Instalación de Cockpit + Error Paquetes Actualizaciones

Los comandos que pondré llevaran sudo delante ya que yo los ejecuto con mi usuario.

En el caso de que en algún momento oportuno sea necesario utilizar la cuenta de root lo pondré.

Primero actualizaremos los paquetes del sistema.

'sudo apt update'

Si nos comenta que tenemos paquetes para actualizar, actualizamos.

'sudo apt upgrade -y'

Ahora procedemos a instalar Cockpit con el siguiente comando:

'sudo apt install cockpit'

Se verá así, nos pedirá confirmación:

```
yoda@vader:~$ sudo apt install cockpit
[sudo] password for yoda:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libevent-pthreads-2.1-7 libmcrypt4 libmecab2 libprotobuf-lite23 mecab-ipadic mecab-ipadic-utf8 mecab-utils
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  cockpit-bridge cockpit-networkmanager cockpit-packagekit cockpit-storaged cockpit-system cockpit-ws
  cracklib-runtime dconf-gsettings-backend dconf-service dnsmasq-base glib-networking glib-networking-common
  glib-networking-services gsettings-desktop-schemas libblockdev-mdraid2 libbluetooth3 libbytesize-common
  libbytesize1 libcrack2 libdconf1 libndp0 libnm0 libpcsclite1 libproxy1v5 libpwquality-common libpwquality-tools
  libpwquality1 libteamdct10 network-manager network-manager-pptp ppp pptp-linux session-migration wamerican
  wpasupplicant
Paquetes sugeridos:
  cockpit-doc cockpit-pcp cockpit-sosreport xdg-utils udisks2-lvm2 sssd-dbus pcscd avahi-autoipd libteam-utils
  wpagui libengine-pkcs11-openssl
Se instalarán los siguientes paquetes NUEVOS:
  cockpit cockpit-bridge cockpit-networkmanager cockpit-packagekit cockpit-storaged cockpit-system cockpit-ws
  cracklib-runtime dconf-gsettings-backend dconf-service dnsmasq-base glib-networking glib-networking-common
  glib-networking-services gsettings-desktop-schemas libblockdev-mdraid2 libbluetooth3 libbytesize-common
  libbytesize1 libcrack2 libdconf1 libndp0 libnm0 libpcsclite1 libproxy1v5 libpwquality-common libpwquality-tools
  libpwquality1 libteamdct10 network-manager network-manager-pptp ppp pptp-linux session-migration wamerican
  wpasupplicant
0 actualizados, 36 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 11,6 MB de archivos.
Se utilizarán 26,6 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
```

Ahora ya estará instalado y nos saldrá un mensaje que indicará que podemos acceder de dos formas, las dos por el puerto 9090:

Con el nombre del servidor, por ejemplo:

https://nombre-servidor:9090

Con la ip del servidor (recomiendo):

https://192.168.x.x o la ip que tengas en el servidor.

Si necesitas saber que ip tiene tu servidor puedes verlo de la siguiente manera.

'ip a'

Con este comando te saldrán todos los datos de las tarjetas.

Tenéis que buscar la línea que sale igual que la de justo abajo que enseño con otra forma.

Otra forma que yo hago para saber mi ip es con el siguiente comando:

'ip a | grep 192.168'

```
yoda@vader:~$ ip a | grep 192.168
    inet 192.168.1.4/24 brd 192.168.1.255 scope global enp7s0
    inet 192.168.1.2/24 brd 192.168.1.255 scope global ens6
yoda@vader:~$
```

De esta manera sacaremos todas las ips que tenemos, en la mayoría de casas tienen una red 192.168.1.0/24 o 192.168.0.0/24 por eso con el comando grep filtro con el comienzo del rango "192.168".

Ahora ya solo nos quedaría permitir en el firewall acceso al puerto 9090 por TCP.

Aunque recomiendo el uso de IPTABLES, en mi caso y para mayor entendimiento lo haremos con UFW.

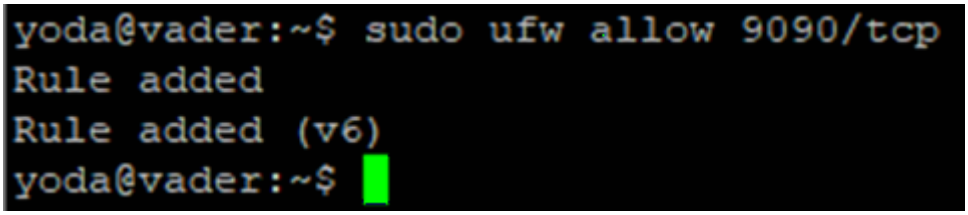
Primero de todo antes de activarlo le añadiremos la regla que permita usar SSH, por si estamos conectados ahora mismo.

'sudo ufw allow ssh'

Después ya podemos activarlo y permitir el puerto 9090 por TCP.

'sudo ufw enable'

'sudo ufw allow 9090/tcp'

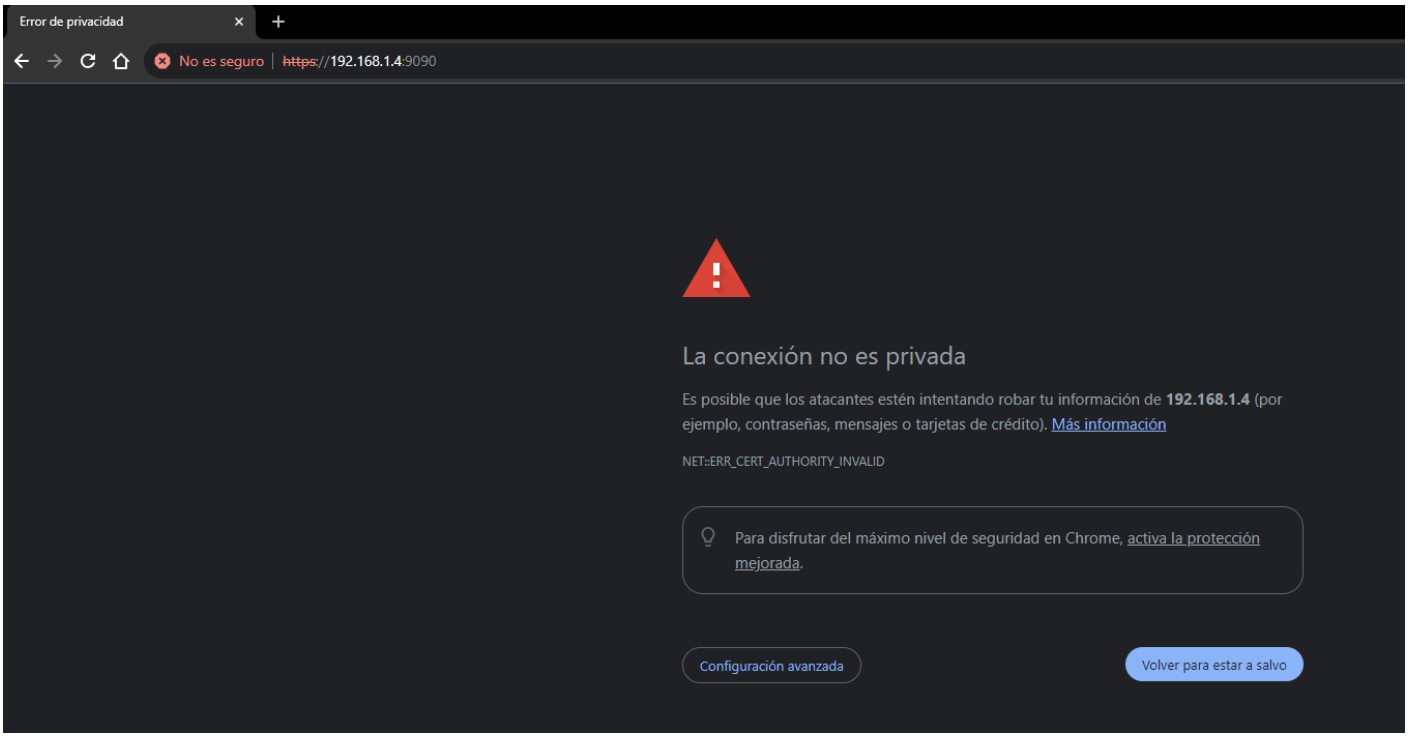


Podemos ver como esta el firewall con el siguiente comando.

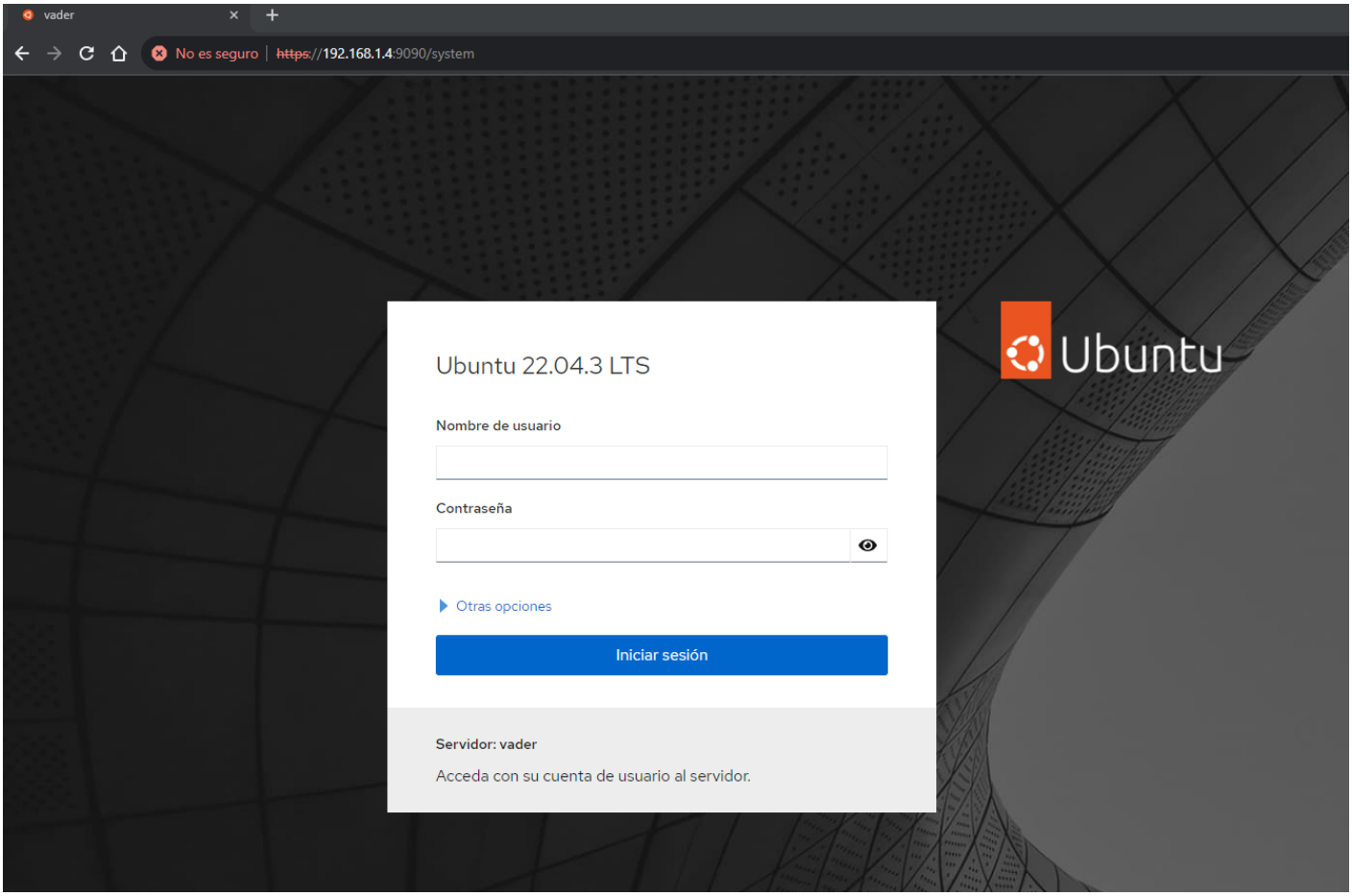
'sudo ufw status'

Y así comprobamos que este todo como lo hemos puesto.

Ahora si intentamos acceder a la página de las dos formas que he indicado antes verás que nos salta un aviso, simplemente le damos a "configuración avanzada" y a "acceder a 192.168.x.x".



Y ya estaríamos dentro.



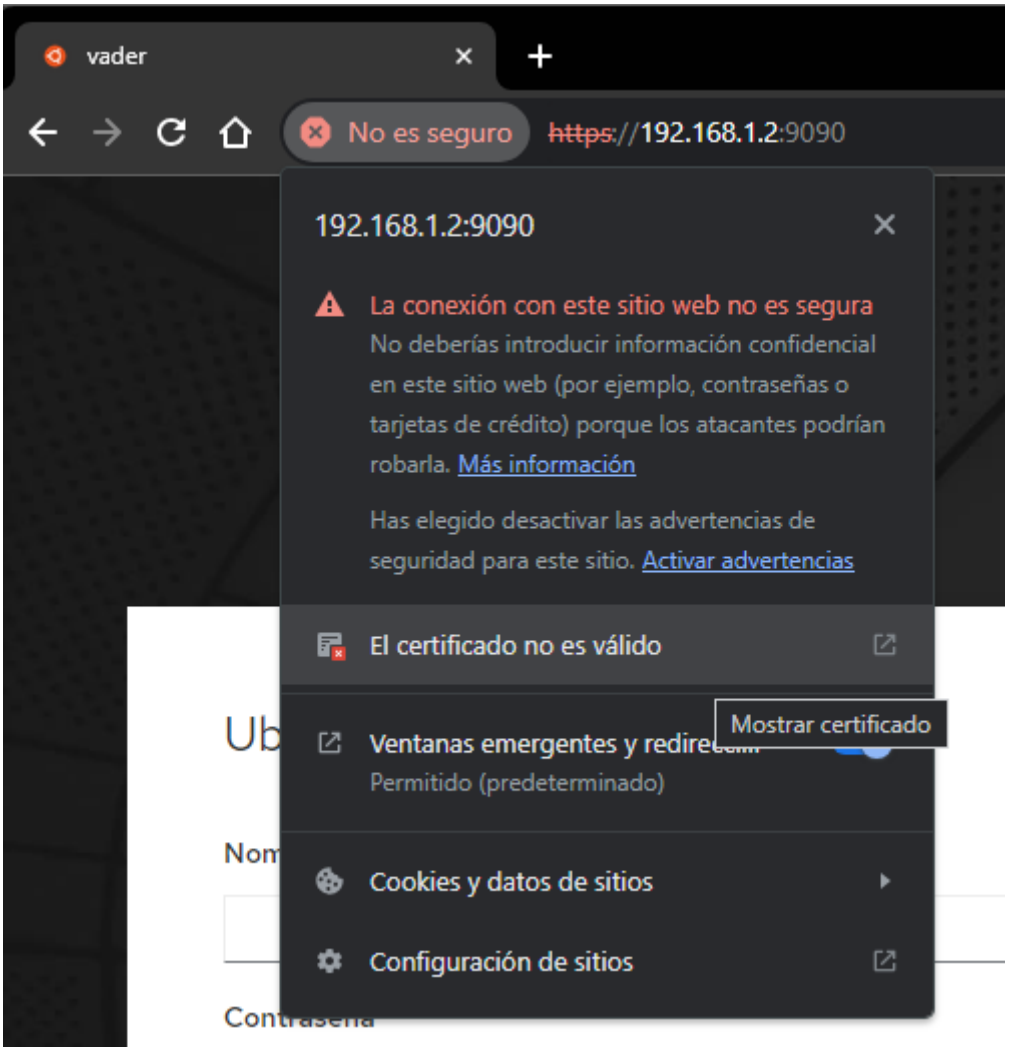
UNA COSA A TENER EN CUENTA ES EL CERTIFICADO PARA QUE TODO VAYA ENCRIPTADO, SI NO, SERÍA UN FALLO DE

SEGURIDAD MUY GRAVE.

ACTUALMENTE COCKPIT VIENE POR DEFECTO CON UN CERTIFICADO BÁSICO. LO PODÉIS AVERIGUAR DE DOS FORMAS.

UNA MEDIANTE EL NAVEGADOR Y LA OTRA CON UN COMANDO.

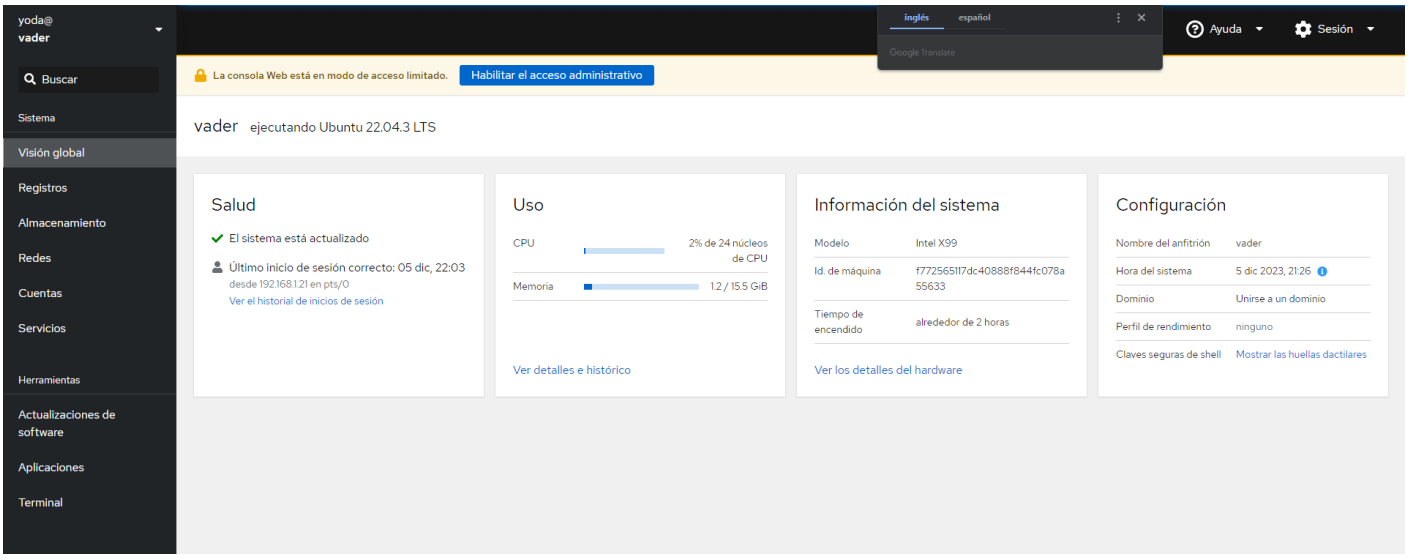
EN EL NAVEGADOR SIMPLEMENTE HAY QUE IR A "NO ES SEGURO" Y SI INDICA ALGO SOBRE UN CERTIFICADO COMO EL DE LA SIGUIENTE FOTO SIGNIFICA QUE LO TIENE ACTIVO.



Ahora accedemos con el usuario y contraseña que tengas en el servidor.

Veremos el panel pero sin tener acceso root. Simplemente le damos a habilitar el acceso administrativo.

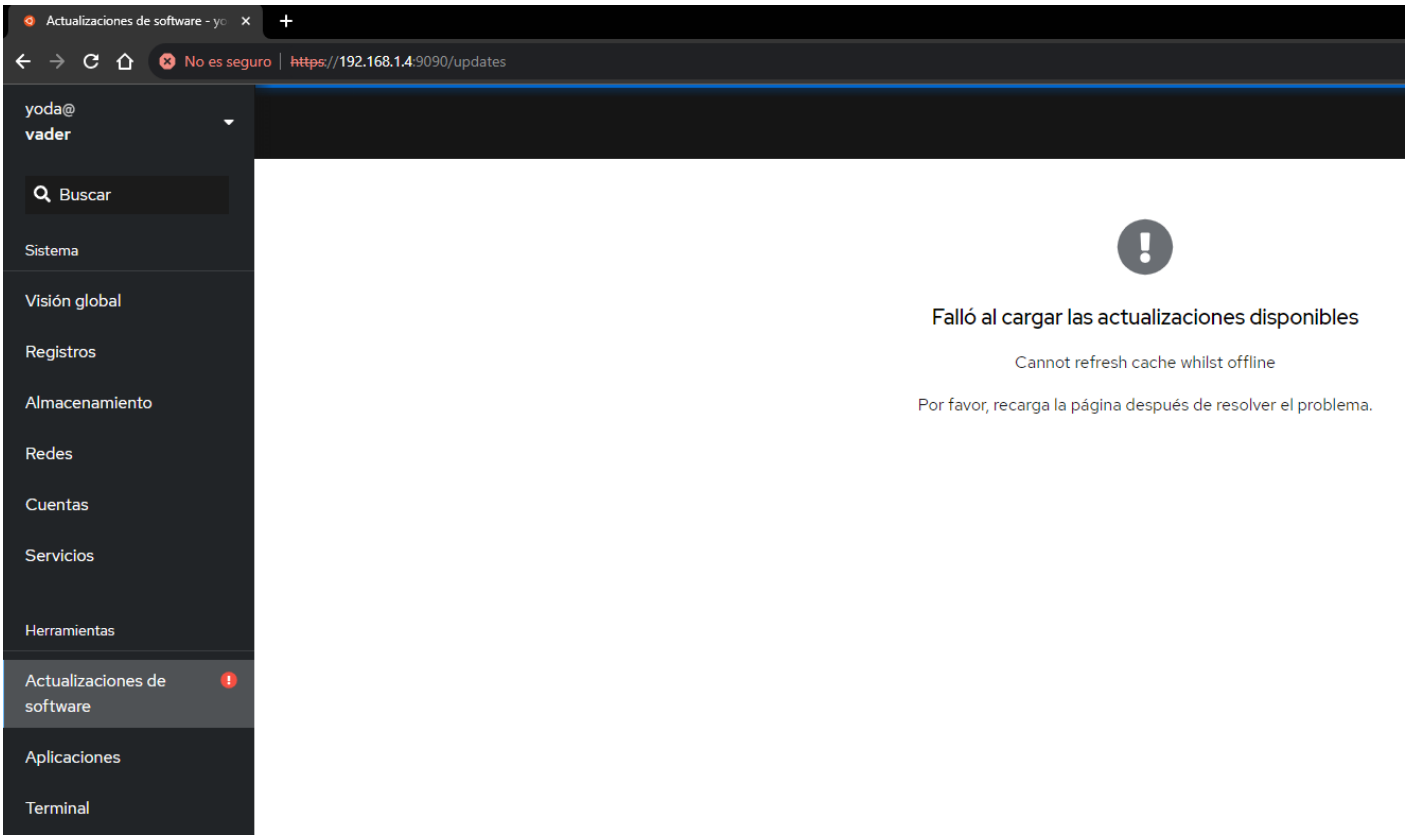
Nos pedirá la contraseña y si el usuario tiene permisos accederá perfectamente.



Una vez dentro podéis ver las tantas cosas que te deja hacer y ver por defecto. Se pueden instalar plugins para aumentar todavía más las posibilidades de esta interfaz.

EXISTE UN FALLO AL INSTALAR COCKPIT QUE SE ARREGLA MUY FÁCIL

Al ir a "Actualizaciones de software" verás que no funciona.



En el servidor tenemos que ir a "/etc/netplan/00-installer-config.yaml" y editarlo añadiendo debajo de network lo siguiente (recordar que en netplan no se puede tabular):

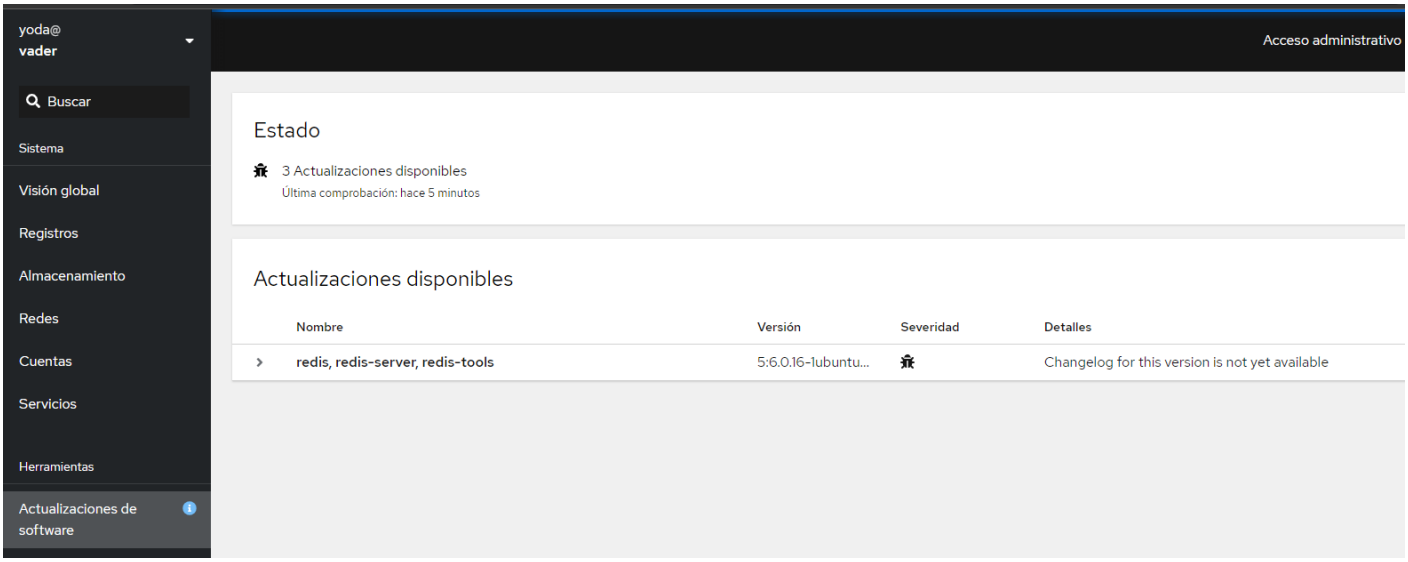
'renderer: NetworkManager'

```
  GNU nano 6.2                                /etc/netplan/00-installer-config.yaml
# This is the network config written by 'subiquity'
network:
  renderer: NetworkManager
  ethernets:
    enp7s0:
```

Realizamos el siguiente comando para confirmar el cambio.

'sudo netplan apply'

Si esta todo perfecto, volvemos a ir a actualizaciones y veremos como ya funciona correctamente.



Revision #4
Created 5 December 2023 21:43:33 by Yoda
Updated 6 December 2023 22:26:00 by Yoda