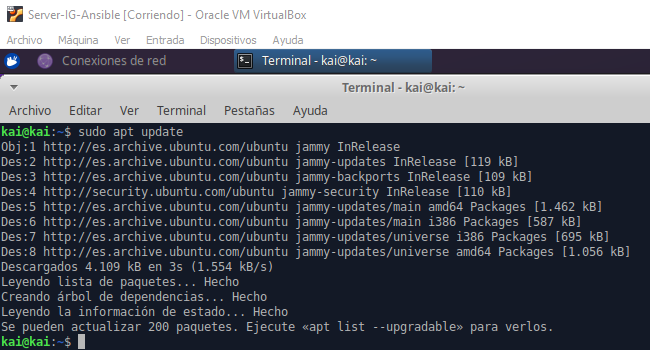
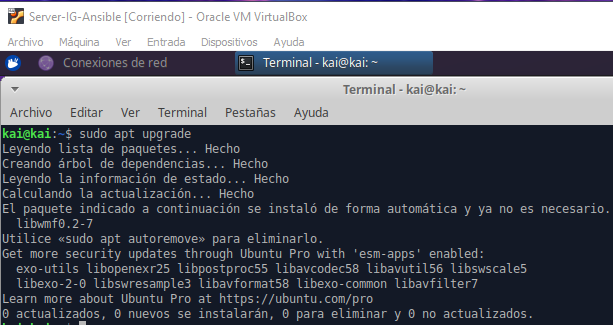


**PART 1**

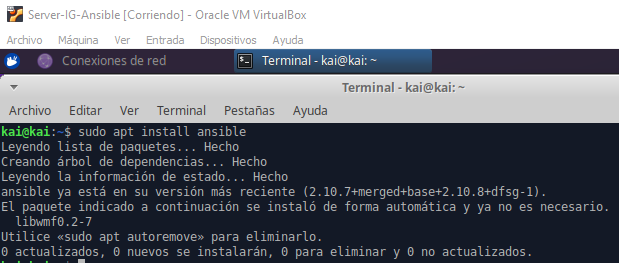
apt update



apt upgrade



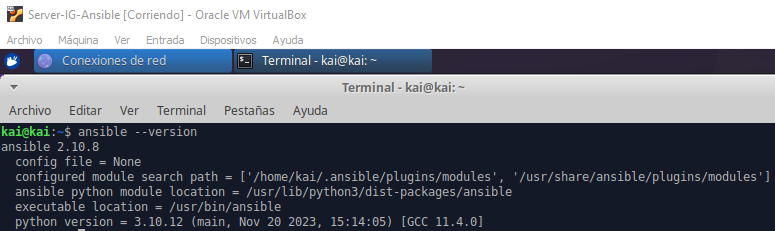
apt install ansible



Comprovarem que la instal·lació ha anat be i, a continuació, utilitzarem la comanda «pip» per instal·lar la versió mes actual.

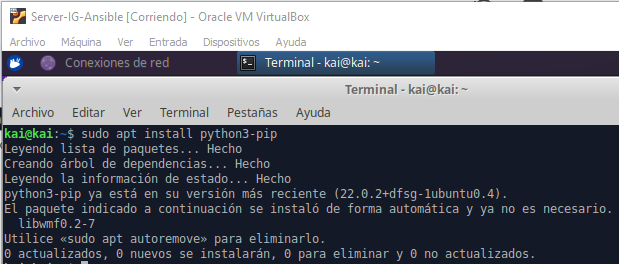
Abans de fer la següent comanda, fes una captura de la versió d’Ansible.

Per fer-ho utilitzarem la comanda “ansible –version”.

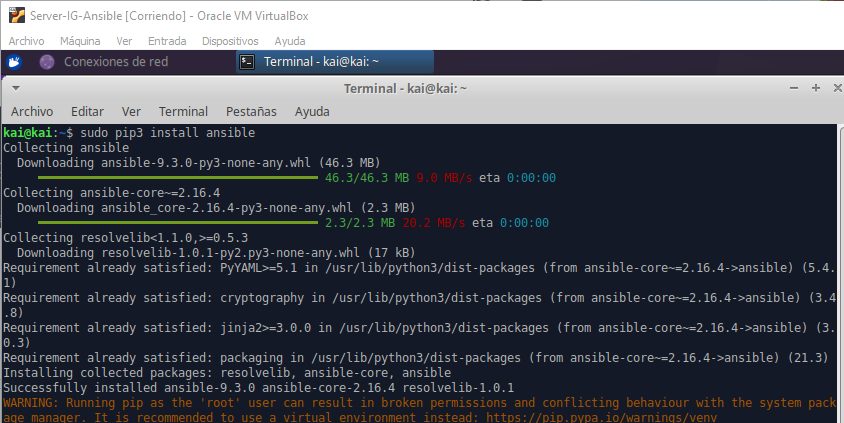


Instalem la versió més nova de ansible.

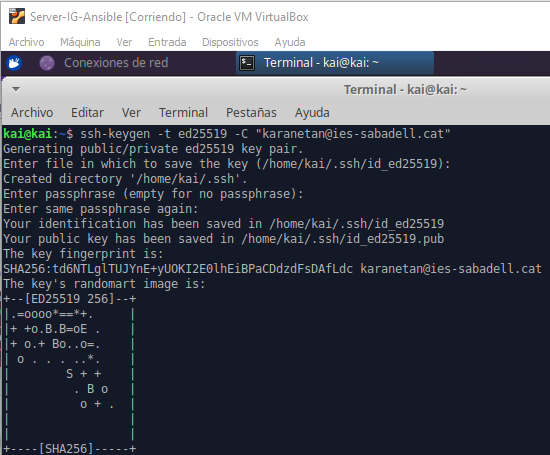
“apt install python3-pip”



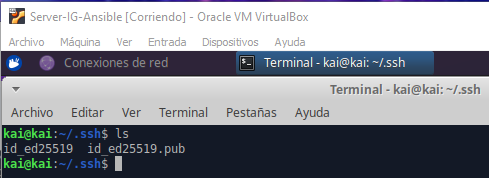
“sudo pip3 install ansible”



ssh-keygen -t ed25519 -C “el\_vostre\_mail@ies-sabadell.cat”



fem un “cd .shh” i després un “ls” per veure les dues claus que hem generat.



La comanda que hem fet servir, genera les claus publica / privada amb l’algoritme d'encriptació de la família «ED» i enllaça aquesta al nostre compte de correu. Quins algoritmes d'encriptació existeixen a més del qual acabem d’utilitzar?

A part de l'algoritme ED25519, hi ha altres algoritmes d'encriptació que es poden utilitzar per generar claus pública/privada, com ara RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), i ECDSA (Elliptic Curve Digital Signature Algorithm).

Quina diferencia hi ha entre ells?

La diferència principal entre aquests algoritmes radica en els mètodes matemàtics que utilitzen per a generar les claus i el nivell de seguretat que proporcionen.

Quins avantatges te la utilització de l’algoritme «ED» respecte al «RSA»?

**Alguns avantatges de l'ús d'ED25519 respecte a RSA són:**

**Eficiència:** Les claus generades són més petites, el que facilita el processament i l'emmagatzematge.

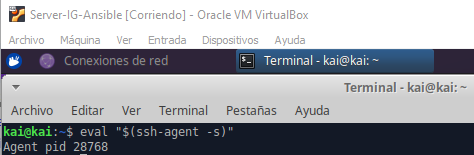
**Velocitat:** Els càlculs amb ED25519 són més ràpids que amb RSA.

**Seguretat:** Malgrat la seva longitud més curta, les claus ED25519 ofereixen un alt nivell de seguretat, ja que són resistents als atacs més comuns.

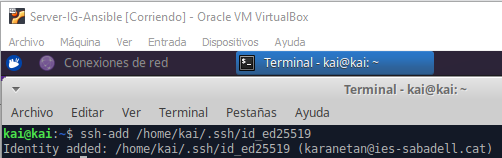
A continuació, ens demanaran una «passphrase». De moment, nosaltres no en farem servir. Explica que es una «passphrase» i quin es el seu objectiu.

Una "passphrase" és una contrasenya llarga i complexa que es fa servir per protegir una clau privada. L'objectiu és augmentar la seguretat de la clau privada afegint una capa addicional de protecció, ja que sense la passphrase, la clau privada no pot ser utilitzada, fins i tot si s'ha accedit al fitxer que la conté.

eval “$(ssh-agent -s)”

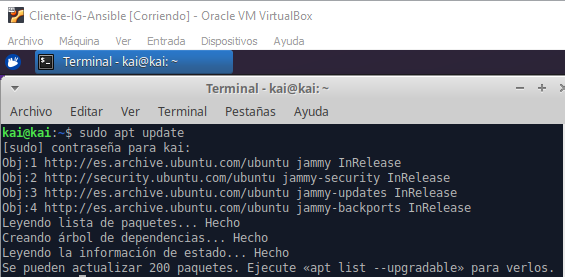


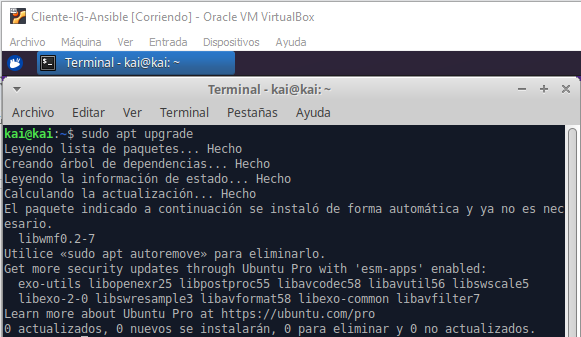
ssh-add /home/vostre\_usuari/.ssh/id\_ed25519



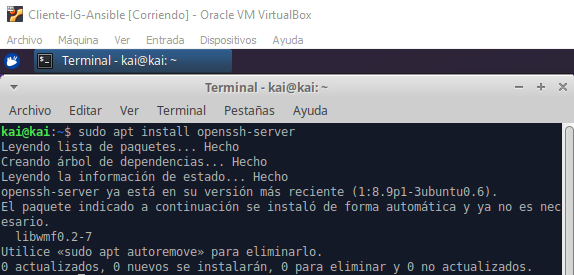
**PART 2**

fem un apt update i un apt upgrade per després instalar el servei ssh.

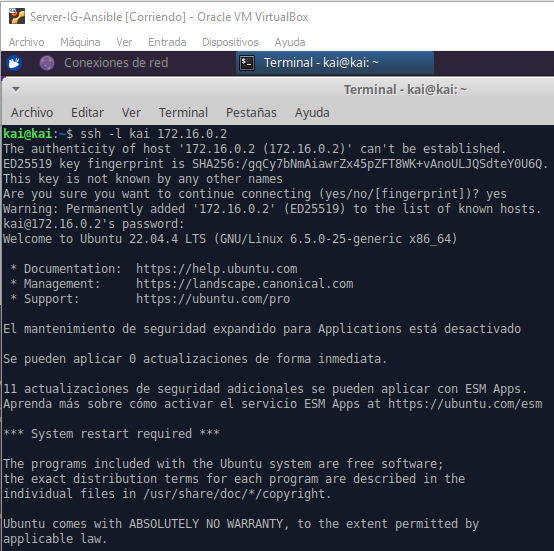




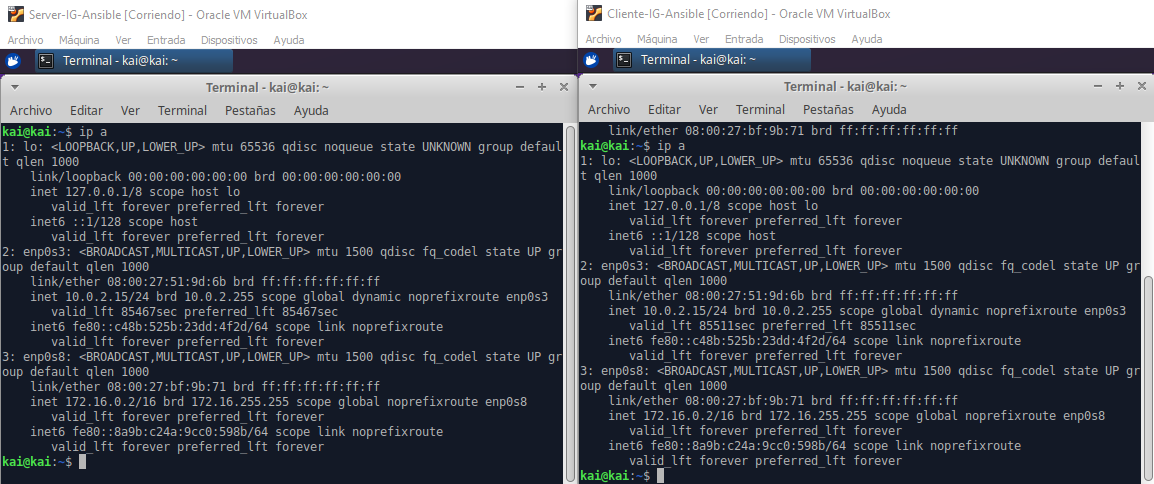
sudo apt install openssh-server.



ssh -l kai 172.16.0.2

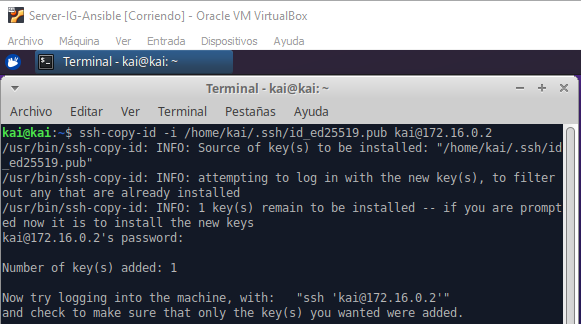


El servidor té la mateixa ip que la del client.



comanda “ssh-copy-id -i /home/kai/.ssh/id\_ed25519.pub kai@172.16.0.2”

Aquesta comanda serveix per pasar la clau pública del servidor al client.

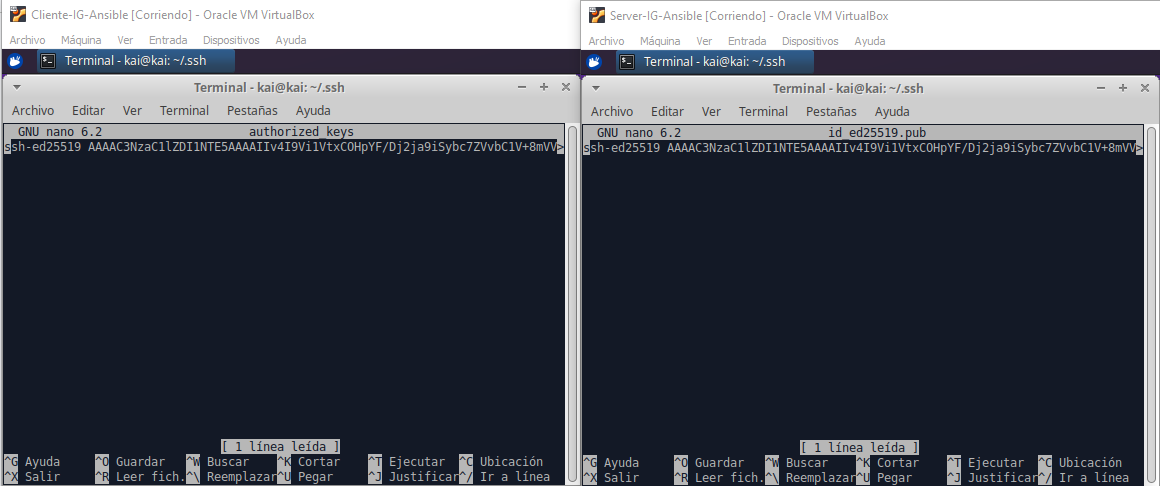


Com podem comprovar-ho? Coincideix amb la clau pública allotjada al servidor?

Desde el client fem un “cd .ssh” i després “nano authorized\_keys” per veure la clau pública.

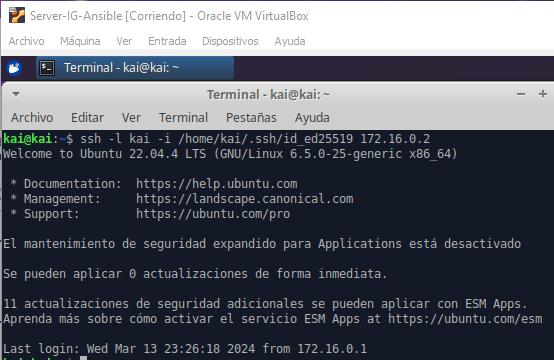
Desde el server fem un “cd .ssh” i després “nano id\_ed25519.pub” per veure la clau publica.

Sí que coincideix.



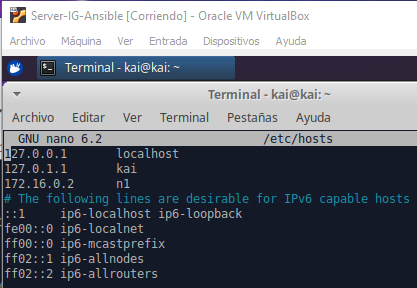
Comprovem que sense que ens demani la contrasenya.

ssh -l kai -i /home/kai/.ssh/id\_ed25519 172.16.0.2



Per últim, afegiu la maquina node com a «n1» dins de l’arxiu «/etc/hosts» i comproveu que podeu establir conexio SSH amb aquest sobrenom.

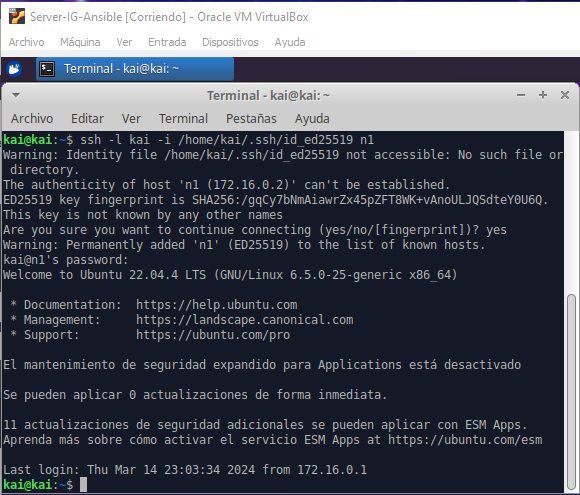
Afegim la ip i el nom al fitxer hosts.



Abans de fer la connexió sortim de la sessió abans on estava en la ip 172.16.0.2, fent un exit.

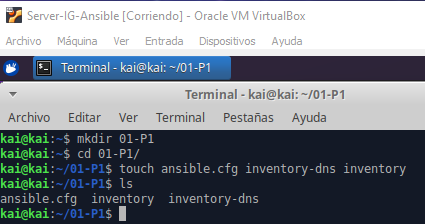


Ara podem fer la connexió amb el nom n1.

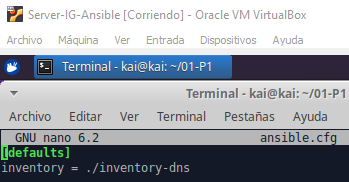


**PART 3**

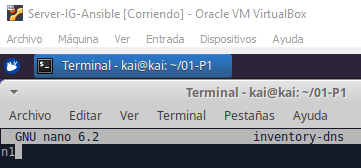
Creem la carpeta 01-P1 amb els arxius corresponents.



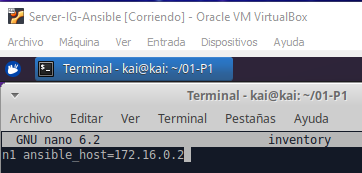
Dins l’arxiu ansible.cfg.



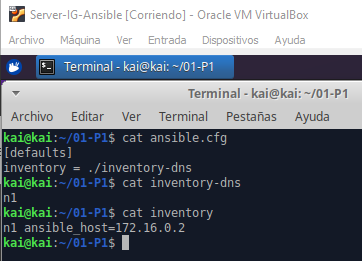
Dins l’arxiu inventory-dns.



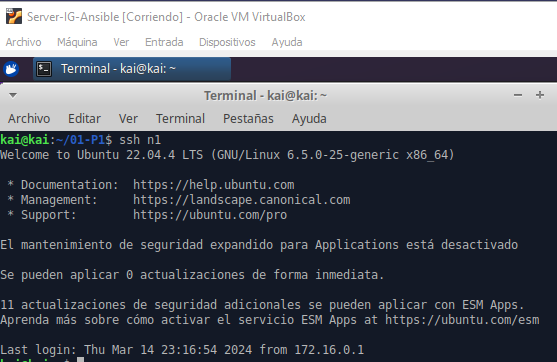
Dins l’arxiu inventory.



Comprovem que els fitxers estan ben escrits.

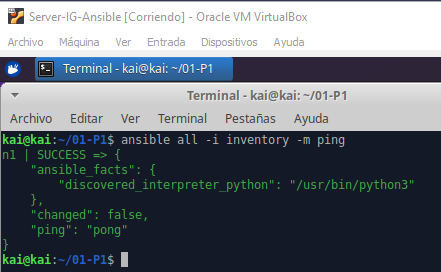


Intentem establir connexió amb el sobrenom n1 amb la comanda “ssh n1”.

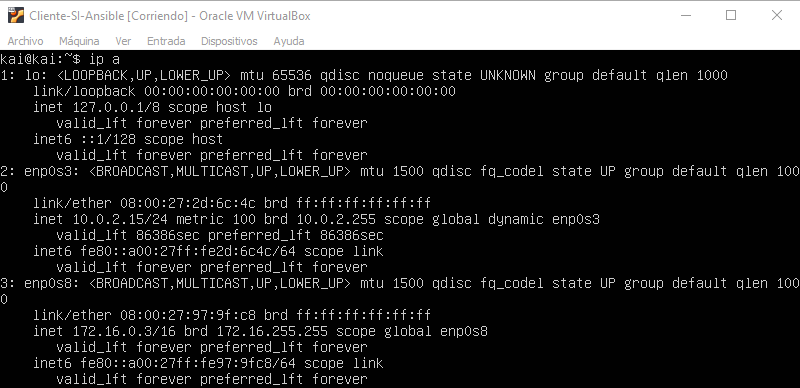


Després sortim fent un èxit per fer un ping a totes les màquines dels nodes encara que només en tinguem una.

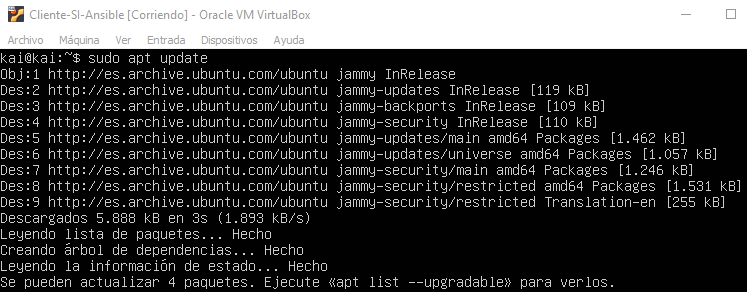
En aquest cas ens surt SUCCESS indicant-nos que el node está operatiu.



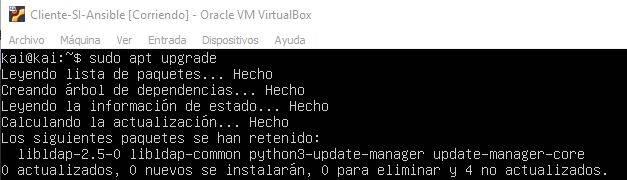
La configuració del client sense interfaç, per fer el node2.



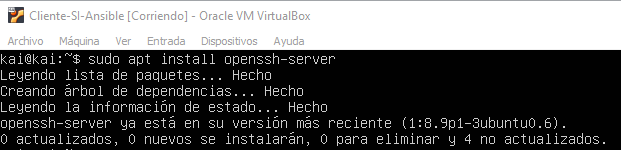
Fem un apt update.



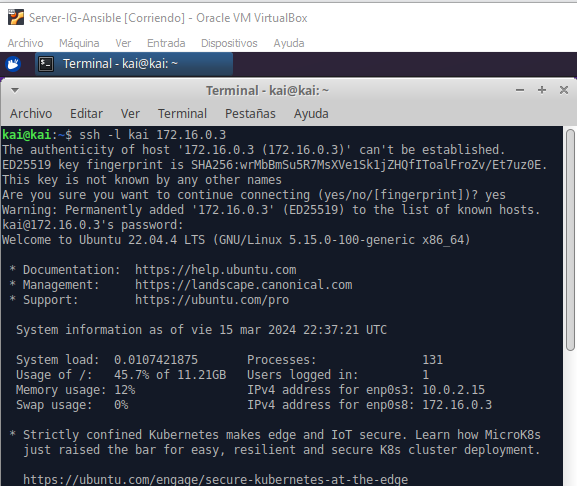
Fem un apt upgrade.



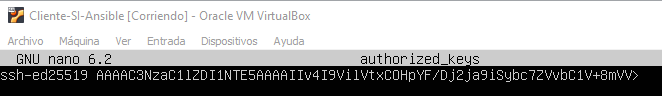
Instalem el openssh-server.



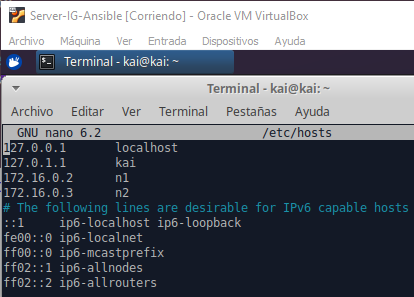
Nos conectamos al nodo2 con la comanda “ssh -l kai 172.16.0.3”



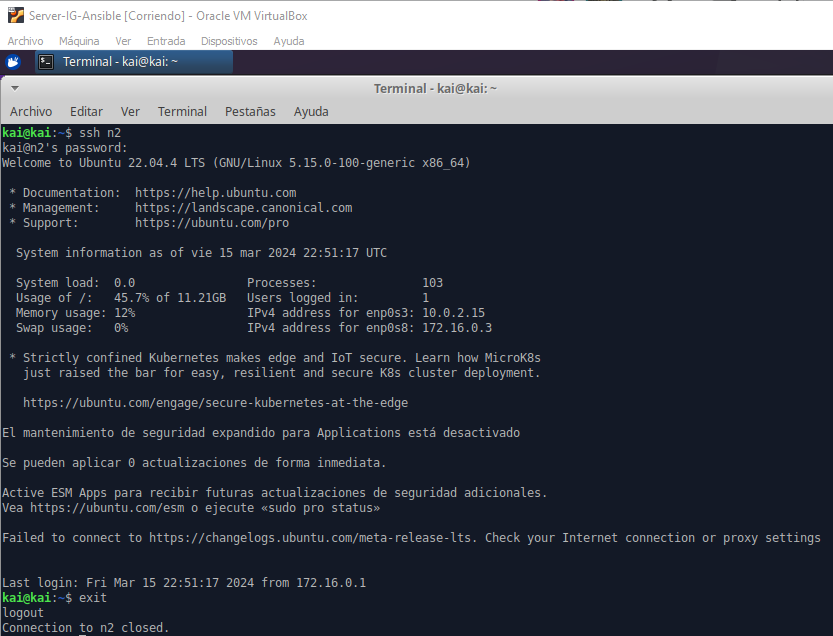
Copiem la clau pública del servidor al cliente sense interfaç al fitxer /.ssh/authorized\_keys



Posem la ip i el nom del node al fitxer /etc/hosts del servidor.

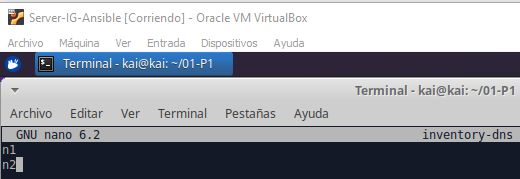


Ens connectem desde el servidor a partir del nom n2 amb la comanda “ssh n2”



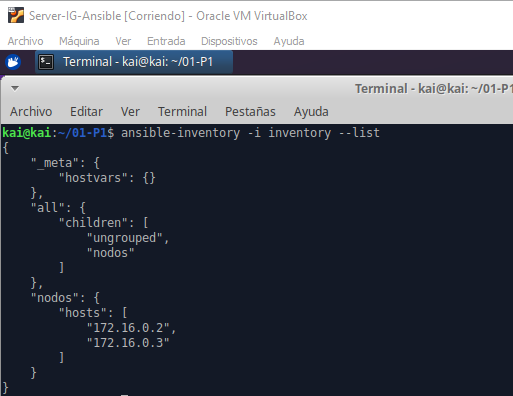
**PART 4**

Afegim el nom del node al fitxer inventory-dns.



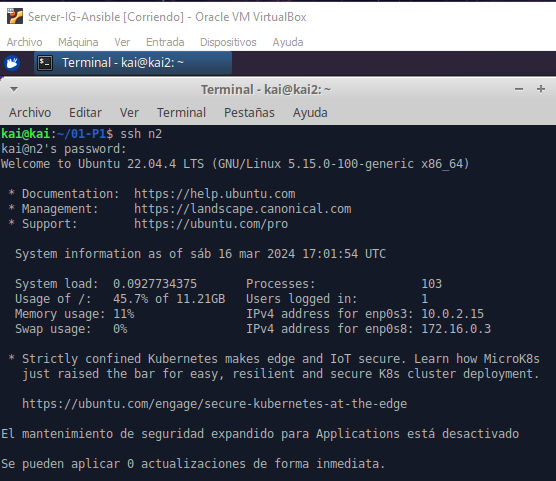
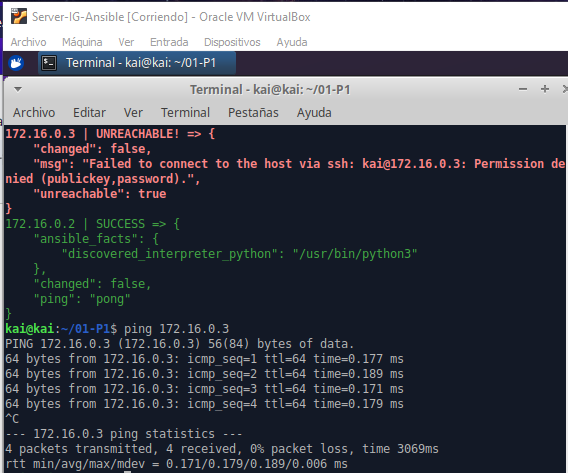
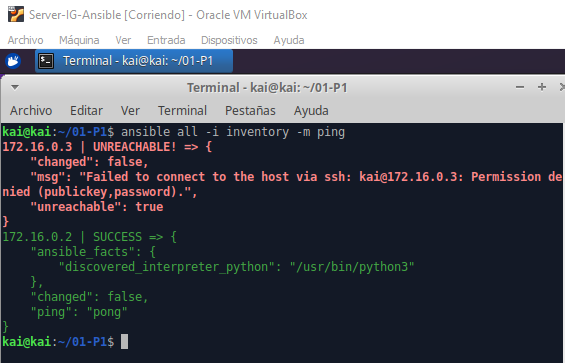
Per comprovar que el que hem fet està bé executem la següent comanda

“ansible-inventory -i inventory –list”



Amb aquesta comanda comprovem que fan ping les màquines.

He intentat arreglar l’error que dona, però no he trobat solució, igualment em deixa conectarme via ssh i les màquines em fan ping i es connecten sense la comanda.



Aquí verifiquem la connectivitat a la màquina utilitzant aquesta ordre (ansible all -i inventari -m ping):

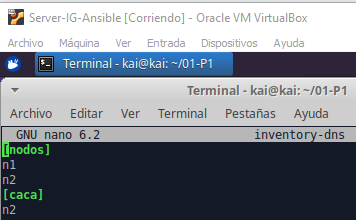
-La direcció IP del node on es va executar la comanda Ansible és 172.20.0.2.

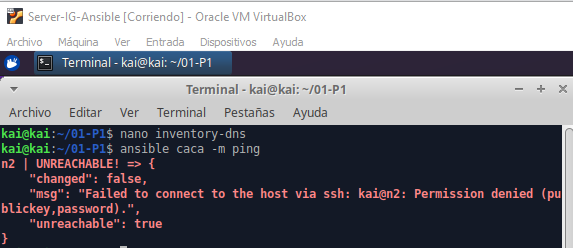
-Èxit: Confirma que el mòdul Ansible s'ha executat correctament al node esmentat.

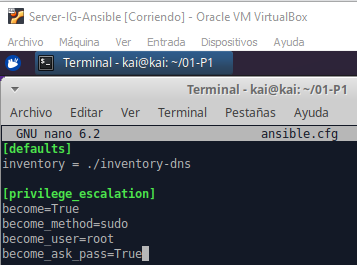
-Informació addicional proporcionada per Ansible sobre el node, com la ubicació de l'intèrpret de Python (/usr/share/python3).

-Sense canvis: Indica que no s'han realitzat modificacions al node com a resultat de l'execució del mòdul ping. En resum, la tasca no va alterar l'estat del sistema.

-Resposta del mòdul ping: El node està disponible i pot respondre a les sol·licituds d'Ansible amb un "pong".







-El bloc [privilege\_escalation] en un fitxer de configuració d'Ansible és utilitzat per gestionar l'escalat de privilegis durant l'execució de tasques. A continuació, expliquem cada camp:

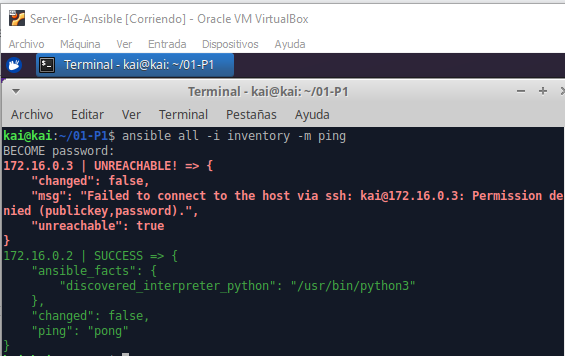
-become=True: Aquesta opció habilita l'escalat de privilegis. Quan es configura com a True, indica que Ansible hauria d'escalat els privilegis per executar tasques amb permisos superiors.

-become\_method=sudo: Aquesta opció especifica el mètode utilitzat per Ansible per a l'escalat de privilegis. En aquest cas, s'utilitza sudo, que és un sistema comú per obtenir privilegis d'administrador en sistemes Unix.

-become\_user=root: Aquesta opció determina l'usuari al qual Ansible hauria d'escalar els privilegis quan executa les tasques. Aquí s'estableix com a root, que és l'usuari amb els més alts privilegis en sistemes Unix.

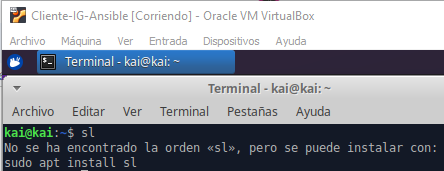
-become\_ask\_pass=True: Aquesta opció indica si Ansible ha de demanar la contrasenya per a l'usuari que es configura com a become\_user quan s'escalten els privilegis. En aquest cas, s'estableix com a True, de manera que Ansible sol·licitarà la contrasenya abans d'escalar els privilegis.

Ara en demana contrasenya abans de fer el ping.

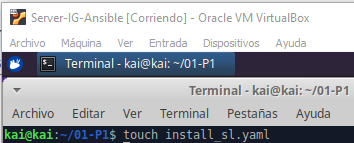


**PLAYBOOKS**

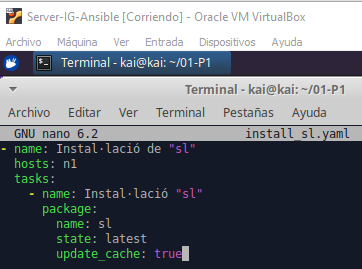
Comprovem que el client no reconeix la comanda sl.



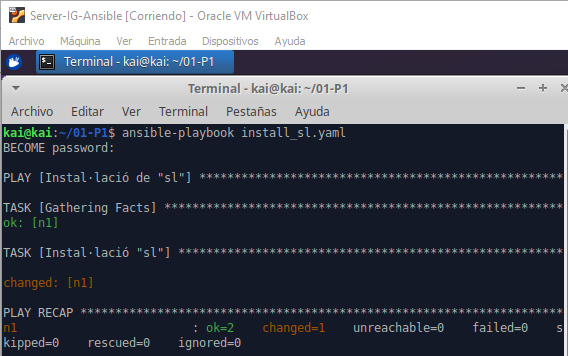
Ara generem l’arxiu al servidor.



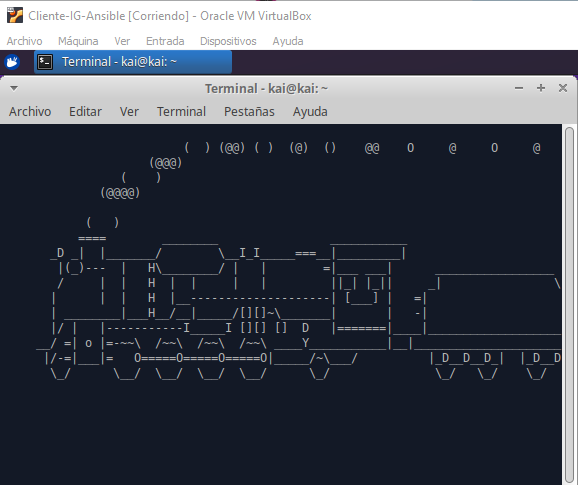
El configurem d’aquesta manera.



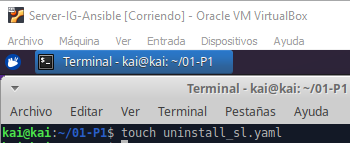
Instal·lem el servei amb aquesta comanda “ansible-playbook install\_sl.yaml”



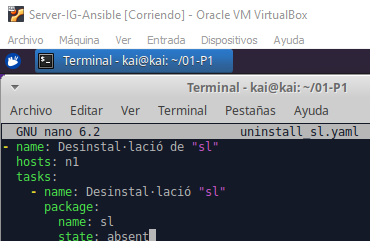
Provem la comanda al client.



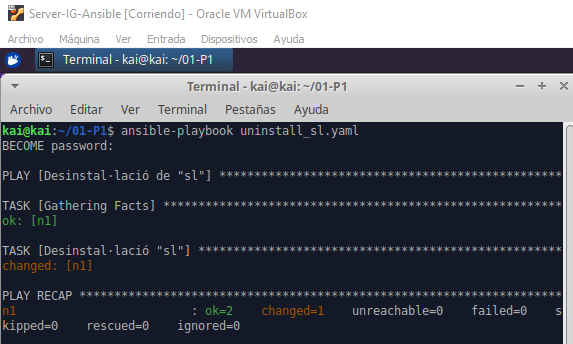
Creem l’arxiu uninstall\_sl.yaml



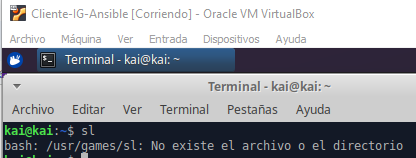
El configurem d’aquesta manera.



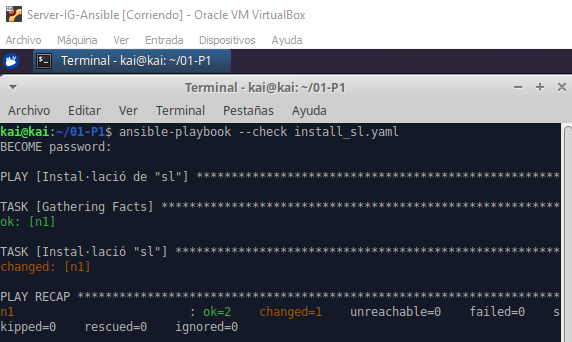
Executem la comanda per desinstalar el programa.



Ja no podem executar la comanda.



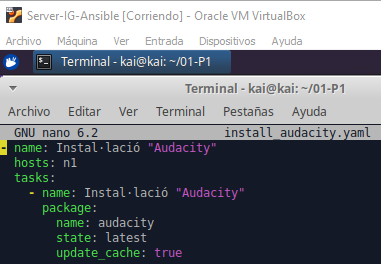
Amb aquesta comanda podríem veure els canvis que es farien si executéssim la comanda.



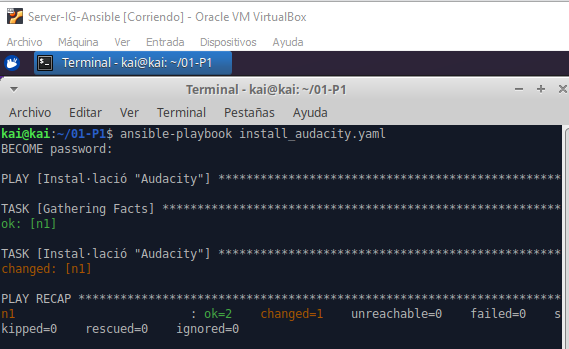
**PLAYBOOK AUDACITY**

Creem el fitxer d'instal·lació audacity

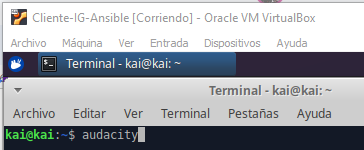
I el configurem d’aquesta manera.



Instal·lem el servei amb la comanda “ansible-palybook install\_audacity.yaml”



Executem la comanda audacity al client amb interfaç



I efectivament s'obre el programa Audacity.

