.30.245
8.8.8.8

Configure...

Host Name: app01.ejemplo.com.uy Apply

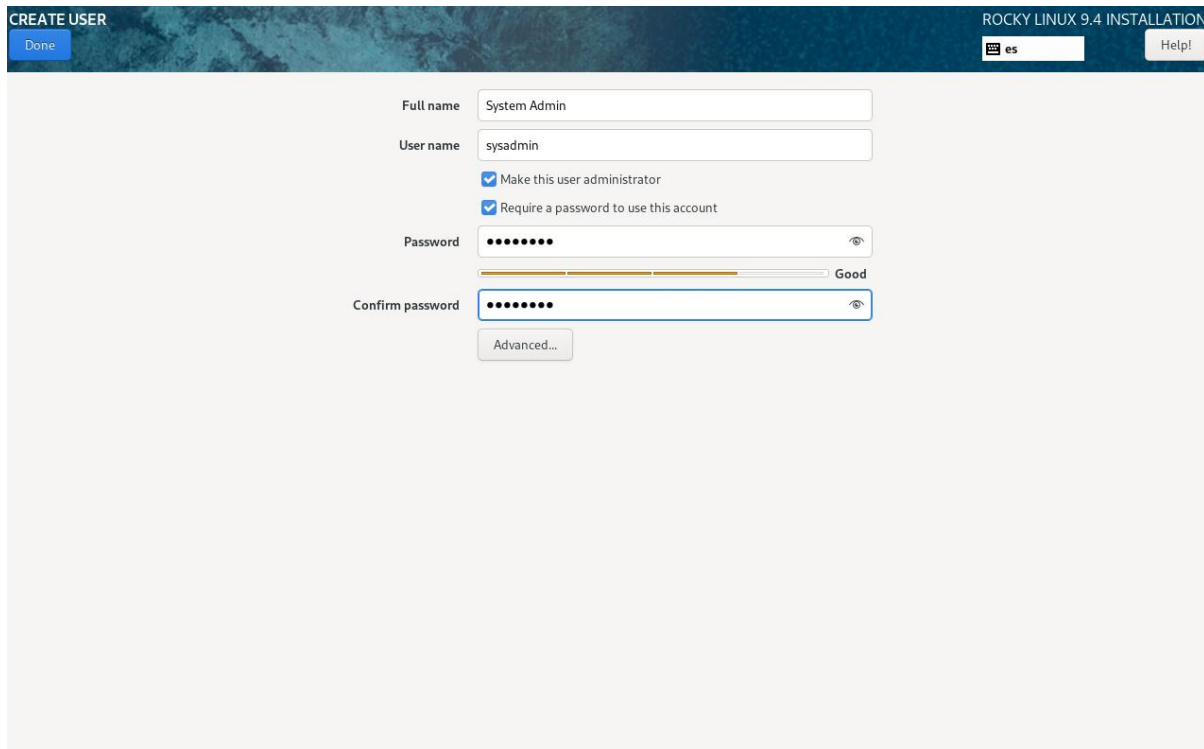
Current host name: app01.ejemplo.com.uy

Selección de software. Se selecciona minimal install.



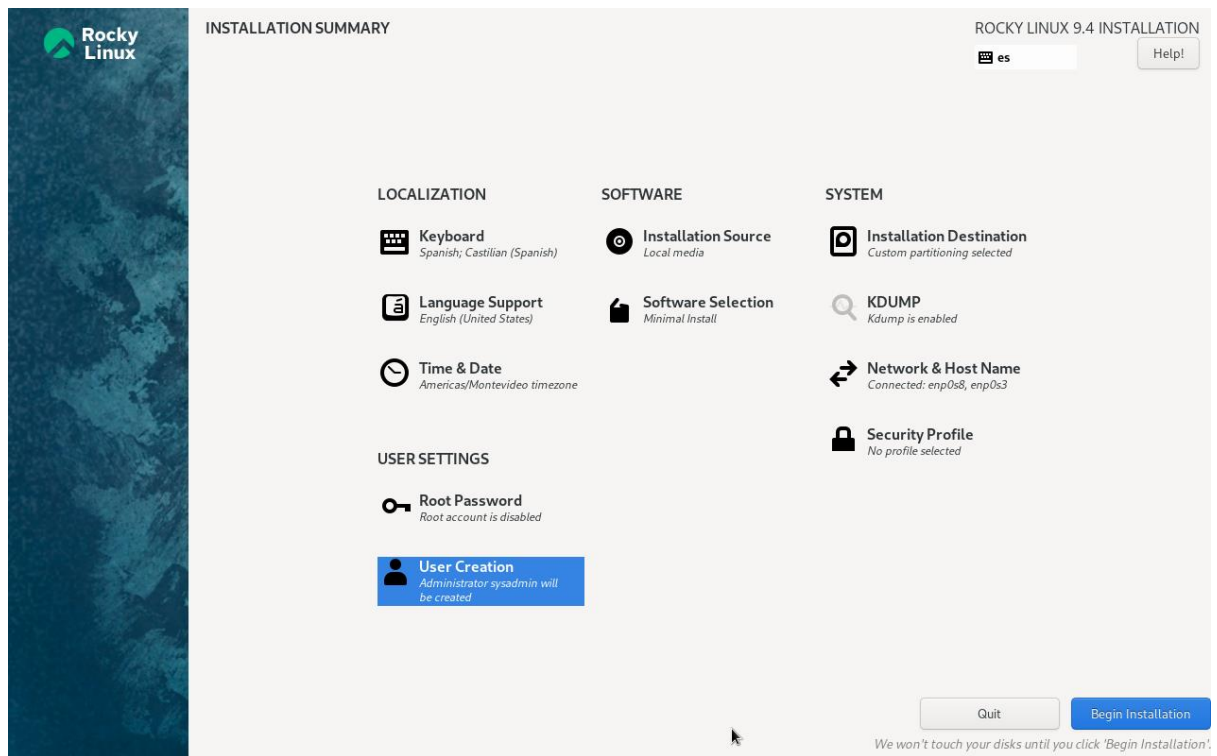
The screenshot shows the 'SOFTWARE SELECTION' window of the Rocky Linux 9.4 installer. The window has a dark blue header with the title 'SOFTWARE SELECTION' on the left and 'ROCKY LINUX 9.4 INSTALLATION' on the right, along with a 'Done' button and a 'Help!' button. The main area is divided into two panels. The left panel, titled 'Base Environment', contains two radio button options: 'Minimal Install' (selected) and 'Custom Operating System'. The right panel, titled 'Additional software for Selected Environment', contains a single checkbox option: 'Standard'. The 'Minimal Install' option is described as 'Basic functionality.' and the 'Custom Operating System' as 'Basic building block for a custom Rocky Linux system.' The 'Standard' option is described as 'The standard installation of Rocky Linux.'

Configuración de usuario con permisos de administrador.



The screenshot shows the 'CREATE USER' window of the Rocky Linux 9.4 installer. The window has a dark blue header with the title 'CREATE USER' on the left and 'ROCKY LINUX 9.4 INSTALLATION' on the right, along with a 'Done' button and a 'Help!' button. The main area is a light gray form with the following fields and options: 'Full name' (text input with 'System Admin'), 'User name' (text input with 'sysadmin'), 'Make this user administrator' (checked checkbox), 'Require a password to use this account' (checked checkbox), 'Password' (password input with a strength indicator showing 'Good'), and 'Confirm password' (password input). There is also an 'Advanced...' button at the bottom.

Resumen de instalación.

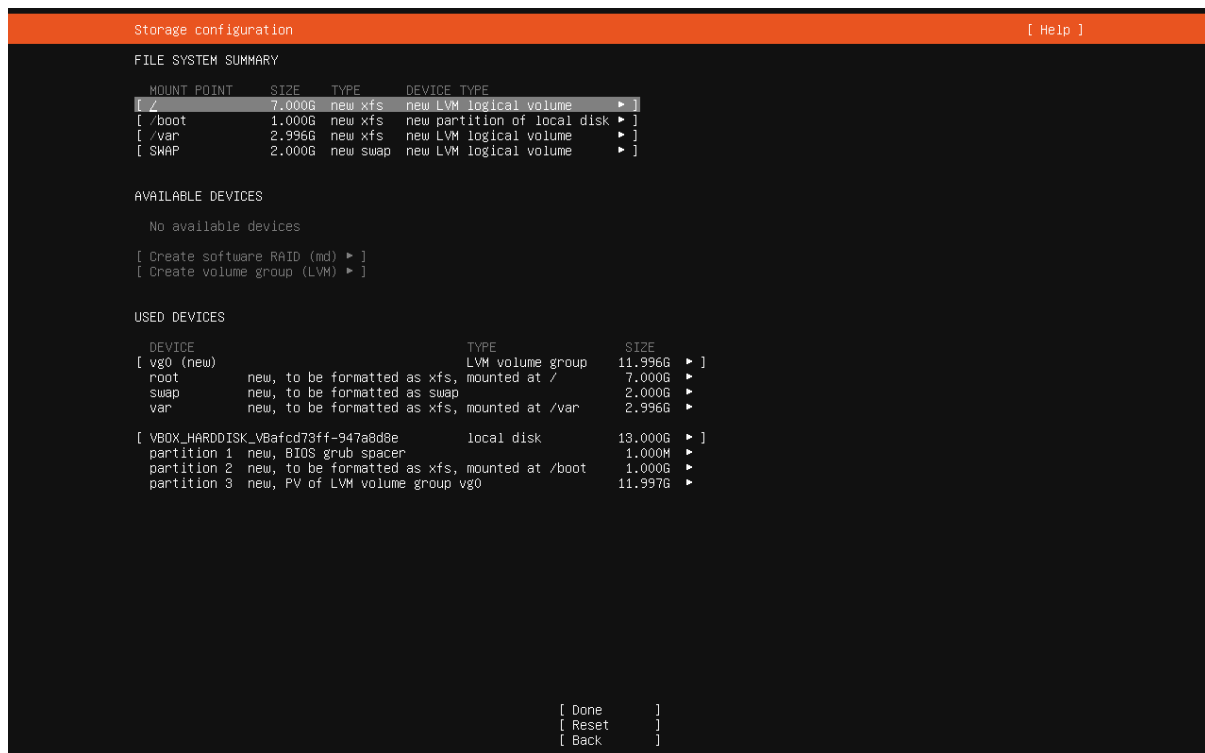


Comandos ejecutados para configurar el direccionamiento IP:

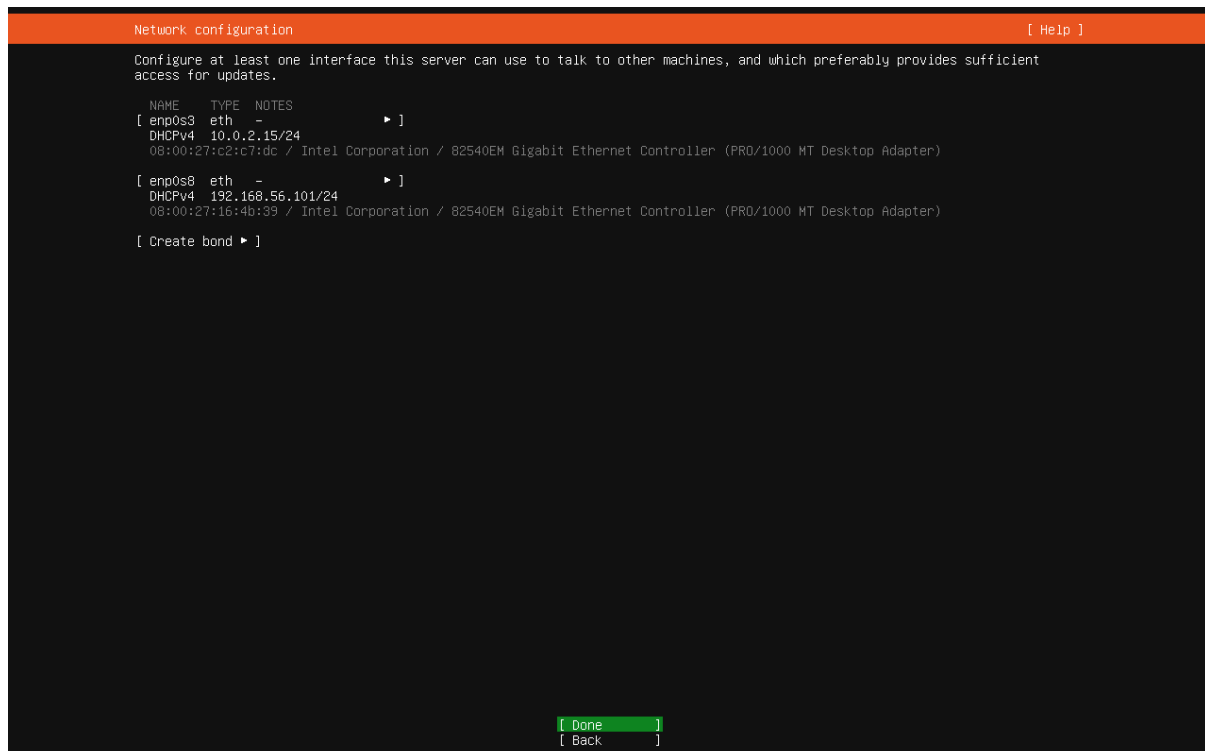
- `sudo nmcli con mod enp0s8 ipv4.addresses 192.168.56.20/24`
- `sudo nmcli con mod enp0s8 ipv4.method manual`
- `sudo nmcli con up enp0s8`

Instalación BD Server

Configuración de LVM.



Configuración de red en instalación.



Selección de software. Se selecciona Ubuntu Server.

Choose the type of installation [Help]

Choose the base for the installation.

(X) Ubuntu Server

The default install contains a curated set of packages that provide a comfortable experience for operating your server.

() Ubuntu Server (minimized)

This version has been customized to have a small runtime footprint in environments where humans are not expected to log in.

Additional options

[] Search for third-party drivers

This software is subject to license terms included with its documentation. Some is proprietary. Third-party drivers should not be installed on systems that will be used for FIPS or the real-time kernel.

[Done]
[Back]

Configuración de usuario con permisos de administrador.

Profile configuration [Help]

Enter the username and password you will use to log in to the system. You can configure SSH access on a later screen, but a password is still needed for sudo.

Your name: System Admin

Your servers name: sd01
The name it uses when it talks to other computers.

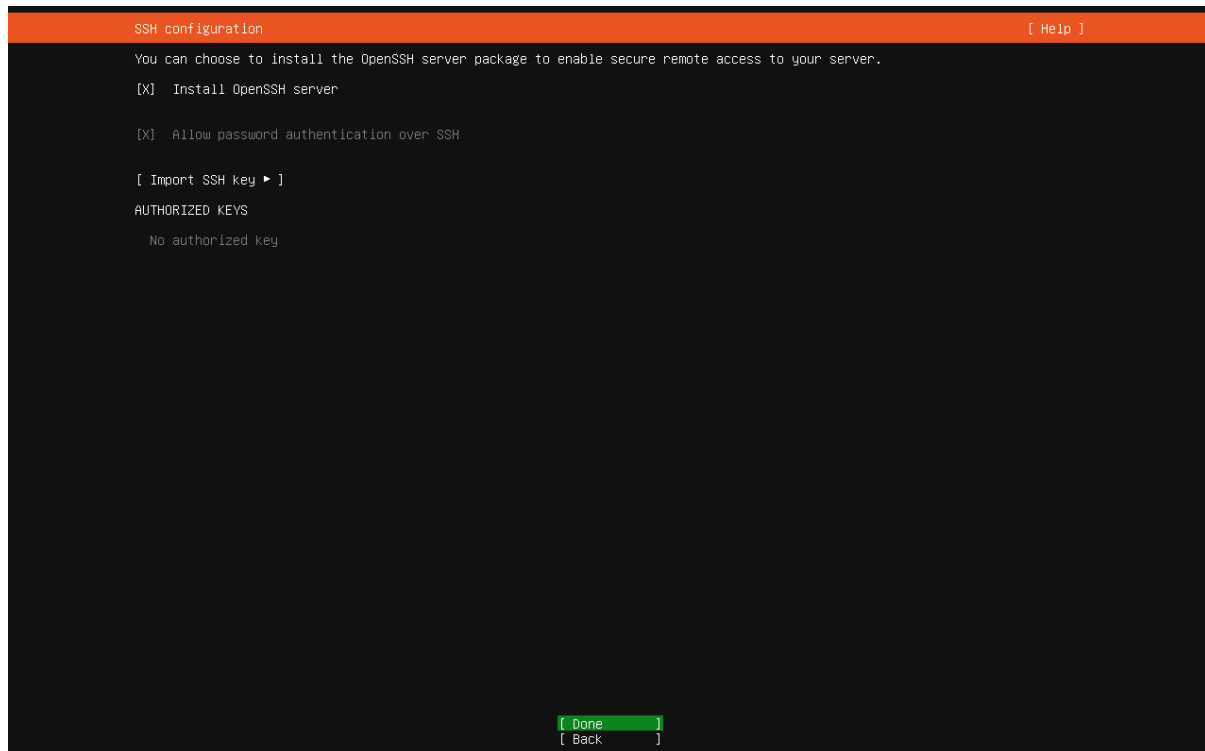
Pick a username: sysadmin

Choose a password: *****

Confirm your password: *****

[Done]

Instalación OpenSSH Server.



Configuración de direccionamiento IP.

[illegible]

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 publica 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](https://github.com/AforGaming/Obl-TallerLinux.git)
-

Se instalan los modulos necesesarios

- 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

```

PLAY [Hardening de servidores] *****

TASK [Gathering Facts] *****
ok: [server02]
ok: [server01]

TASK [hardening : Configuro opciones de seguridad de ssh] *****
ok: [server02]
ok: [server01]

TASK [hardening : Ver resultado de tarea anterior] *****
ok: [server01] => {
  "results_sshd": {
    "backup": "",
    "changed": false,
    "diff": [
      {
        "after": "",
        "after_header": "/etc/ssh/sshd_config (content)",
        "before": "",
        "before_header": "/etc/ssh/sshd_config (content)"
      },
      {
        "after_header": "/etc/ssh/sshd_config (file attributes)",
        "before_header": "/etc/ssh/sshd_config (file attributes)"
      }
    ],
    "failed": false,
    "msg": ""
  }
}
ok: [server02] => {
  "results_sshd": {
    "backup": "",
    "changed": false,
    "diff": [
      {
        "after": "",
        "after_header": "/etc/ssh/sshd_config (content)",
        "before": "",
        "before_header": "/etc/ssh/sshd_config (content)"
      },
      {
        "after_header": "/etc/ssh/sshd_config (file attributes)",
        "before_header": "/etc/ssh/sshd_config (file attributes)"
      }
    ],
    "failed": false,
    "msg": ""
  }
}

PLAY RECAP *****
server01      : ok=3    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
server02      : ok=3    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

```

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 : Permite 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>

The screenshot shows the GitHub repository page for 'Obl-TallerLinux' by 'AforGaming'. The repository is public and has 2 branches and 0 tags. The main branch is selected. The repository contains several files and folders:

File/Folder	Description	Last Commit
collections	Creacion playbook webserver	14 hours ago
img	Rename hardenig_playbook.png to hardening_playbook.png	1 hour ago
inventory	Creacion de playbook hardening y arreglo inventario	yesterday
roles	Carga de documentacion y arreglo playbook tomcat	1 hour ago
README.md	Carga de documentacion y arreglo playbook tomcat	1 hour ago
database.yml	Creacion de playbook de BD	11 hours ago
hardening.yml	Creacion de playbook hardening y arreglo inventario	yesterday
tomcat.yml	Creacion de playbook de BD	11 hours ago
webserver.yml	Creacion de playbook de BD	11 hours ago

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”.

Merge develop to main - playbooks terminados #1

The screenshot shows the GitHub pull request page for 'AforGaming' merged 7 commits into 'main' from 'develop'. The pull request is titled 'Merge develop to main - playbooks terminados #1'. The pull request was successfully merged and closed. The pull request description states: 'Se hace merge desde la rama develop a la main, ya que todos los playbooks fueron desarrollados.' The pull request was created by 'AforGaming' and merged by 'AforGaming'.

The commit history shows the following commits:

- Se crea inventario de Ansible (a32a256)
- Creacion de playbook hardening y arreglo inventario (656fc0b)
- Creacion playbook webserver (aecb41)
- Creacion de playbook para instalacion de tomcat (b3c34ce)
- Creacion de playbook de BD (b09c316)
- Arreglos en varios plabooks (82e46c7)
- Arreglos en playbook database y tomcat (2fab42)

The pull request was successfully merged and closed. The pull request description states: 'Se hace merge desde la rama develop a la main, ya que todos los playbooks fueron desarrollados.' The pull request was created by 'AforGaming' and merged by 'AforGaming'.

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:

[Obl-TallerLinux](#) / tomcat.yml



```
1 ---
2 - name: Instalacion de tomcat
3   hosts: app
4   become: true
5   user: sysadmin
6   roles:
7     - tomcat
```

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:

Obl-TallerLinux / roles / database /

Aaron Noguera

Arreglos en playbook database y tomcat

Zfab42 · 3 hours ago History

Inventario

Obl-TallerLinux / inventory /

Aaron Noguera

Creacion de playbook hardening y arreglo inventario

656fc0b · yesterday History

Módulos

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

Obl-TallerLinux / collections / requirements.yml

Aaron Noguera

Creacion playbook webserver

aecbb41 · 16 hours ago History

Code

Blame

5 líneas (5 loc) · 76 Bytes

Code 55% faster with GitHub Copilot

Raw

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>

