Chapitre 3 – Configuration de serveurs et d'applications avec Ansible

- Vous êtes chargé d'installer un serveur Ansible. Il s'agit d'un outil open source DevOps qui automatise le provisionnement, la gestion des configurations ainsi que le déploiement des applications sur initialement des serveurs Linux. La plateforme Ansible gère les différents nœuds à l'aide du protocole SSH et ne nécessite aucune installation de logiciel supplémentaire sur ceux-ci.
- Pour mener à bien votre mission, vous disposez d'un serveur que vous nommerez **Ansible** sur lequel est installé le système d'exploitation Linux **Debian 13 (Trixie)**. L'environnement de bureau a été gardé pour bénéficier d'un navigateur.

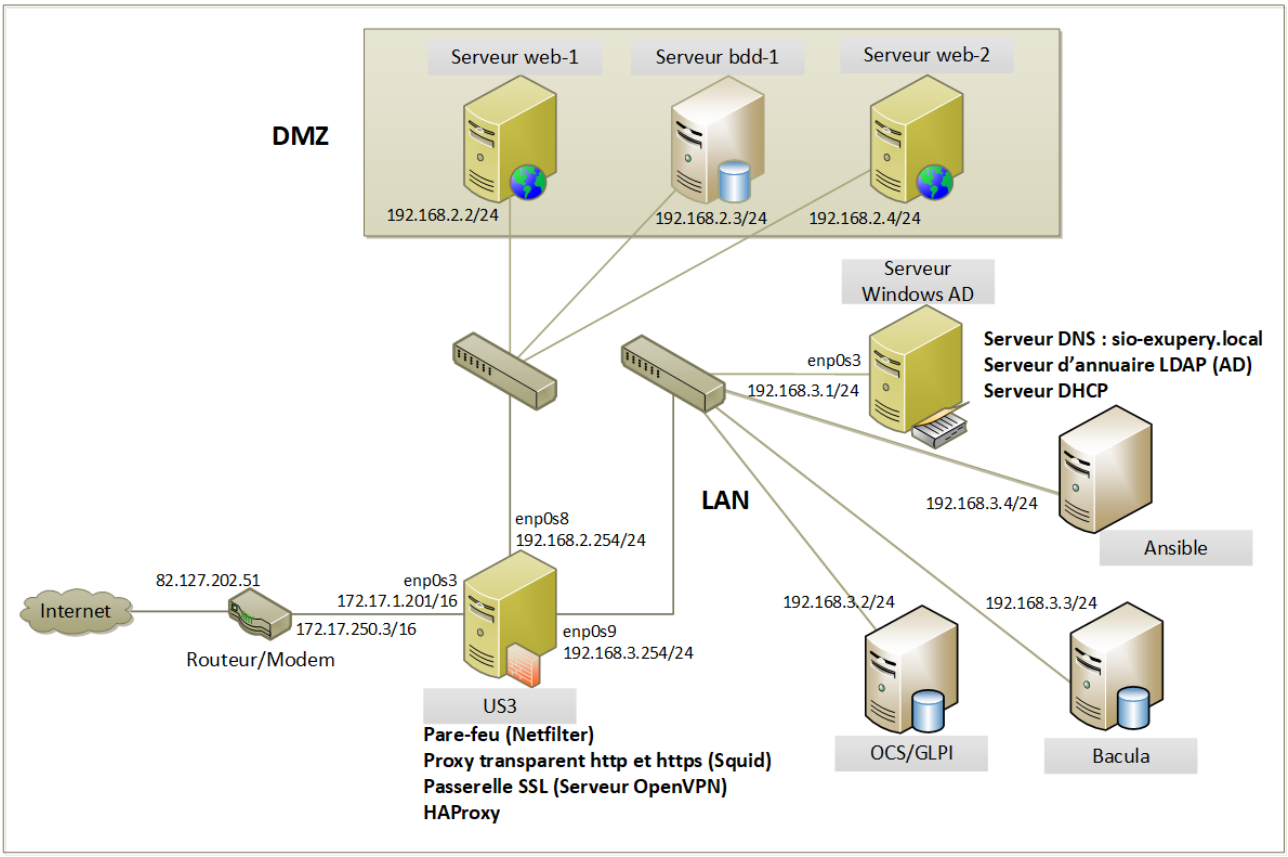


Table des matières

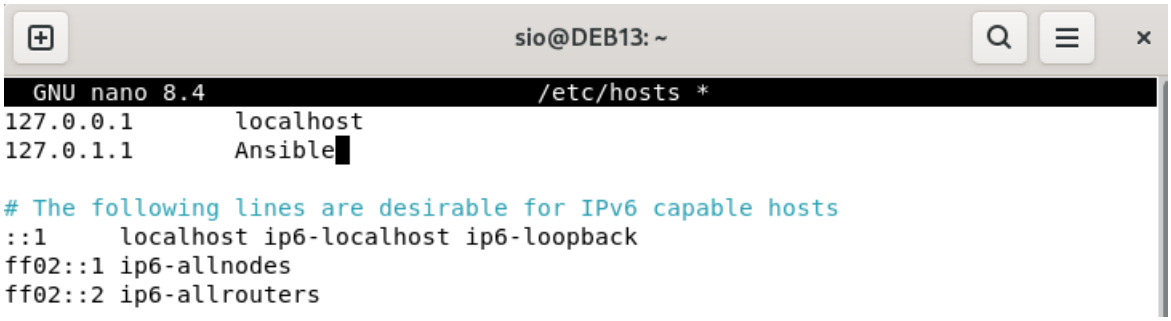
https://docs.ansible.com/projects/ansible/latest/installation_guide/intro_installation.html

https://blog.stephane-robert.info/docs/developper/programmation/python/pipx/

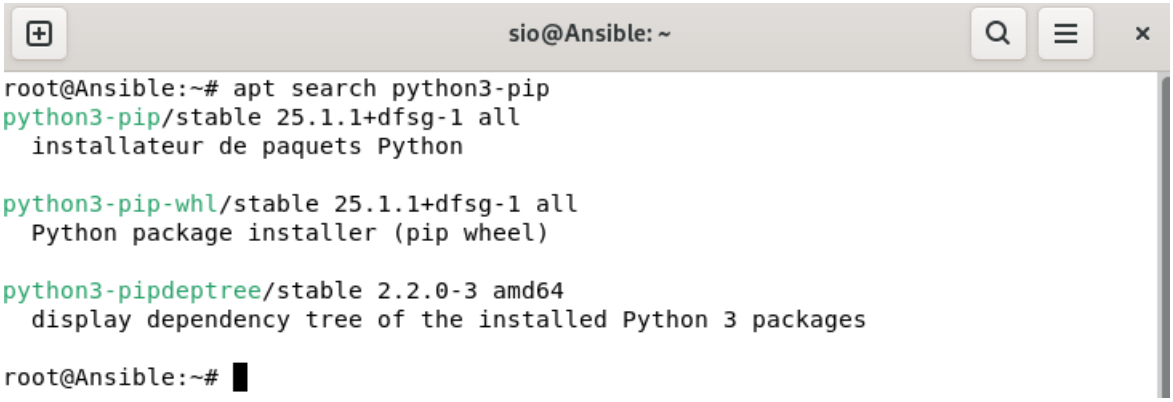
https://pipx.pypa.io/stable/installation/

https://blog.stephane-robert.info/docs/infra-as-code/gestion-de-configuration/ansible/

1. Installation d'Ansible.



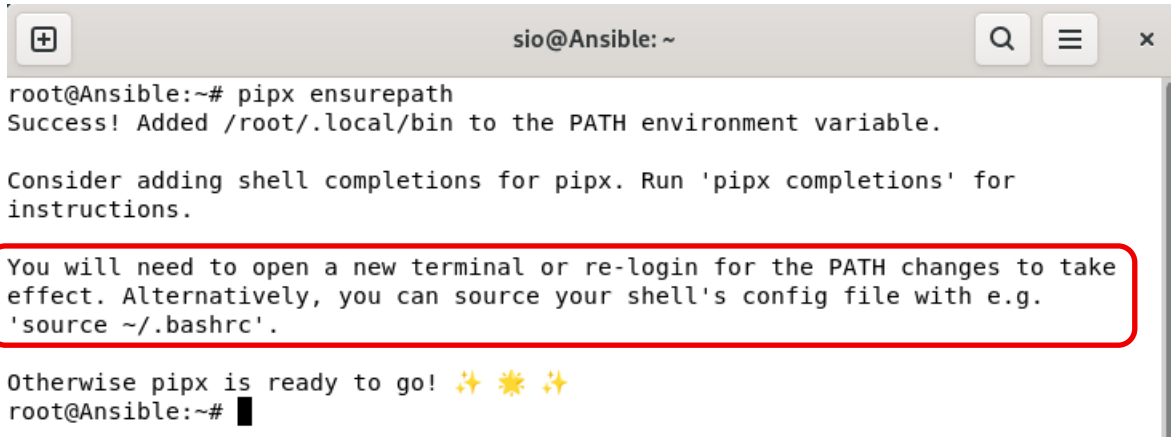
Installation d'Ansible via le gestionnaire de paquets Apt ou à l'aide de l'outil pip de Python



```
sio@Ansible: ~
root@Ansible:~# apt-get install python3-pip
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libexpat1-dev libjs-sphinxdoc libpython3-dev libpython3.13-dev python3-dev
  python3-packaging python3-wheel python3.13-dev zlib1g-dev
Paquets suggérés :
  python3-setuptools
Les NOUVEAUX paquets suivants seront installés :
  libexpat1-dev libjs-sphinxdoc libpython3-dev libpython3.13-dev python3-dev
  python3-packaging python3-pip python3-wheel python3.13-dev zlib1g-dev
0 mis à jour, 10 nouvellement installés, 0 à enlever et 22 non mis à jour.
Il est nécessaire de prendre 8 477 kB dans les archives.
Après cette opération, 41,3 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```

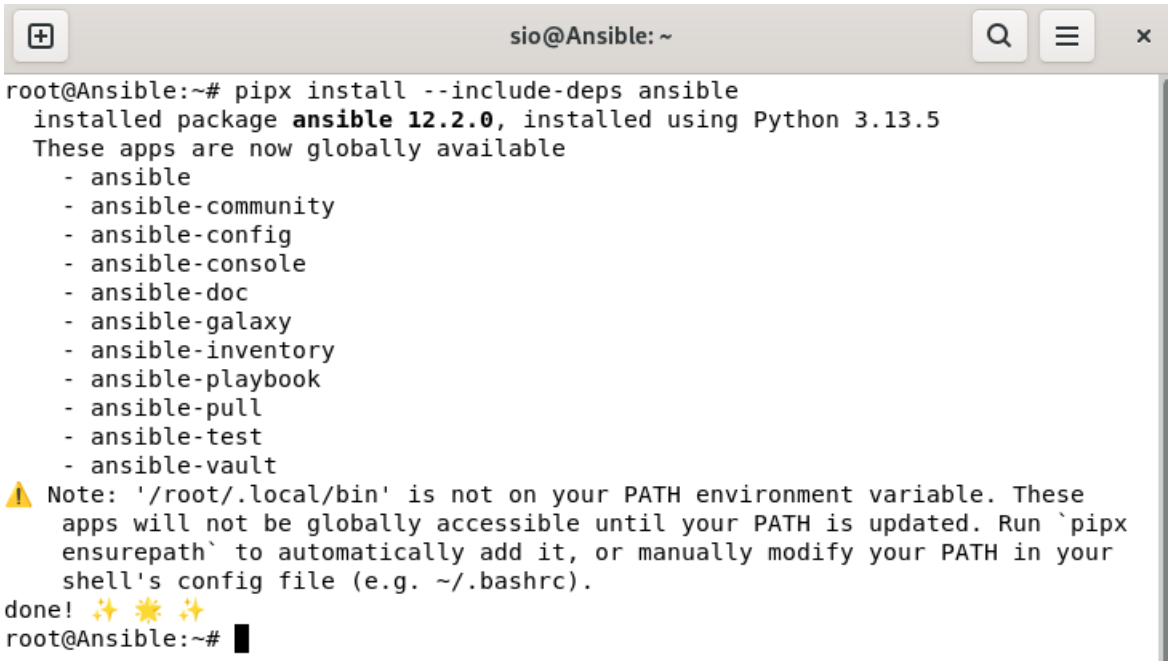
```
sio@Ansible: ~
root@Ansible:~# pip install ansible
error: externally-managed-environment

× This environment is externally managed
╰─> To install Python packages system-wide, try apt install
    python3-xyz, where xyz is the package you are trying to
    install.

    If you wish to install a non-Debian-packaged Python package,
    create a virtual environment using python3 -m venv path/to/venv.
    Then use path/to/venv/bin/python and path/to/venv/bin/pip. Make
    sure you have python3-full installed.

    If you wish to install a non-Debian packaged Python application,
    it may be easiest to use pipx install xyz, which will manage a
    virtual environment for you. Make sure you have pipx installed.

    See /usr/share/doc/python3.13/README.venv for more information.

note: If you believe this is a mistake, please contact your Python installation
or OS distribution provider. You can override this, at the risk of breaking your
 Python installation or OS, by passing --break-system-packages.
hint: See PEP 668 for the detailed specification.
root@Ansible:~#
```

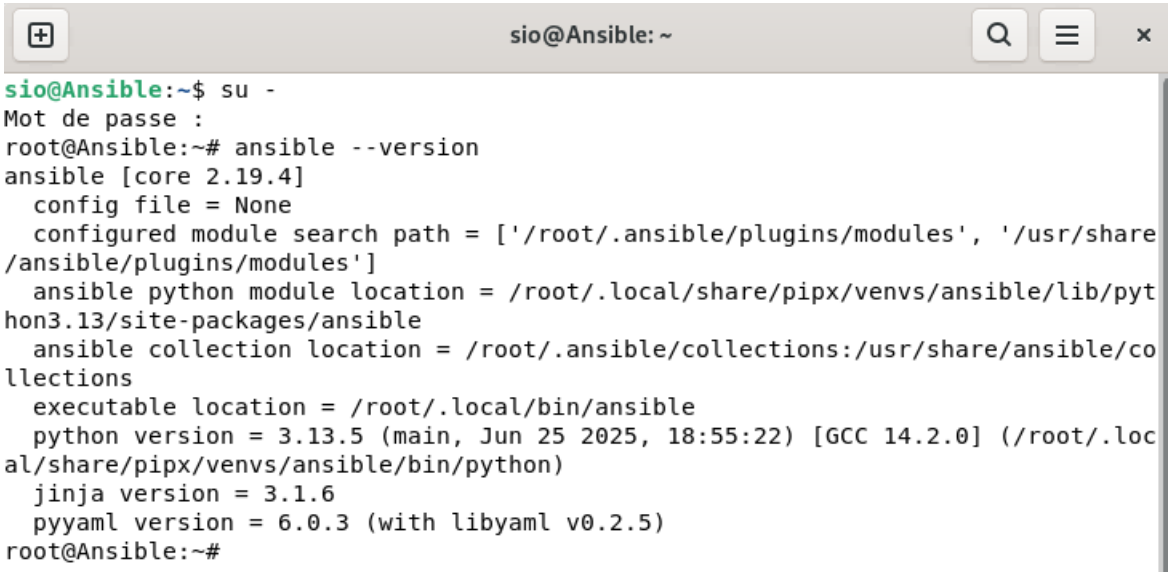
```
sio@Ansible: ~
root@Ansible:~# apt-get install pipx
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  python3-argcomplete python3-click python3-packaging python3-pip-whl
  python3-platformdirs python3-setuptools-whl python3-userpath python3-venv
  python3.13-venv
Les NOUVEAUX paquets suivants seront installés :
  pipx python3-argcomplete python3-click python3-packaging python3-pip-whl
  python3-platformdirs python3-setuptools-whl python3-userpath python3-venv
  python3.13-venv
0 mis à jour, 10 nouvellement installés, 0 à enlever et 109 non mis à jour.
Il est nécessaire de prendre 3 830 kB dans les archives.
Après cette opération, 7 745 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
```


sio@Ansible: ~
root@Ansible:~# pipx ensurepath
Success! Added /root/.local/bin to the PATH environment variable.
Consider adding shell completions for pipx. Run 'pipx completions' for instructions.
You will need to open a new terminal or re-login for the PATH changes to take effect. Alternatively, you can source your shell's config file with e.g. 'source ~/.bashrc'.
Otherwise pipx is ready to go! ✨ 🌟 ✨
root@Ansible:~#

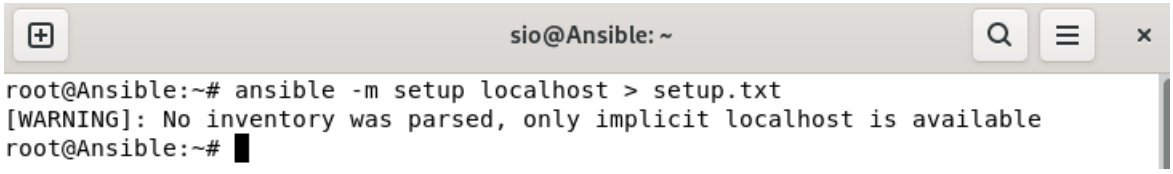

sio@Ansible: ~
root@Ansible:~# pipx ensurepath --global
/usr/local/bin is already in PATH.
⚠️ All pipx binary directories have been appended to PATH. If you are sure you want to proceed, try again with the '--force' flag.
Otherwise pipx is ready to go! ✨ 🌟 ✨
root@Ansible:~#


sio@Ansible: ~
root@Ansible:~# pipx install --include-deps ansible
⡿ installing ansible


sio@Ansible: ~
root@Ansible:~# pipx install --include-deps ansible
installed package ansible 12.2.0, installed using Python 3.13.5
These apps are now globally available
- ansible
- ansible-community
- ansible-config
- ansible-console
- ansible-doc
- ansible-galaxy
- ansible-inventory
- ansible-playbook
- ansible-pull
- ansible-test
- ansible-vault
⚠️ Note: '/root/.local/bin' is not on your PATH environment variable. These apps will not be globally accessible until your PATH is updated. Run `pipx ensurepath` to automatically add it, or manually modify your PATH in your shell's config file (e.g. ~/.bashrc).
done! ✨ 🌟 ✨
root@Ansible:~#



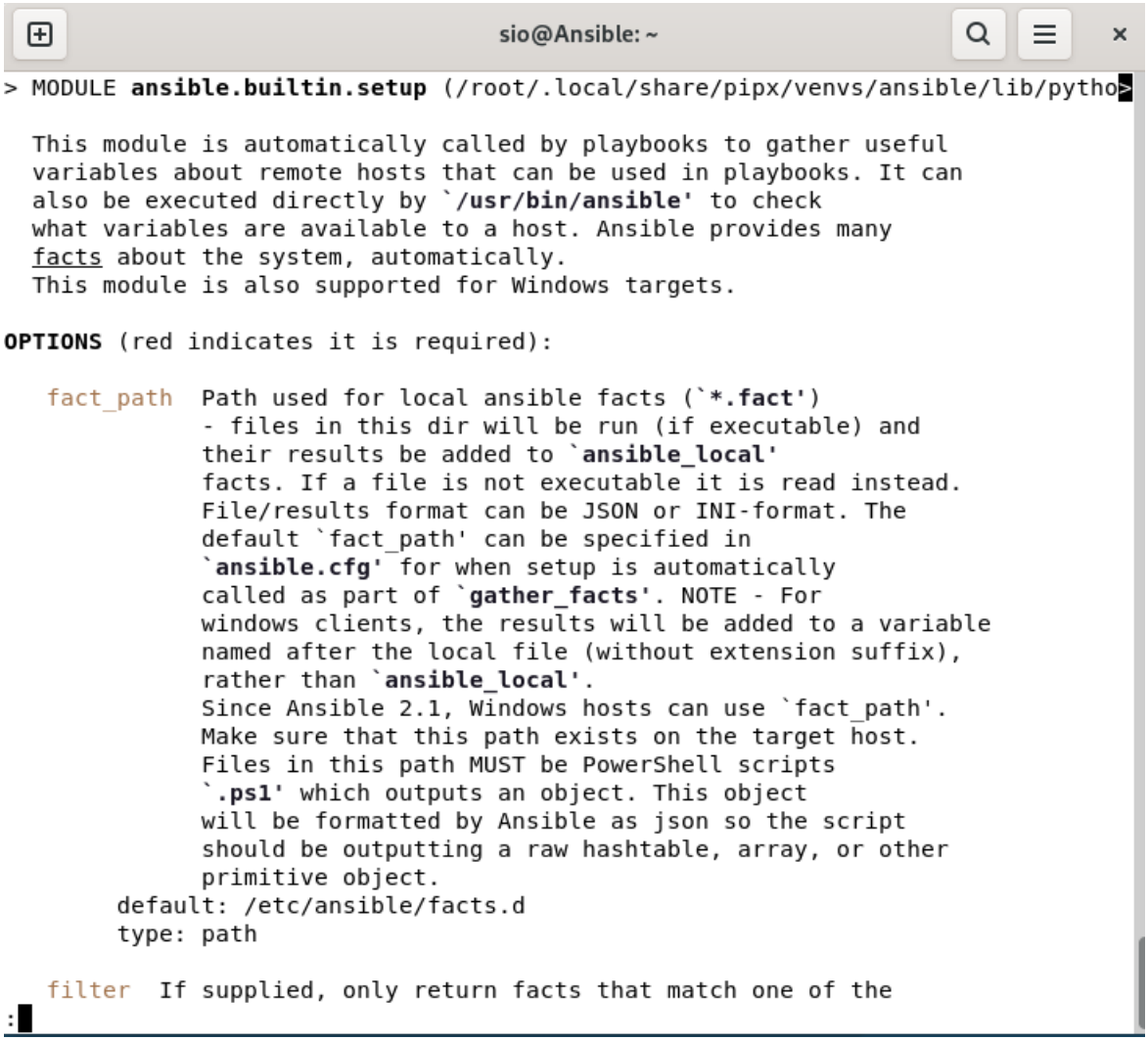
2. Premier module avec Ansible (setup).

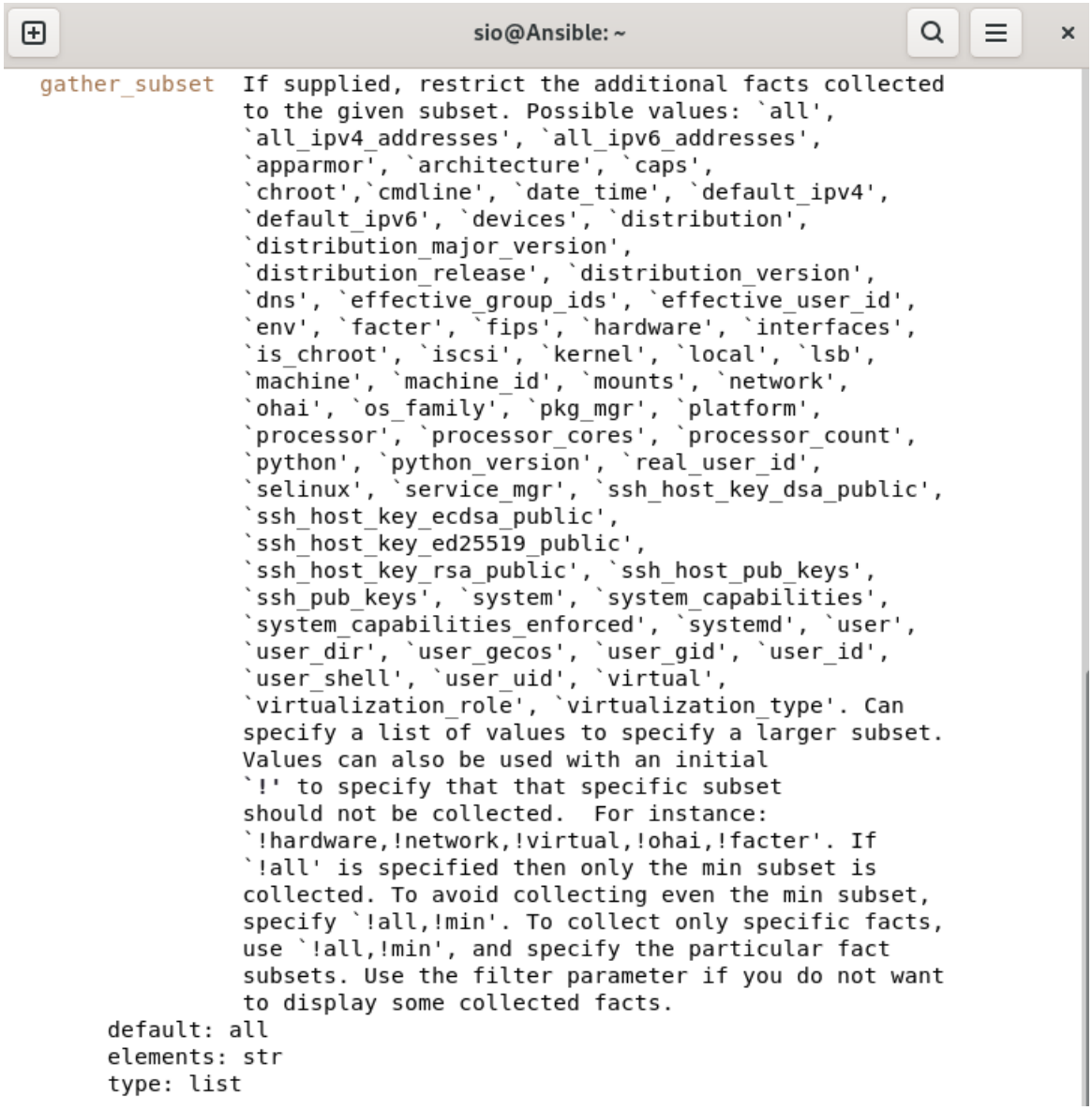



sio@Ansible: ~
root@Ansible:~# cat setup.txt
localhost | SUCCESS => {
"ansible_facts": {
"ansible_all_ipv4_addresses": [
"10.0.2.15"
],
"ansible_all_ipv6_addresses": [
"fd17:625c:f037:2:a00:27ff:fe71:3345",
"fe80::a00:27ff:fe71:3345",
"fd17:625c:f037:2:406f:55c9:f0e6:2987"
],
"ansible_apparmor": {
"status": "enabled"
},
"ansible_architecture": "x86_64",
"ansible_bios_date": "12/01/2006",
"ansible_bios_vendor": "innotek GmbH",
"ansible_bios_version": "VirtualBox",
"ansible_board_asset_tag": "NA",
"ansible_board_name": "VirtualBox",
"ansible_board_serial": "0",
"ansible_board_vendor": "Oracle Corporation",
"ansible_board_version": "1.2",
"ansible_chassis_asset_tag": "NA",
"ansible_chassis_serial": "NA",
"ansible_chassis_vendor": "Oracle Corporation",
"ansible_chassis_version": "NA",
"ansible_cmdline": {
"BOOT_IMAGE": "/boot/vmlinuz-6.12.48+deb13-amd64",
"quiet": true,
"ro": true,
"root": "UUID=9ccbd479-6936-430a-8f70-1ed16e8b90e6"
},
"ansible_date_time": {
"date": "2025-11-15",
"day": "15",
"epoch": "1763241666",
"epoch_int": "1763241666",
"hour": "22",
"iso8601": "2025-11-15T21:21:06Z",
"iso8601_basic": "20251115T222106176844",
"iso8601_basic_short": "20251115T222106",
"iso8601_micro": "2025-11-15T21:21:06.176844Z",
"minute": "21",

3. Aide et documentation officielle

3.1. Ansible-doc setup

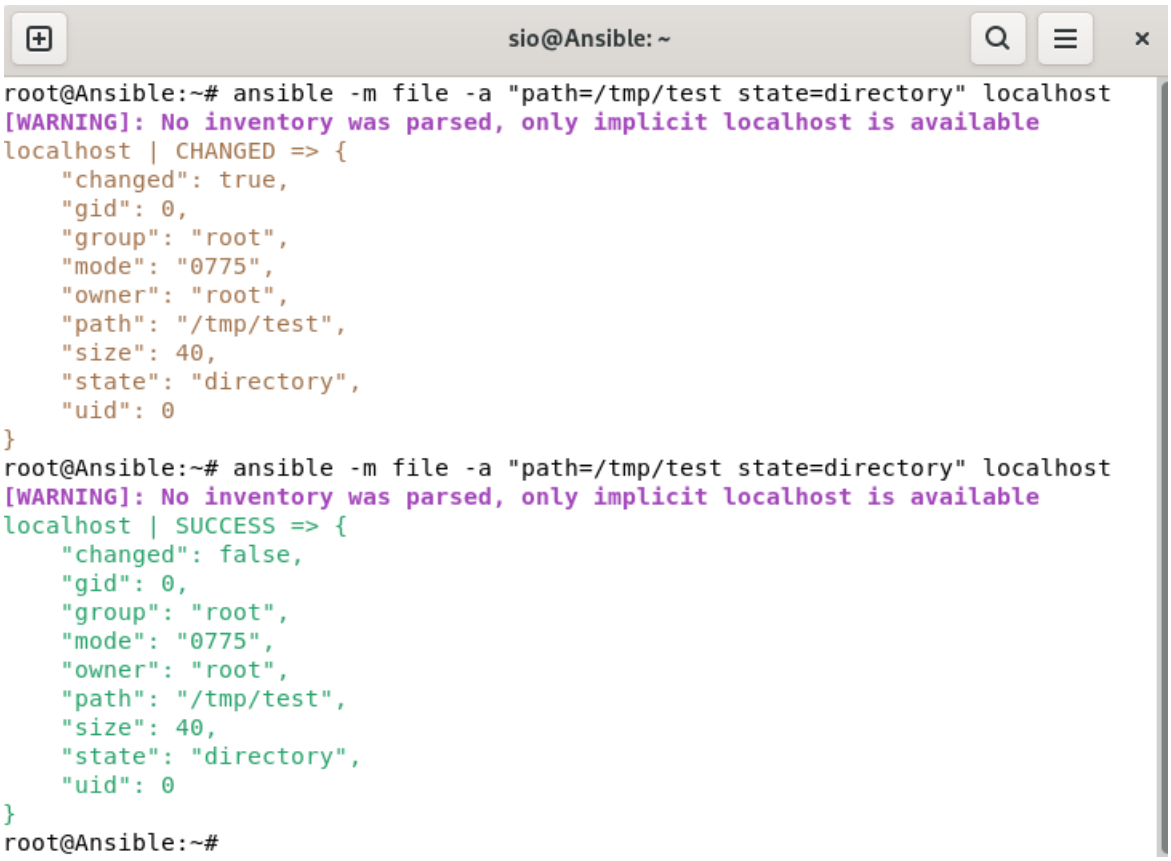

sio@Ansible: ~
> MODULE ansible.builtin.setup (/root/.local/share/pipx/venvs/ansible/lib/pytho
This module is automatically called by playbooks to gather useful
variables about remote hosts that can be used in playbooks. It can
also be executed directly by `/usr/bin/ansible' to check
what variables are available to a host. Ansible provides many
facts about the system, automatically.
This module is also supported for Windows targets.
OPTIONS (red indicates it is required):
fact_path Path used for local ansible facts (`*.fact')
- files in this dir will be run (if executable) and
their results be added to `ansible_local'
facts. If a file is not executable it is read instead.
File/results format can be JSON or INI-format. The
default `fact_path' can be specified in
`ansible.cfg' for when setup is automatically
called as part of `gather_facts'. NOTE - For
windows clients, the results will be added to a variable
named after the local file (without extension suffix),
rather than `ansible_local'.
Since Ansible 2.1, Windows hosts can use `fact_path'.
Make sure that this path exists on the target host.
Files in this path MUST be PowerShell scripts
`.ps1' which outputs an object. This object
will be formatted by Ansible as json so the script
should be outputting a raw hashtable, array, or other
primitive object.
default: /etc/ansible/facts.d
type: path
filter If supplied, only return facts that match one of the
:

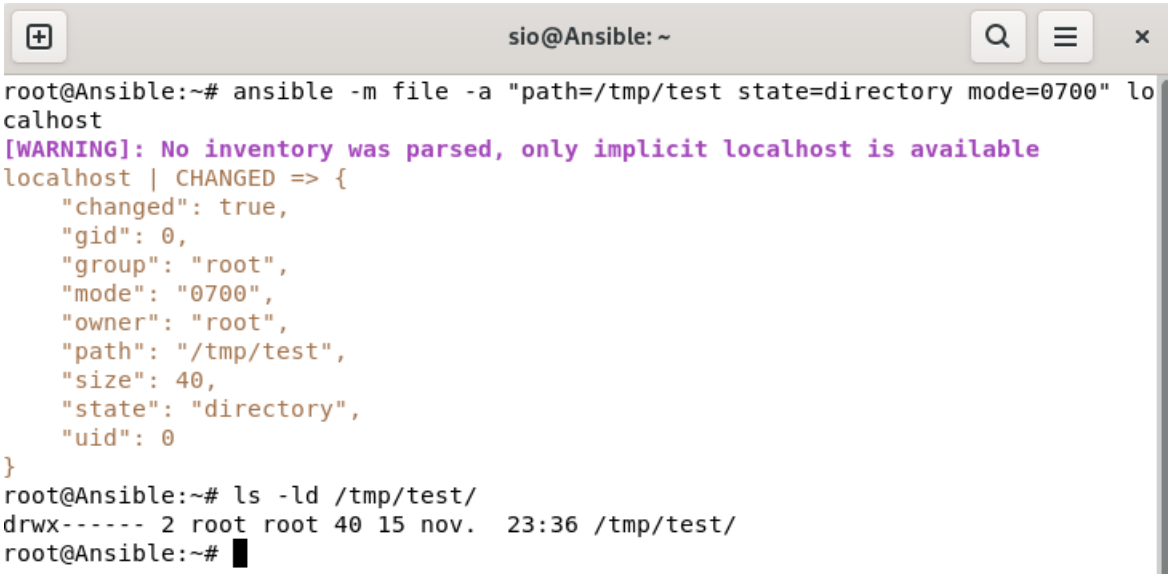

sio@Ansible: ~
gather_subset If supplied, restrict the additional facts collected to the given subset. Possible values: `all', `all_ipv4_addresses', `all_ipv6_addresses', `apparmor', `architecture', `caps', `chroot',`cmdline', `date_time', `default_ipv4', `default_ipv6', `devices', `distribution', `distribution_major_version', `distribution_release', `distribution_version', `dns', `effective_group_ids', `effective_user_id', `env', `facter', `fips', `hardware', `interfaces', `is_chroot', `iscsi', `kernel', `local', `lsb', `machine', `machine_id', `mounts', `network', `ohai', `os_family', `pkg_mgr', `platform', `processor', `processor_cores', `processor_count', `python', `python_version', `real_user_id', `selinux', `service_mgr', `ssh_host_key_dsa_public', `ssh_host_key_ecdsa_public', `ssh_host_key_ed25519_public', `ssh_host_key_rsa_public', `ssh_host_pub_keys', `ssh_pub_keys', `system', `system_capabilities', `system_capabilities_enforced', `systemd', `user', `user_dir', `user_gecos', `user_gid', `user_id', `user_shell', `user_uid', `virtual', `virtualization_role', `virtualization_type'. Can specify a list of values to specify a larger subset. Values can also be used with an initial `!' to specify that that specific subset should not be collected. For instance: `!hardware,!network,!virtual,!ohai,!facter'. If `!all' is specified then only the min subset is collected. To avoid collecting even the min subset, specify `!all,!min'. To collect only specific facts, use `!all,!min', and specify the particular fact subsets. Use the filter parameter if you do not want to display some collected facts.
default: all
elements: str
type: list

3.2. Documentation officielle

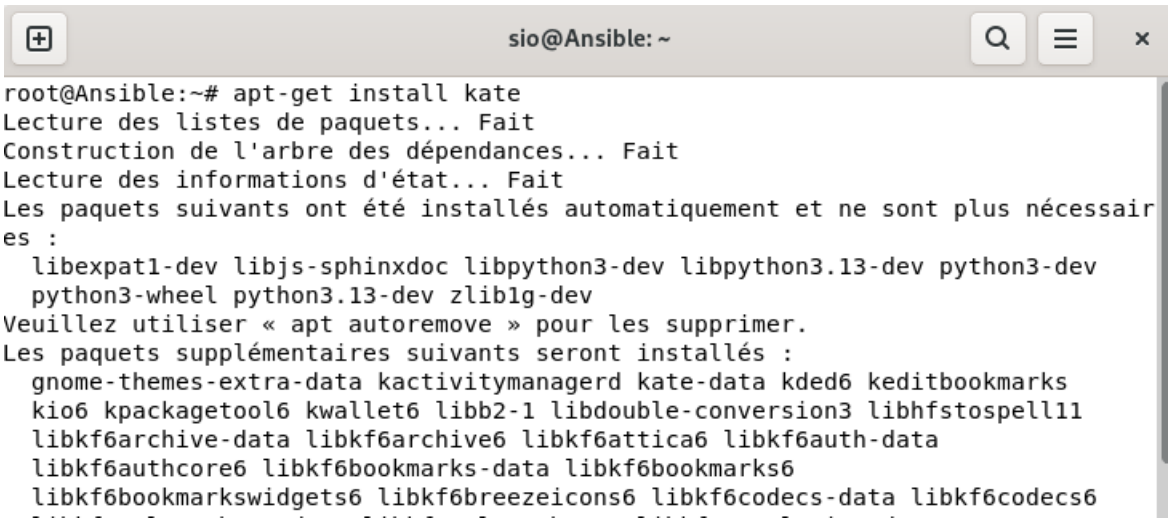
https://docs.ansible.com/

4. Idempotence : exemple avec gestion des répertoires



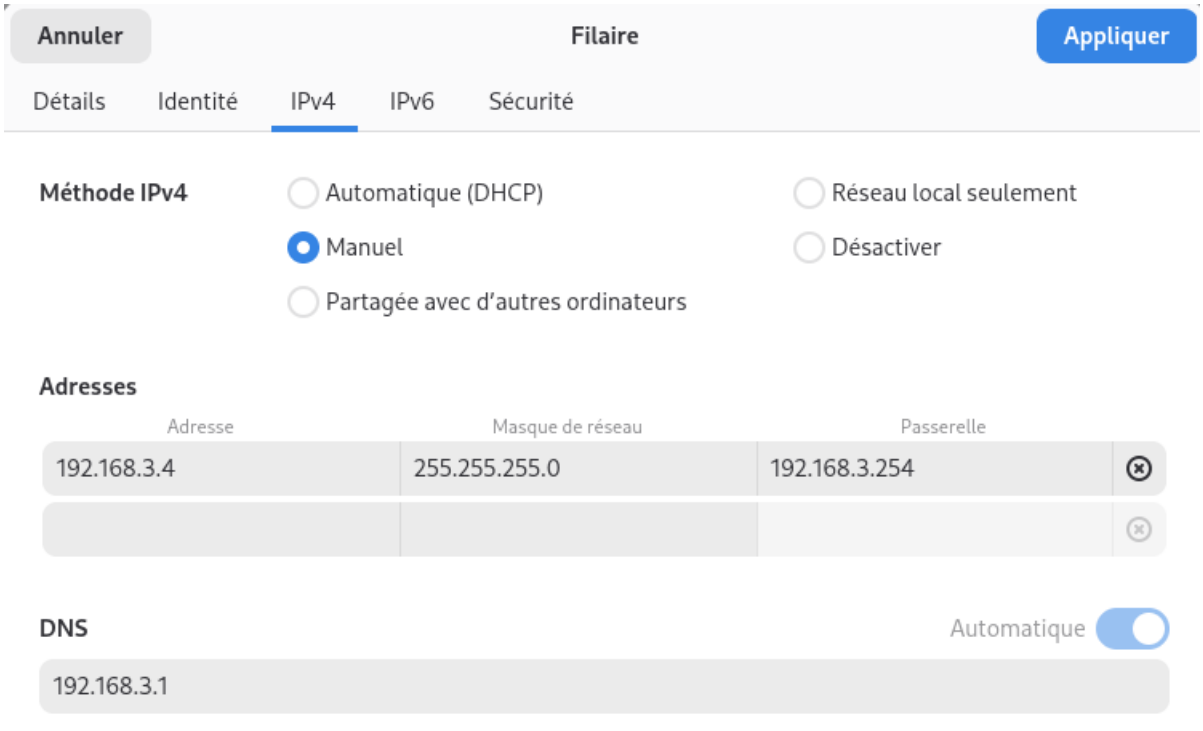


5. Création d'un fichier d'inventaire

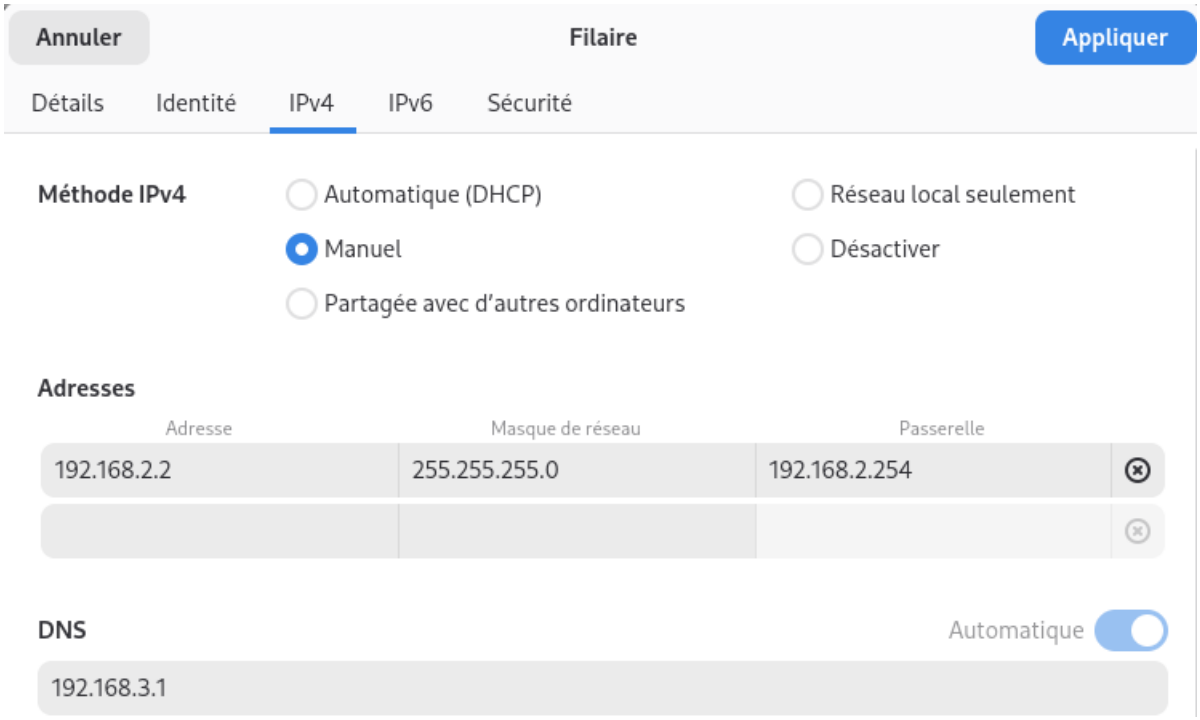


VM pfSense à démarrer

VM Ansible : Réseau interne LAN



VM web-1 et bdd-1 (clones Debian13) : Réseau interne DMZ



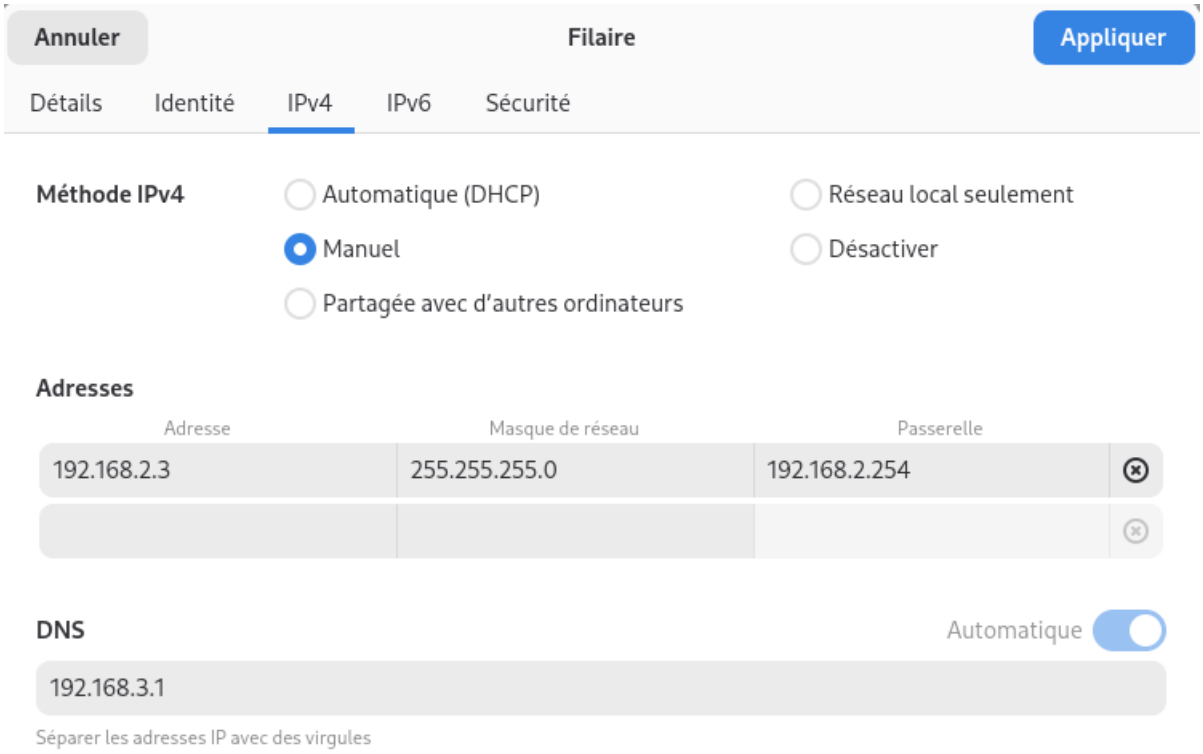

```
sio@web1: ~
 GNU nano 8.4                    /etc/hosts
127.0.0.1       localhost
192.168.2.2     web-1

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
sio@web1: ~
 GNU nano 8.4                    /etc/hostname
web-1
```

```
sio@web-1: ~
root@web-1:~# ss -antp4
State      Recv-Q     Send-Q       Local Address:Port        Peer Address:Port
Process
LISTEN     0          128                0.0.0.0:22               0.0.0.0:*
 users:(("sshd",pid=1014,fd=6))
LISTEN     0          4096             127.0.0.1:631              0.0.0.0:*
 users:(("cupsd",pid=995,fd=7))
root@web-1:~#
```

```
sio@web1: ~
 GNU nano 8.4                /etc/ssh/sshd_config

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
sio@Ansible: ~
root@Ansible:~# systemctl restart sshd
root@Ansible:~#
```

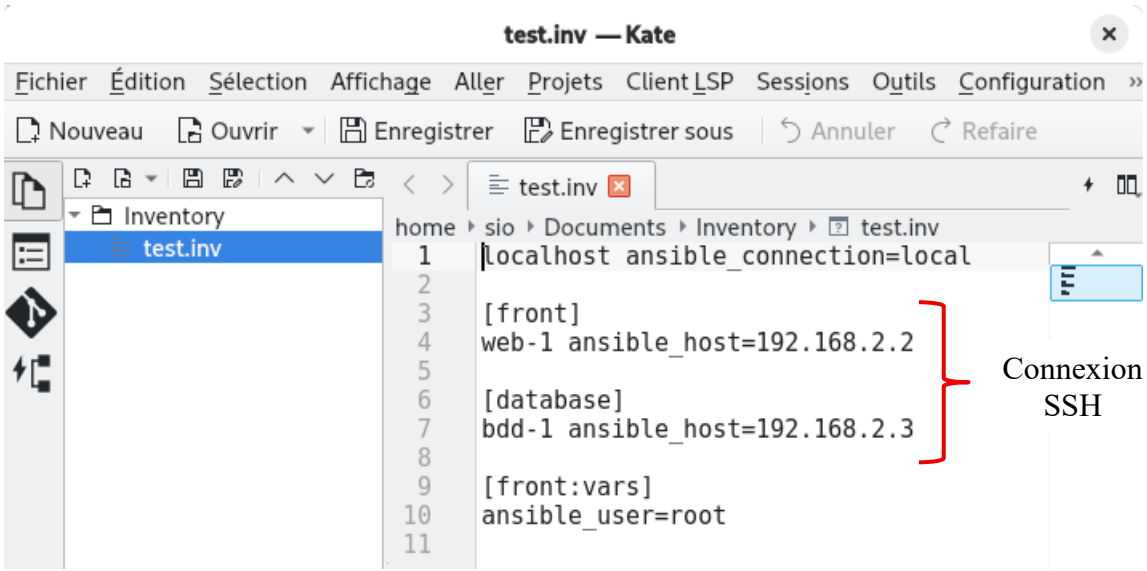



```
sio@bdd-1: ~
 GNU nano 8.4                    /etc/hosts
127.0.0.1       localhost
192.168.2.3     bdd-1

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

```
sio@bdd-1: ~
 GNU nano 8.4                    /etc/hostname
bdd-1
```

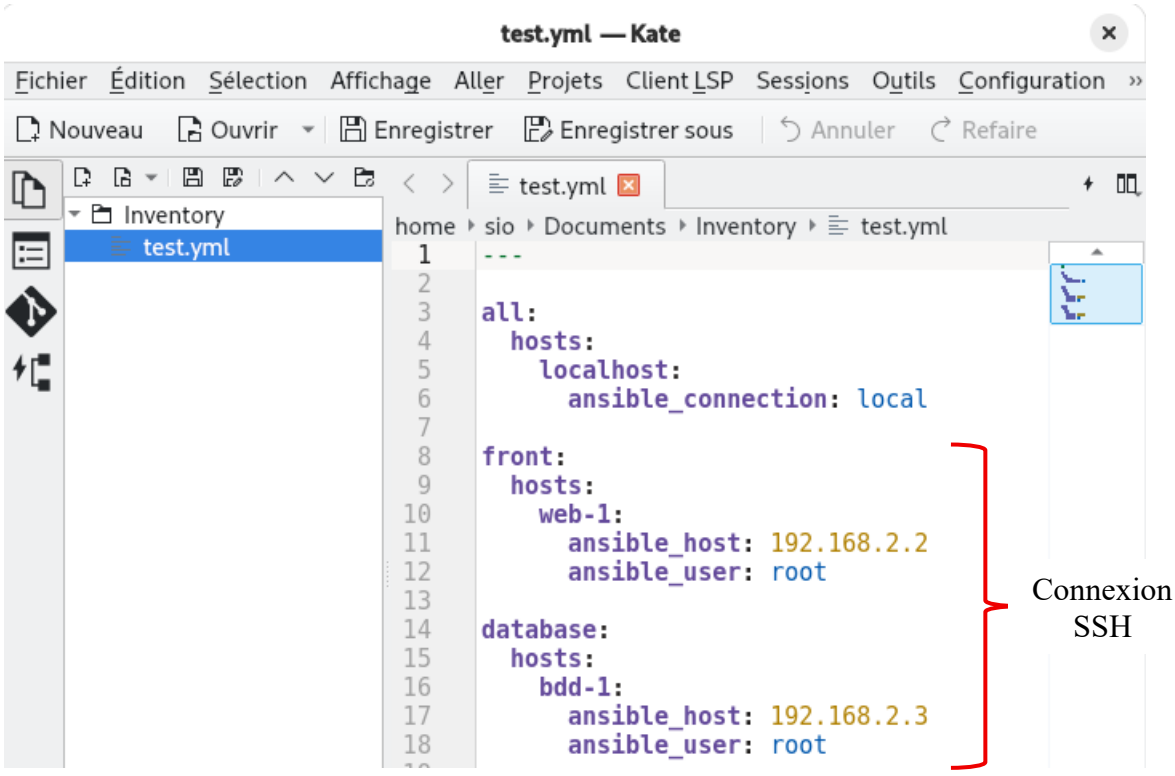
```
sio@bdd-1: ~
root@bdd-1:~# ss -antp4
State      Recv-Q     Send-Q       Local Address:Port        Peer Address:Port
Process
LISTEN     0          128                0.0.0.0:22               0.0.0.0:*
 users:(("sshd",pid=1017,fd=6))
LISTEN     0          4096             127.0.0.1:631              0.0.0.0:*
 users:(("cupsd",pid=997,fd=7))
root@bdd-1:~#
```

Fichier d'inventaire au format INI :



```
root@Ansible:~# cd /home/sio/Documents/
root@Ansible:/home/sio/Documents# ansible -i Inventory/test.inv -m debug -a var=
groups localhost
localhost | SUCCESS => {
    "groups": {
        "all": [
            "localhost",
            "web-1",
            "bdd-1"
        ],
        "database": [
            "bdd-1"
        ],
        "front": [
            "web-1"
        ],
        "ungrouped": [
            "localhost"
        ]
    }
}
```

Fichier d'inventaire au format YAML :



```
sio@Ansible: ~
root@Ansible:/home/sio/Documents# ansible -i Inventory/test.yml -m debug -a var=
groups localhost
localhost | SUCCESS => {
    "groups": {
        "all": [
            "localhost",
            "web-1",
            "bdd-1"
        ],
        "database": [
            "bdd-1"
        ],
        "front": [
            "web-1"
        ],
        "ungrouped": [
            "localhost"
        ]
    }
}
```

6. Connexion aux serveurs avec le protocole SSH

⇨ Mettre en place l'authentification par clés (nous avions vu au Chapitre 10 - Administration à distance et échanges sécurisés - qu'il était fortement recommandé de recourir à une authentification par clés plutôt que par mot de passe lors d'une connexion SSH).

Sur le **client SSH Ansible**, générez, à l'aide de la commande **ssh-keygen -b 256 -t ecdsa**, la paire de clés publique/privée de l'utilisateur en cours (root en l'occurrence) pour l'algorithme EcDSA afin de pouvoir s'authentifier sur le serveur OpenSSH. Le générateur de clés va placer les deux clés dans **$HOME/.ssh/** : une validation du fichier de sauvegarde par défaut de la clé vous est demandée (tapez **Entrée**), ainsi qu'une passphrase pour crypter la clé privée qui va être enregistrée sur la machine cliente (mettez « MaPassphrase »). Vous obtenez l'empreinte de la clé publique de l'utilisateur :

```
sio@Ansible: ~
root@Ansible:~# ssh-keygen -b 256 -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/root/.ssh/id_ecdsa):
Enter passphrase for "/root/.ssh/id_ecdsa" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_ecdsa
Your public key has been saved in /root/.ssh/id_ecdsa.pub
The key fingerprint is:
SHA256:BqjS5I4PJQyuwT74CxrzRDKRD7GLaNU6C8nPWor+pLo root@Ansible
The key's randomart image is:
+---[ECDSA 256]---+
|.                |
| +  ..           |
|* .....          |
|OOo..  .         |
|XOBo    S        |
|=@+ o  .         |
|Ooo*             |
|oXB              |
|E**o             |
+----[SHA256]-----+
root@Ansible:~#
```

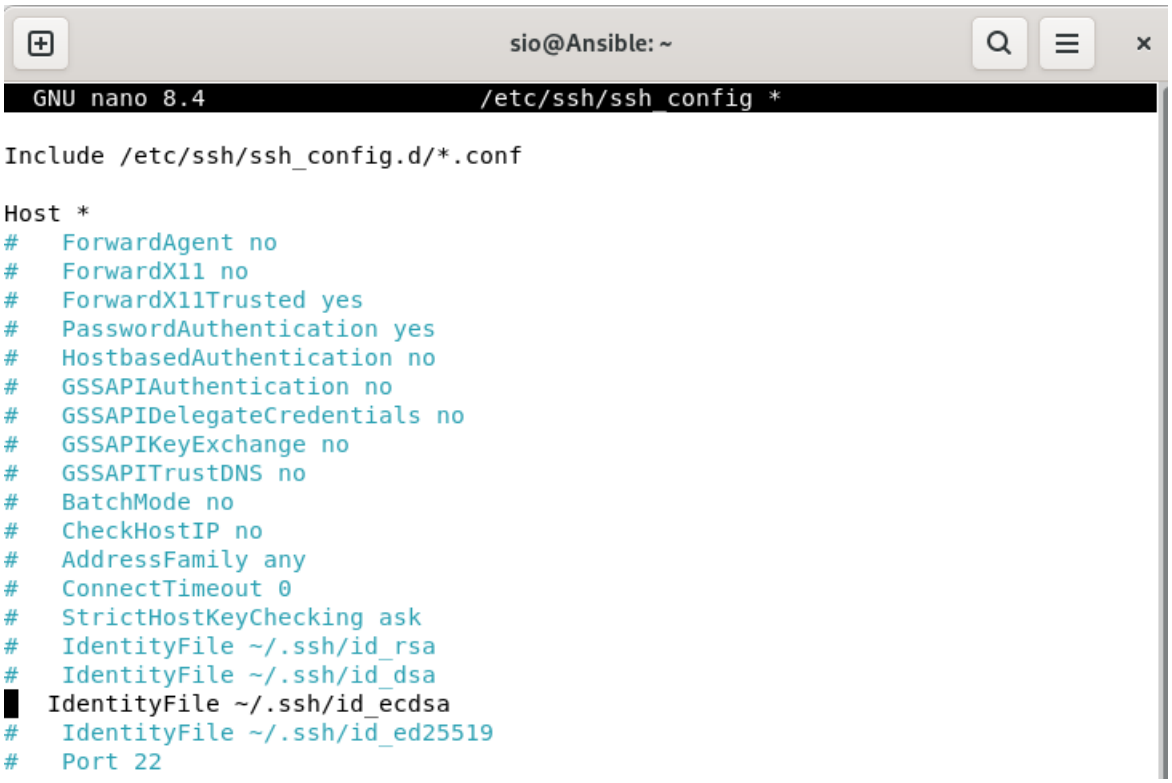
NB : la commande ssh-keygen saisie sans paramètre crée une paire de clés Ed25519 (cf. Chapitre 10).

ssh-keygen a généré deux clés :

- une **clé privée** qui est **$HOME/.ssh/id_ecdsa** à laquelle vous seul devez avoir accès ;
- une **clé publique** qui est **$HOME/.ssh/id_ecdsa.pub**, qui peut être connue par tout le monde.

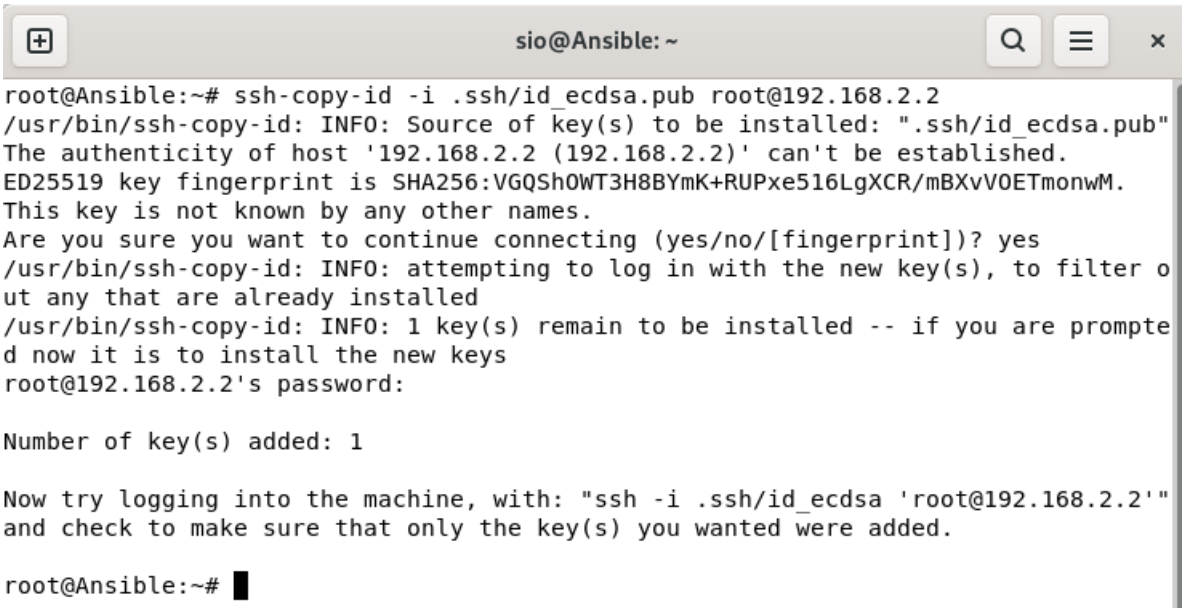
Sur les deux serveurs SSH web-1 et bdd-1, décommentez les lignes **PubkeyAuthentication yes** et **AuthorizedKeysFile** dans le fichier de configuration du démon SSH : **/etc/ssh/sshd_config** :

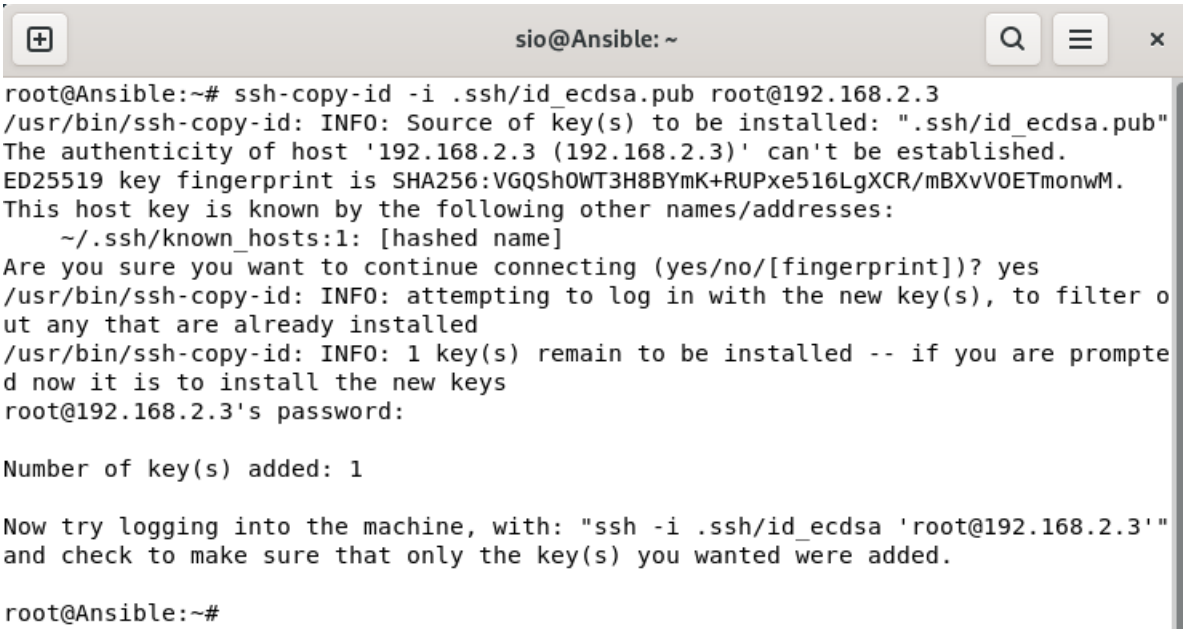
Sur le client SSH Ansible, enlevez le # de commentaire dans le fichier de configuration du client ssh (**/etc/ssh/ssh_config**) sur les lignes indiquées ci-dessous et relancez le service ssh :



Il s'agit maintenant d'envoyer, depuis le client SSH Ansible, la clé publique **id_ecdsa.pub** aux deux serveurs SSH web-1 et bdd-1.

Plutôt que de se servir de la commande **scp** et d'ajouter ensuite sur le serveur SSH web-1 la clé publique du client SSH au fichier **authorized_keys** (ou bien de réaliser un simple copier/coller permis par les additions invité), vous allez utiliser la commande spéciale **ssh-copy-id**. Le mot de passe du compte **root** du serveur vous est demandé (c'est la dernière fois) :



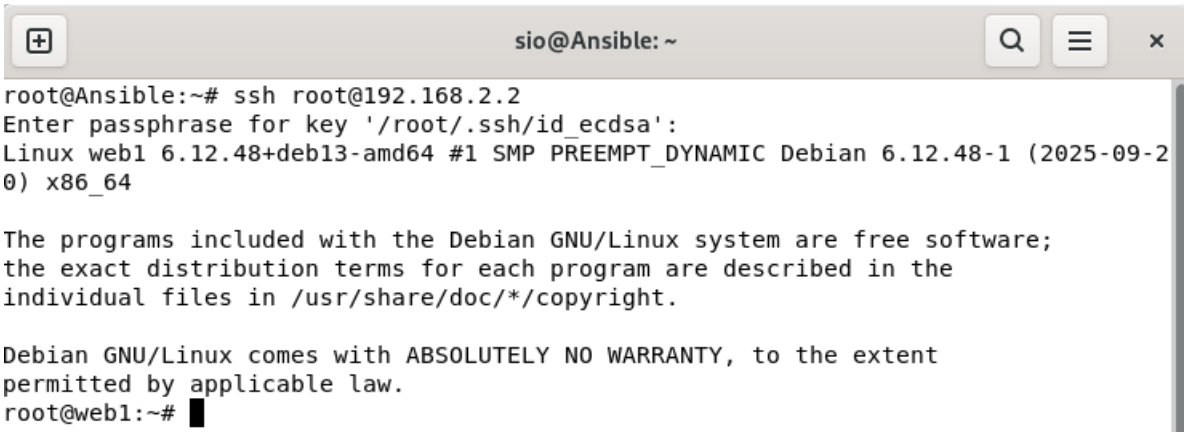


La clé publique **id_ecdsa.pub** a été envoyée aux 2 serveurs et a été automatiquement ajoutée au fichier **authorized_keys**.

Sur les serveurs SSH web-1 et bdd-1, vérifiez la présence dans le fichier **/root/.ssh/authorized_keys** de la clé publique :

Pour vérifier le bon fonctionnement de l'authentification par clés, connectez-vous ensuite à partir du client SSH Ansible au serveur SSH web-1. La passphrase mise en place pour crypter la clé privée vous est demandée afin que le client puisse résoudre le challenge.

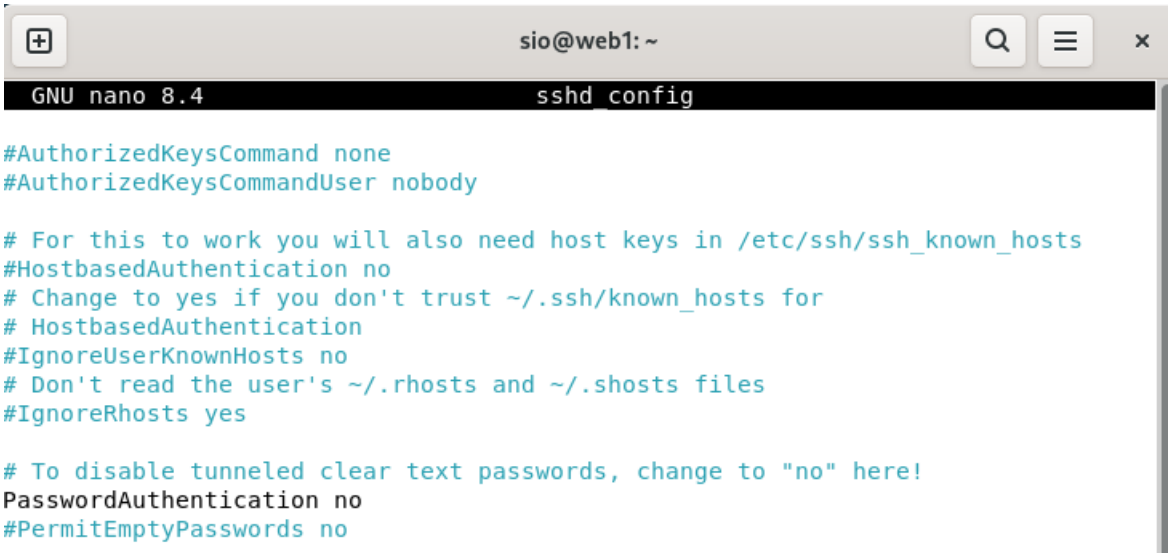
Cf. §6 Fonctionnement de l'authentification par clés de chiffrement avec OpenSSH (B3-SSH-MITM-Annexes accompagnant le Chapitre 10)

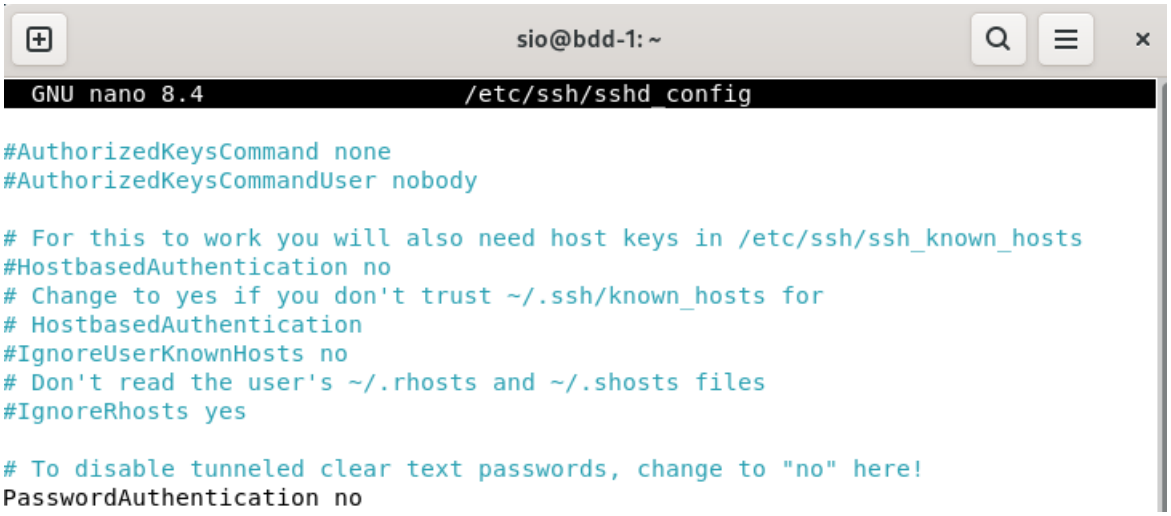


Terminez la session SSH sur le client Ansible en saisissant **exit.**

Testez également la connexion au serveur ssh bdd-1 et terminez la session en saisissant exit.

Sur les deux serveurs SSH web-1 et bdd-1, désactivez l'authentification par mot de passe pour juste conserver celle par clés dans le fichier de configuration **/etc/ssh/sshd_config.** Décommentez pour ce faire la directive **PasswordAuthentication** et affectez-lui le paramètre **no**.





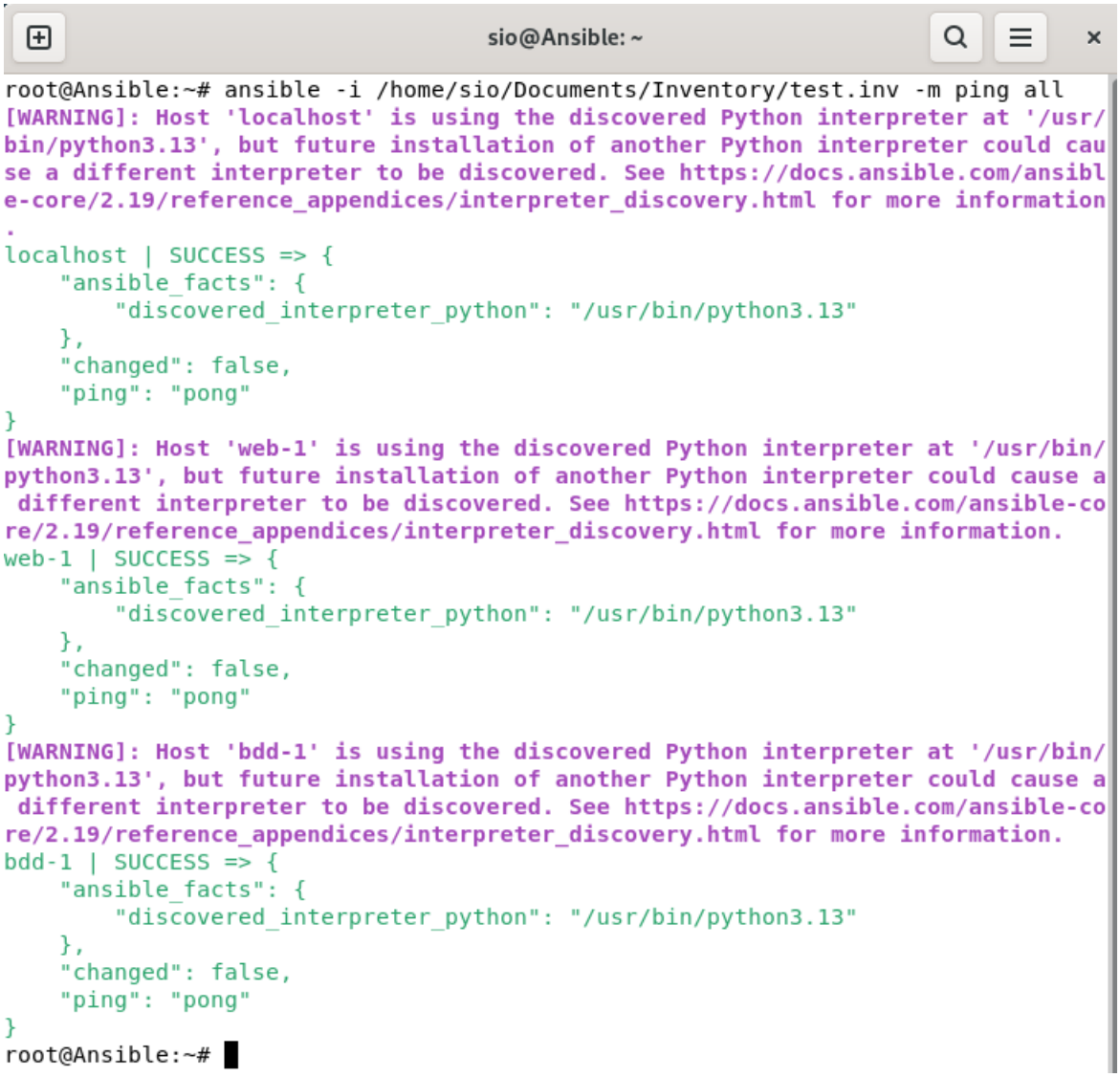
Redémarrez ensuite sur chaque machine le service SSH pour que la modification du fichier soit prise en compte.

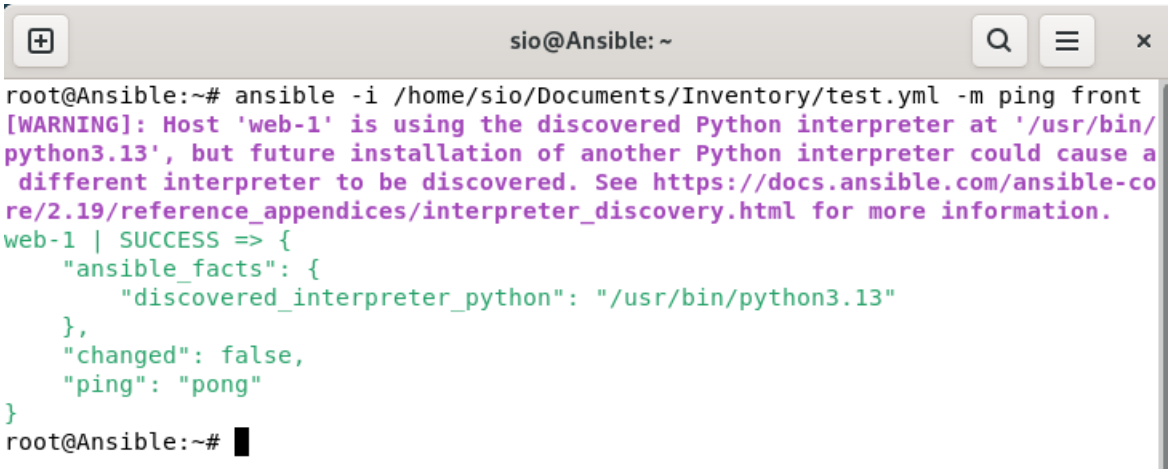
Activez l'**agent SSH** sur le client SSH Ansible (programme qui tourne en arrière-plan et qui garde en mémoire la clé privée) en saisissant les commandes **ssh-agent /bin/bash** et **ssh-add** (l'agent SSH vous demande la passphrase).

⇨ Pensez à ressaisir ces 2 commandes à chaque redémarrage de la VM Ansible.

7. Test de communication avec le module ping

Réalisez le test de communication avec les machines de l'inventaire (groupe all puis front) :

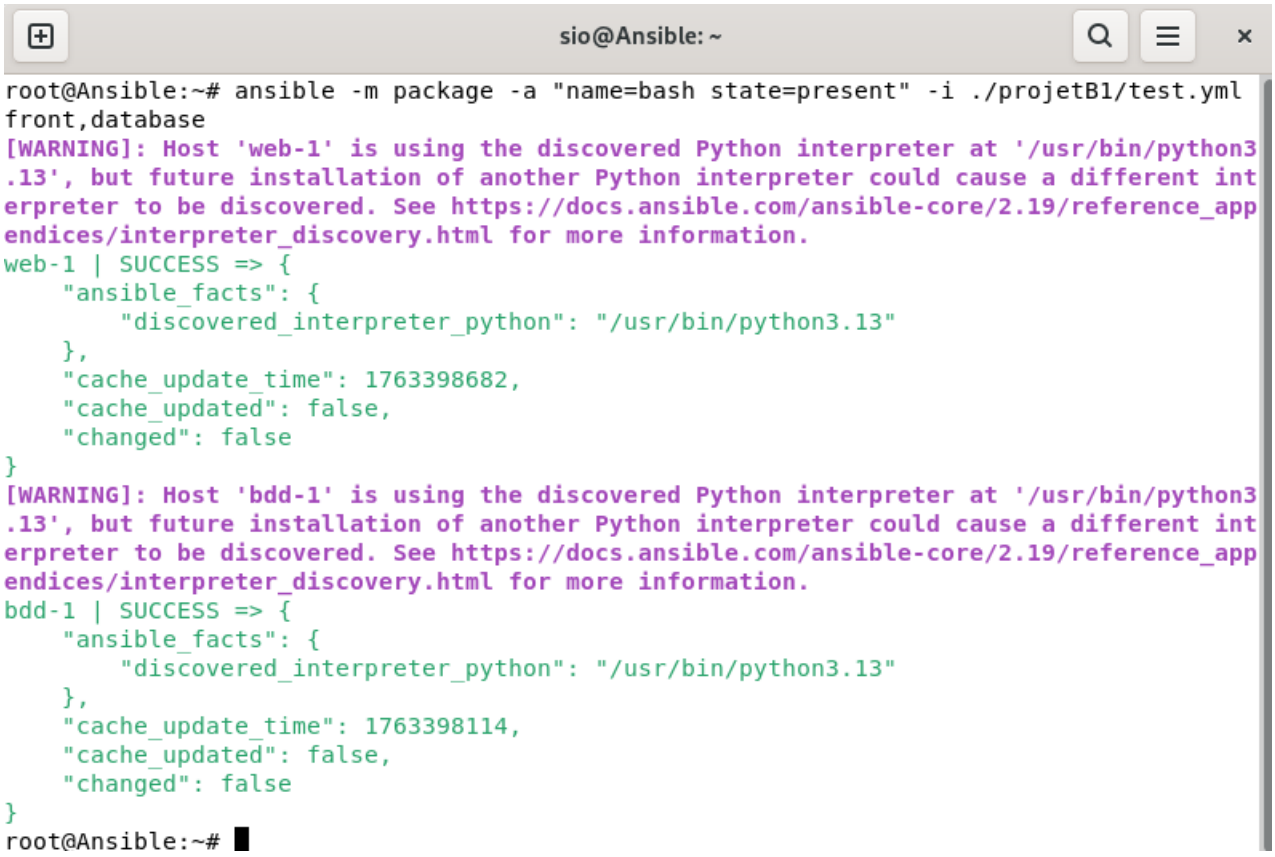




8. Installation d'un serveur Apache (en mode ad-hoc)

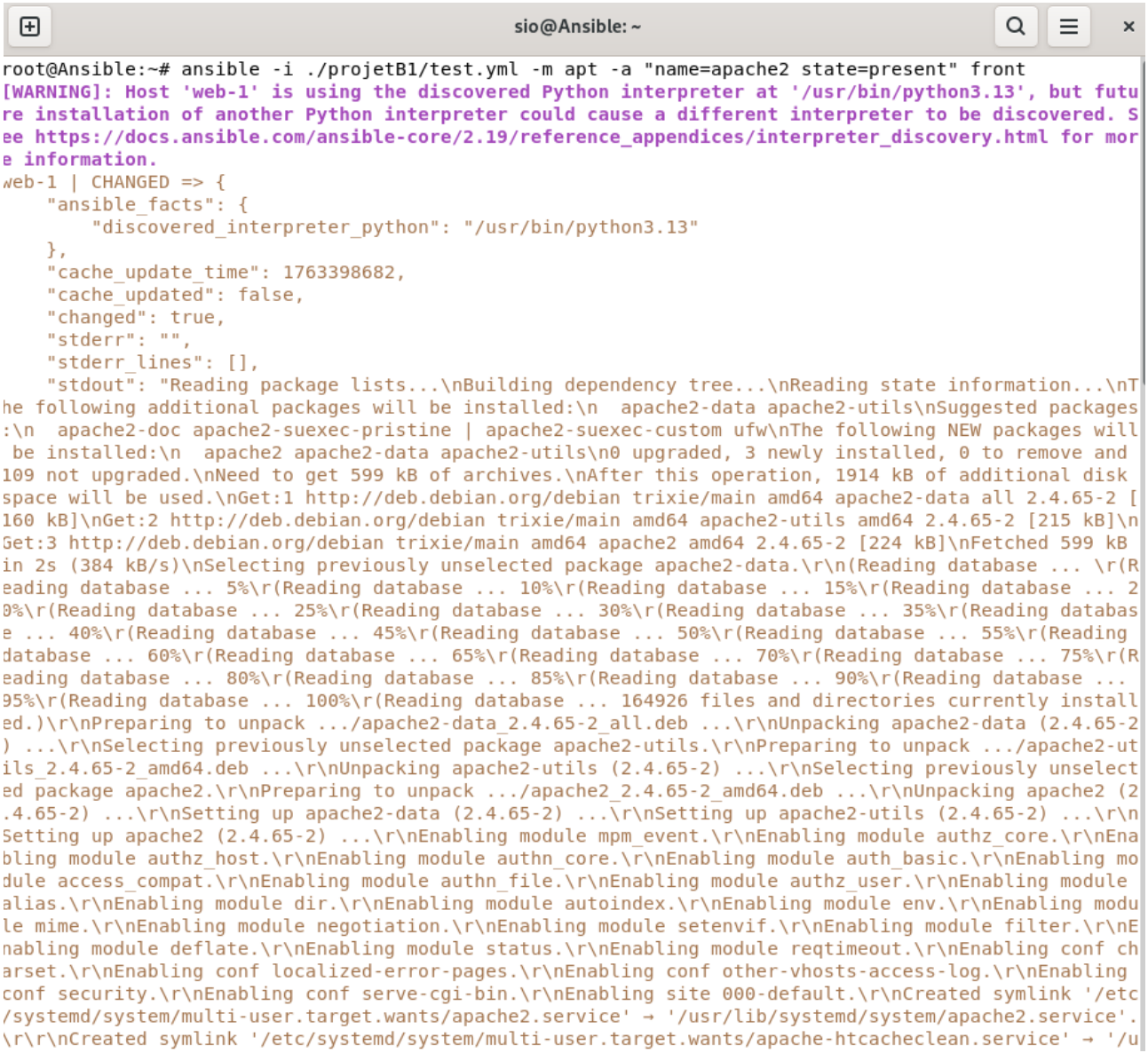
S'assurer de la présence d'un paquet (exemple bash) : module apt

Si distribution différente (Debian et Red Hat par exemple) : module package



⇨ Vérifier au préalable la résolution DNS (adresse IP du serveur DNS dans la configuration IP des VM web-1 et bdd-1 ainsi que les règles sur OPT1 de pfSense : requêtes DNS port UDP 53)

Installation du serveur Apache sur les machines du groupe front (module apt) :


sio@Ansible: ~
root@Ansible:~# ansible -i ./projetB1/test.yml -m apt -a "name=apache2 state=present" front
[WARNING]: Host 'web-1' is using the discovered Python interpreter at '/usr/bin/python3.13', but futu
re installation of another Python interpreter could cause a different interpreter to be discovered. S
ee https://docs.ansible.com/ansible-core/2.19/reference_appendices/interpreter_discovery.html for mor
e information.
web-1 | CHANGED => {
"ansible_facts": {
"discovered_interpreter_python": "/usr/bin/python3.13"
},
"cache_update_time": 1763398682,
"cache_updated": false,
"changed": true,
"stderr": "",
"stderr_lines": [],
"stdout": "Reading package lists...\nBuilding dependency tree...\nReading state information...\nT
he following additional packages will be installed:\n apache2-data apache2-utils\nSuggested packages
:\n apache2-doc apache2-suexec-pristine | apache2-suexec-custom ufw\nThe following NEW packages will
be installed:\n apache2 apache2-data apache2-utils\n0 upgraded, 3 newly installed, 0 to remove and
109 not upgraded.\nNeed to get 599 kB of archives.\nAfter this operation, 1914 kB of additional disk
space will be used.\nGet:1 http://deb.debian.org/debian trixie/main amd64 apache2-data all 2.4.65-2 [
160 kB]\nGet:2 http://deb.debian.org/debian trixie/main amd64 apache2-utils amd64 2.4.65-2 [215 kB]\n
Get:3 http://deb.debian.org/debian trixie/main amd64 apache2 amd64 2.4.65-2 [224 kB]\nFetched 599 kB
in 2s (384 kB/s)\nSelecting previously unselected package apache2-data.\r\n(Reading database ... \r(R
eading database ... 5%\r(Reading database ... 10%\r(Reading database ... 15%\r(Reading database ... 2
0%\r(Reading database ... 25%\r(Reading database ... 30%\r(Reading database ... 35%\r(Reading databas
e ... 40%\r(Reading database ... 45%\r(Reading database ... 50%\r(Reading database ... 55%\r(Reading
database ... 60%\r(Reading database ... 65%\r(Reading database ... 70%\r(Reading database ... 75%\r(R
eading database ... 80%\r(Reading database ... 85%\r(Reading database ... 90%\r(Reading database ...
95%\r(Reading database ... 100%\r(Reading database ... 164926 files and directories currently install
ed.)\r\nPreparing to unpack .../apache2-data_2.4.65-2_all.deb ...\r\nUnpacking apache2-data (2.4.65-2
) ...\r\nSelecting previously unselected package apache2-utils.\r\nPreparing to unpack .../apache2-ut
ils_2.4.65-2_amd64.deb ...\r\nUnpacking apache2-utils (2.4.65-2) ...\r\nSelecting previously unselect
ed package apache2.\r\nPreparing to unpack .../apache2_2.4.65-2_amd64.deb ...\r\nUnpacking apache2 (2
.4.65-2) ...\r\nSetting up apache2-data (2.4.65-2) ...\r\nSetting up apache2-utils (2.4.65-2) ...\r\n
Setting up apache2 (2.4.65-2) ...\r\nEnabling module mpm_event.\r\nEnabling module authz_core.\r\nEna
bling module authz_host.\r\nEnabling module authn_core.\r\nEnabling module auth_basic.\r\nEnabling mo
dule access_compat.\r\nEnabling module authn_file.\r\nEnabling module authz_user.\r\nEnabling module
alias.\r\nEnabling module dir.\r\nEnabling module autoindex.\r\nEnabling module env.\r\nEnabling modu
le mime.\r\nEnabling module negotiation.\r\nEnabling module setenvif.\r\nEnabling module filter.\r\nE
nabling module deflate.\r\nEnabling module status.\r\nEnabling module reqtimeout.\r\nEnabling conf ch
arset.\r\nEnabling conf localized-error-pages.\r\nEnabling conf other-vhosts-access-log.\r\nEnabling
conf security.\r\nEnabling conf serve-cgi-bin.\r\nEnabling site 000-default.\r\nCreated symlink '/etc
/systemd/system/multi-user.target.wants/apache2.service' → '/usr/lib/systemd/system/apache2.service'.
\r\r\nCreated symlink '/etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service' → '/u

```
sr/lib/systemd/system/apache-htcacheclean.service'.\r\r\nProcessing triggers for man-db (2.13.1-1) ..
.\r\n",
    "stdout_lines": [
        "Reading package lists...",
        "Building dependency tree...",
        "Reading state information...",
        "The following additional packages will be installed:",
        "  apache2-data apache2-utils",
        "Suggested packages:",
        "  apache2-doc apache2-suexec-pristine | apache2-suexec-custom ufw",
        "The following NEW packages will be installed:",
        "  apache2 apache2-data apache2-utils",
        "0 upgraded, 3 newly installed, 0 to remove and 109 not upgraded.",
        "Need to get 599 kB of archives.",
        "After this operation, 1914 kB of additional disk space will be used.",
        "Get:1 http://deb.debian.org/debian trixie/main amd64 apache2-data all 2.4.65-2 [160 kB]",
        "Get:2 http://deb.debian.org/debian trixie/main amd64 apache2-utils amd64 2.4.65-2 [215 kB]",
        "Get:3 http://deb.debian.org/debian trixie/main amd64 apache2 amd64 2.4.65-2 [224 kB]",
        "Fetched 599 kB in 2s (384 kB/s)",
        "Selecting previously unselected package apache2-data.",
        "(Reading database ... ",
        "(Reading database ... 5%",
        "(Reading database ... 10%",
        "(Reading database ... 15%",
        "(Reading database ... 20%",
        "(Reading database ... 25%",
        "(Reading database ... 30%",
        "(Reading database ... 35%",
        "(Reading database ... 40%",
        "(Reading database ... 45%",
        "(Reading database ... 50%",
        "(Reading database ... 55%",
        "(Reading database ... 60%",
        "(Reading database ... 65%",
        "(Reading database ... 70%",
        "(Reading database ... 75%",
        "(Reading database ... 80%",
        "(Reading database ... 85%",
        "(Reading database ... 90%",
        "(Reading database ... 95%",
        "(Reading database ... 100%",
        "(Reading database ... 164926 files and directories currently installed.)",
        "Preparing to unpack .../apache2-data_2.4.65-2_all.deb ...",
        "Unpacking apache2-data (2.4.65-2) ...",
```

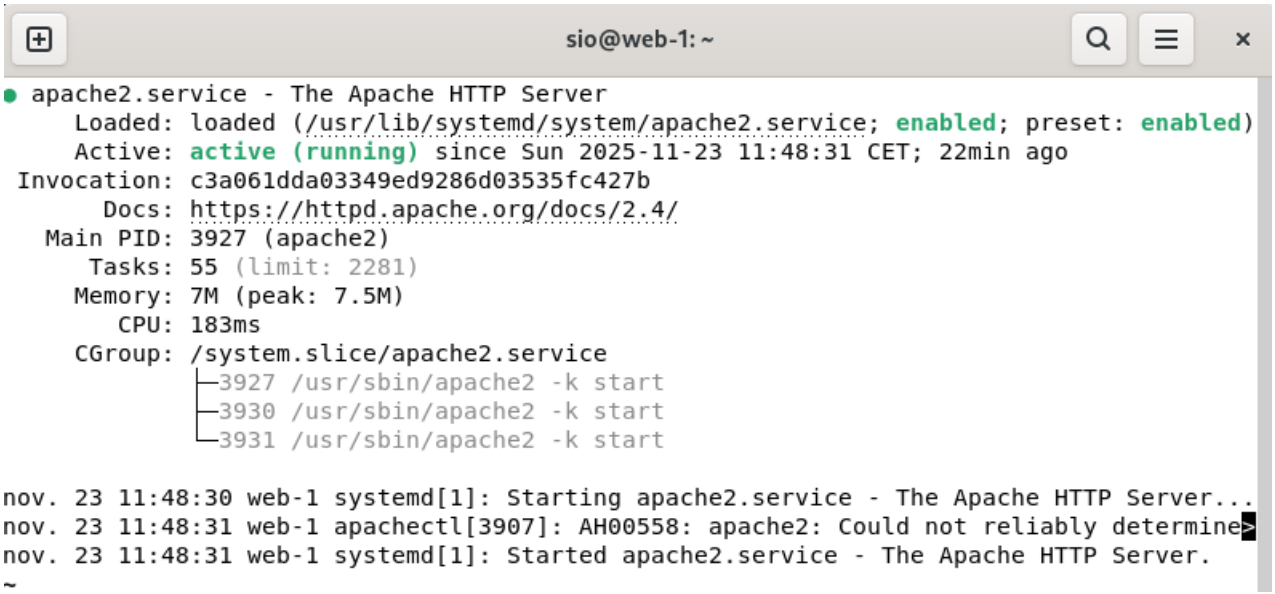
```
        "Selecting previously unselected package apache2-utils.",
        "Preparing to unpack .../apache2-utils_2.4.65-2_amd64.deb ...",
        "Unpacking apache2-utils (2.4.65-2) ...",
        "Selecting previously unselected package apache2.",
        "Preparing to unpack .../apache2_2.4.65-2_amd64.deb ...",
        "Unpacking apache2 (2.4.65-2) ...",
        "Setting up apache2-data (2.4.65-2) ...",
        "Setting up apache2-utils (2.4.65-2) ...",
        "Setting up apache2 (2.4.65-2) ...",
        "Enabling module mpm_event.",
        "Enabling module authz_core.",
        "Enabling module authz_host.",
        "Enabling module authn_core.",
        "Enabling module auth_basic.",
        "Enabling module access_compat.",
        "Enabling module authn_file.",
        "Enabling module authz_user.",
        "Enabling module alias.",
        "Enabling module dir.",
        "Enabling module autoindex.",
        "Enabling module env.",
        "Enabling module mime.",
        "Enabling module negotiation.",
        "Enabling module setenvif.",
        "Enabling module filter.",
        "Enabling module deflate.",
        "Enabling module status.",
        "Enabling module reqtimeout.",
        "Enabling conf charset.",
        "Enabling conf localized-error-pages.",
        "Enabling conf other-vhosts-access-log.",
        "Enabling conf security.",
        "Enabling conf serve-cgi-bin.",
        "Enabling site 000-default.",
        "Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' → '/usr/lib/sy
stemd/system/apache2.service'.",
        "",
        "Created symlink '/etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service' →
'/usr/lib/systemd/system/apache-htcacheclean.service'.",
        "",
        "Processing triggers for man-db (2.13.1-1) ..."
    ]
}
root@Ansible:~#
```

Fichier de configuration .ansible.cfg à créer dans le répertoire personnel pour évincer le Warning :

```
sio@Ansible: ~
  GNU nano 8.4                        .ansible.cfg *
[defaults]
interpreter_python=auto_silent
```

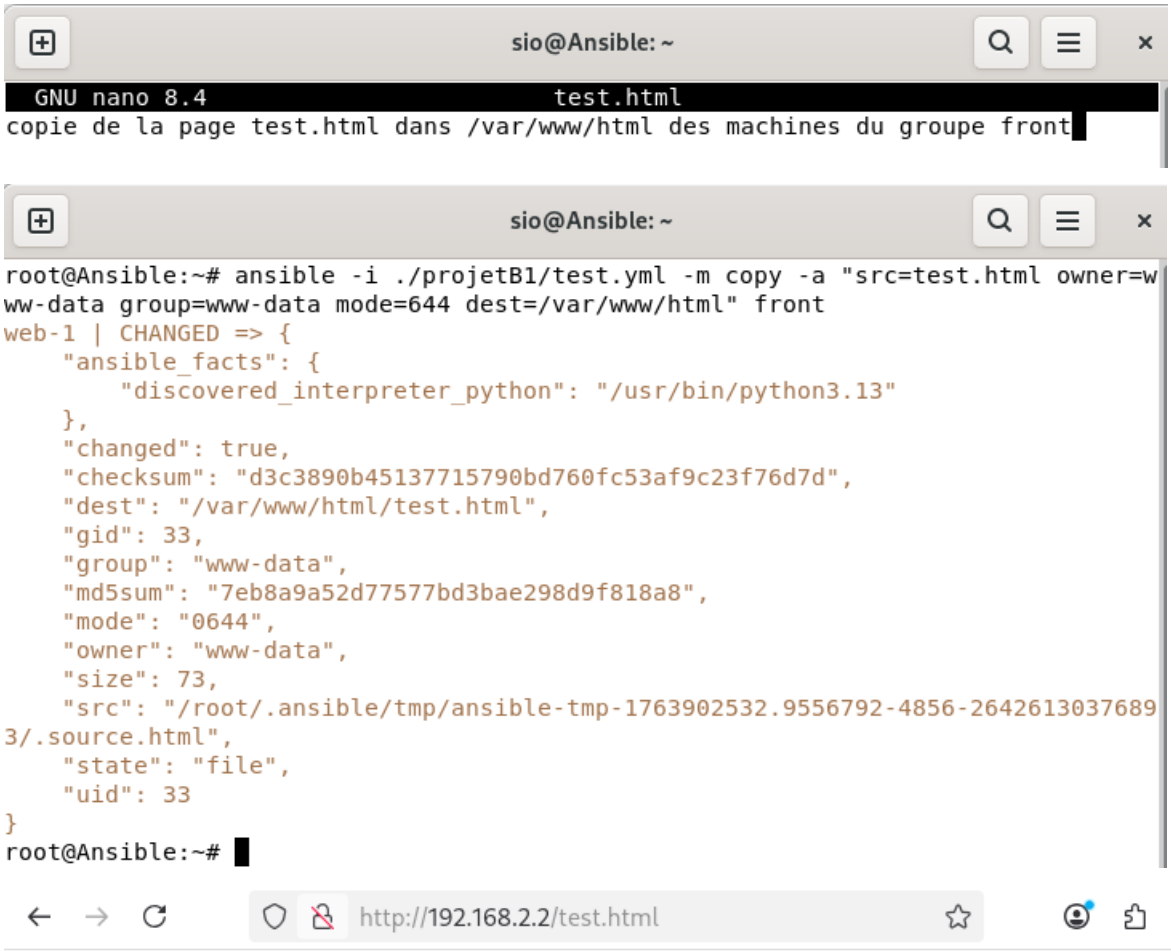
```
sio@Ansible: ~
root@Ansible:~# ansible -i ./projetB1/test.yml -m apt -a "name=apache2 state=present" front
web-1 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3.13"
    },
    "cache_update_time": 1763897039,
    "cache_updated": false,
    "changed": false
}
root@Ansible:~#
```

Systemctl status apache2 sur la VM web-1 :



Test depuis la VM Ansible :

Page test.html à créer pour la copier dans le répertoire de publication avec Ansible (module copy) :



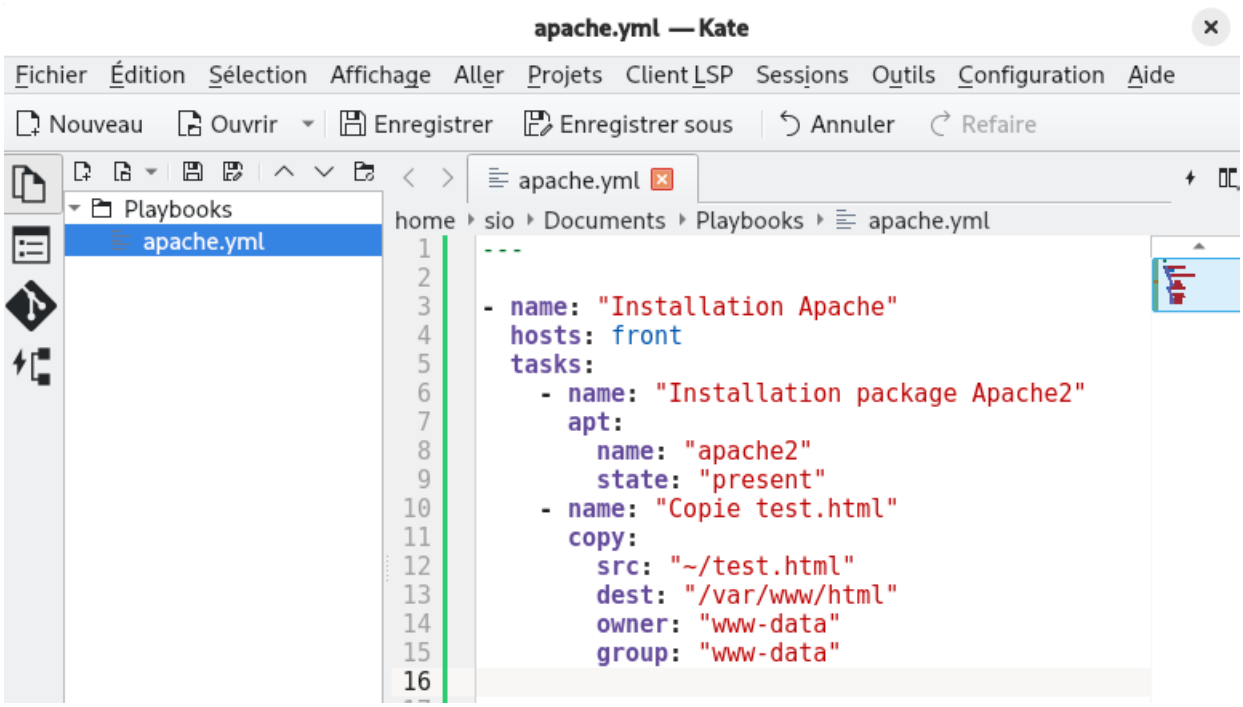
9. Premier playbook

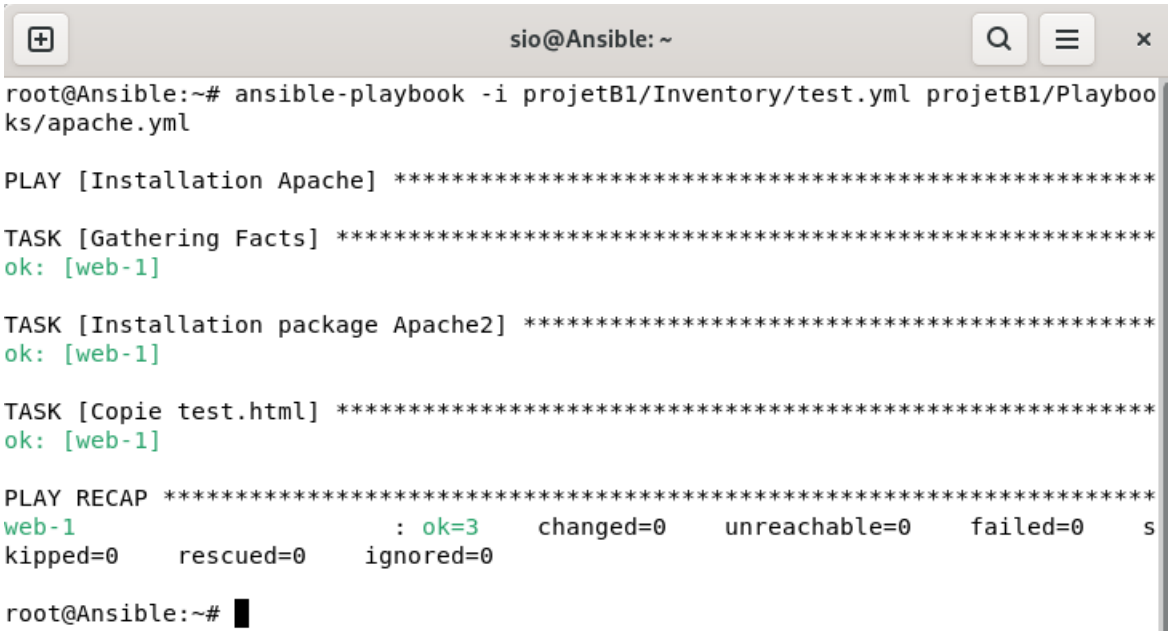
Un playbook est un fichier au format YAML qui va lister un ensemble d'opérations.

Structure d'un playbook :

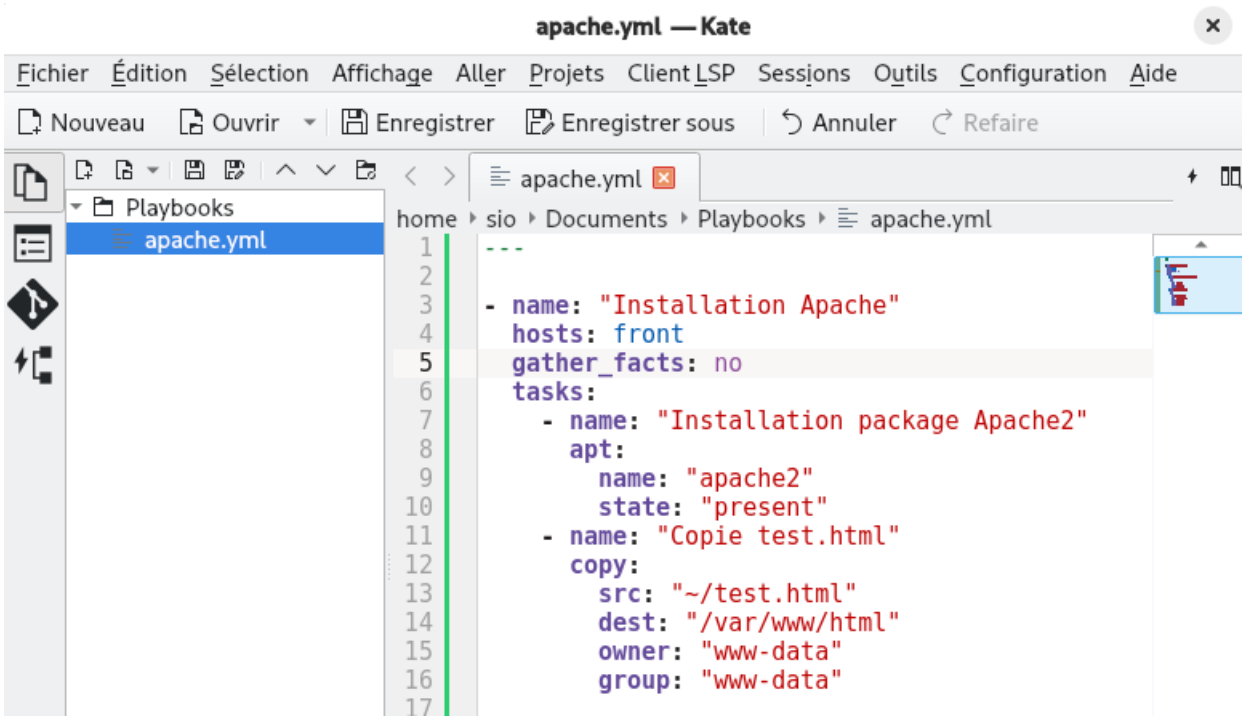
- Un fichier yaml démarre par 3 tirets ;
- le nom du playbook (champ name) ;
- La liste des machines concernées (champ hosts) ;
- La gestion du lancement de la collecte des informations (module setup) concernant la machine (champ gather_facts) ;
- la liste des opérations à effectuer (tasks).

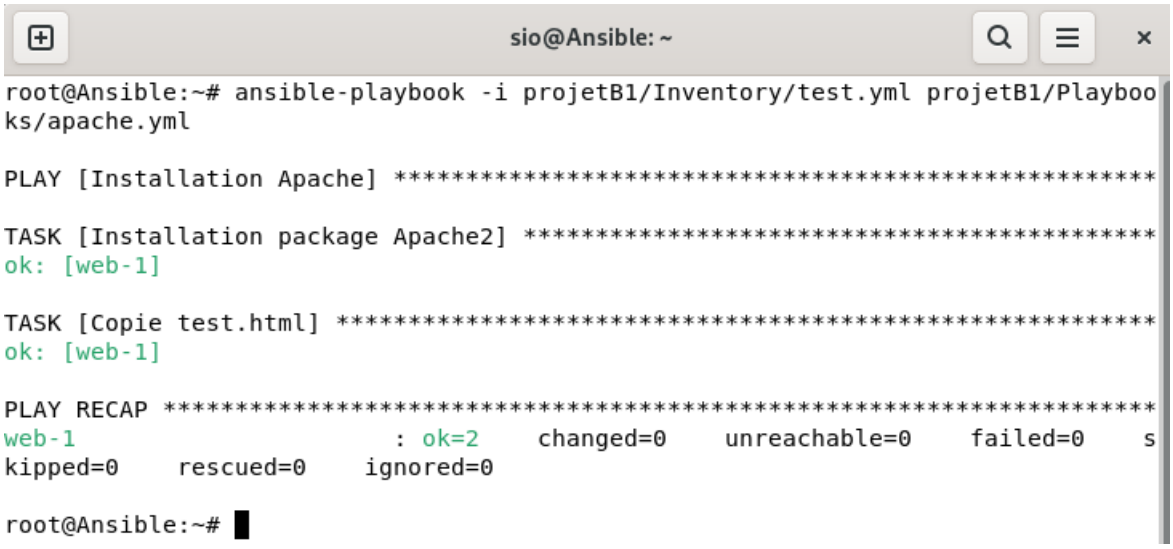
Playbook apache.yml : modules apt et copy





⇨ Pas de récupération des informations concernant les machines (gather_facts : no) :

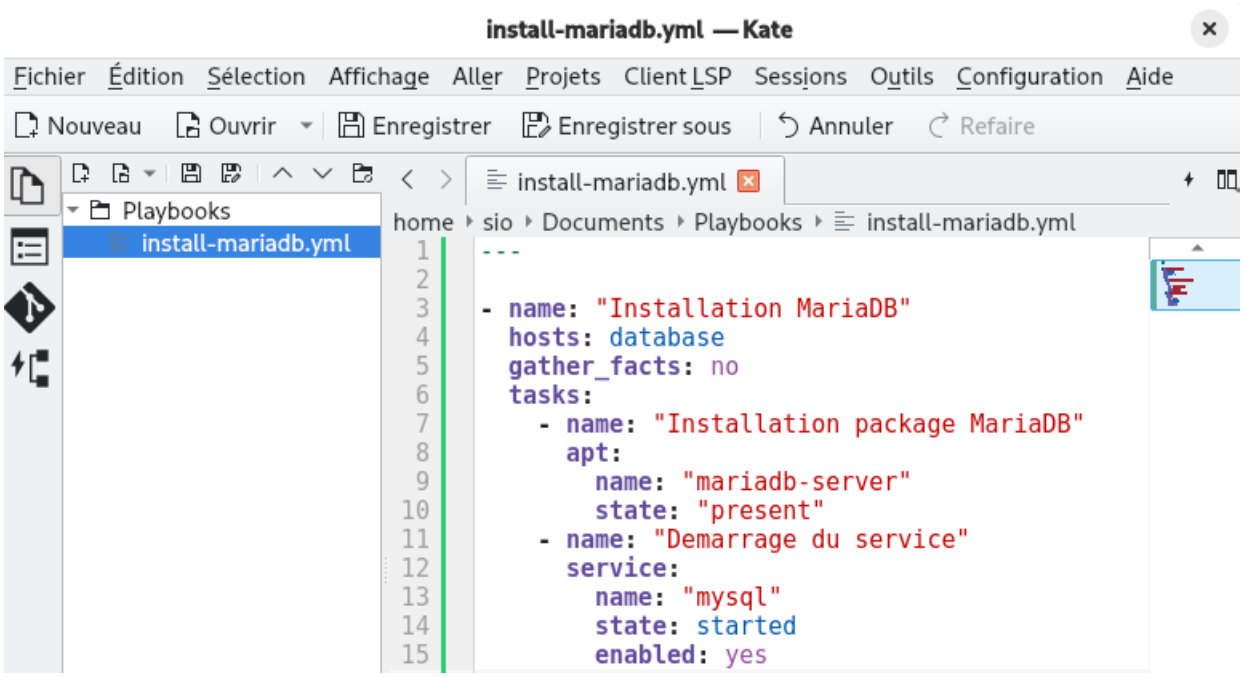


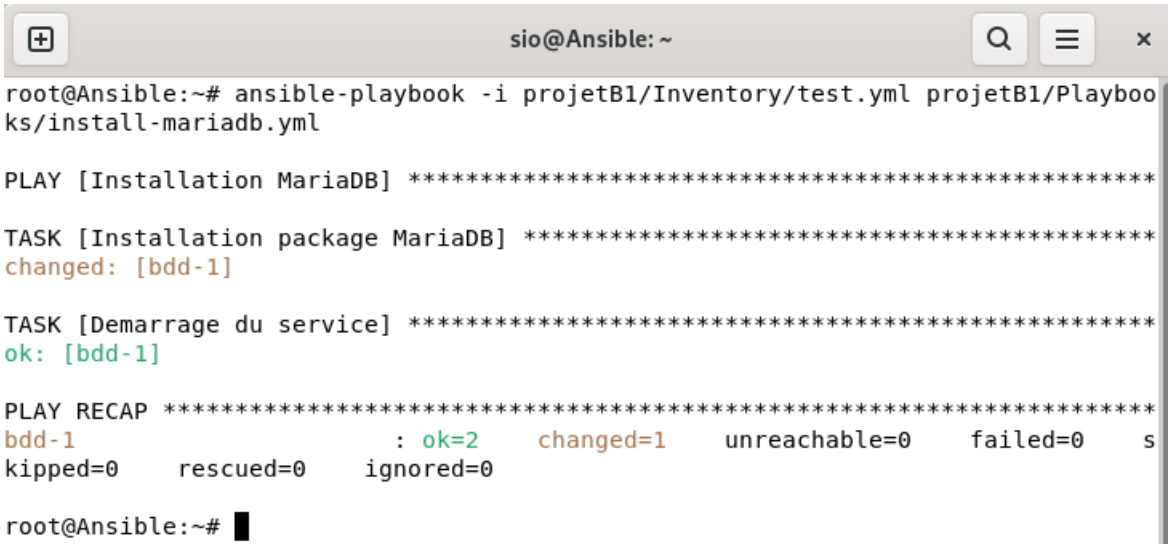


10. Installation d'un serveur MariaDB

⇨ Installation du serveur MariaDB sur les machines du groupe database :

Playbook install-mariadb.yml : modules apt et service





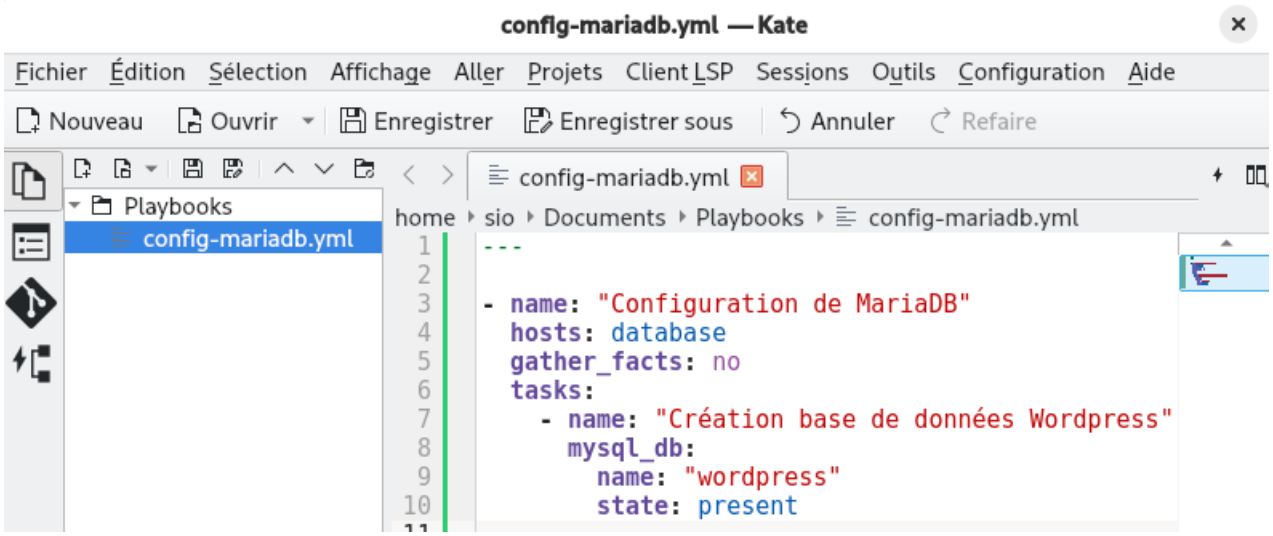
Vérification sur la VM bdd-1 :

```
sio@bdd-1: ~
root@bdd-1:~# ss -antp4
State      Recv-Q     Send-Q          Local Address:Port           Peer Address:Port
Process
LISTEN     0          128                0.0.0.0:22                  0.0.0.0:*
 users:(("sshd",pid=1013,fd=6))
LISTEN     0          4096             127.0.0.1:631                 0.0.0.0:*
 users:(("cupsd",pid=991,fd=7))
LISTEN     0          80               127.0.0.1:3306                0.0.0.0:*
 users:(("mariadbd",pid=4482,fd=28))
root@bdd-1:~# systemctl status mariadb
● mariadb.service - MariaDB 11.8.3 database server
     Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-11-23 17:07:20 CET; 8min ago
 Invocation: 212b52d8086042d599fb20d395a4e7f3
       Docs: man:mariadbd(8)
             https://mariadb.com/kb/en/library/systemd/
   Main PID: 4482 (mariadbd)
     Status: "Taking your SQL requests now..."
      Tasks: 9 (limit: 15060)
     Memory: 121.6M (peak: 126.4M)
        CPU: 1.920s
     CGroup: /system.slice/mariadb.service
             └─4482 /usr/sbin/mariadbd
```

11. Configuration de la base de données

⇨ Création de la base de données wordpress

Playbook config-mariadb.yml : module mysql_db



```
sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Playbo
oks/config-mariadb.yml

PLAY [Configuration de MariaDB] ************************************************

TASK [Création base de données Wordpress] **************************************
[ERROR]: Task failed: Module failed: A MySQL module is required: for Python 2.7 eit
her PyMySQL, or MySQL-python, or for Python 3.X mysqlclient or PyMySQL. Consider se
tting ansible_python_interpreter to use the intended Python version.
Origin: /root/projetB1/Playbooks/config-mariadb.yml:7:7

5   gather_facts: no
6   tasks:
7     - name: "Création base de données Wordpress"
        ^ column 7

fatal: [bdd-1]: FAILED! => {"ansible_facts": {"discovered_interpreter_python": "/us
r/bin/python3.13"}, "changed": false, "msg": "A MySQL module is required: for Pytho
n 2.7 either PyMySQL, or MySQL-python, or for Python 3.X mysqlclient or PyMySQL. Co
nsider setting ansible_python_interpreter to use the intended Python version."}

PLAY RECAP *********************************************************************
bdd-1                      : ok=0    changed=0    unreachable=0    failed=1    skip
ped=0    rescued=0    ignored=0

root@Ansible:~#
```

⇨ Installation du module avant la création de la base de données :

config-mariadb.yml — Kate

Fichier Édition Sélection Affichage Aller Projets Client LSP Sessions Outils Configuration Aide

Nouveau Ouvrir Enregistrer Enregistrer sous Annuler Refaire

Playbooks
config-mariadb.yml

config-mariadb.yml

home ▸ sio ▸ Documents ▸ Playbooks ▸ config-mariadb.yml

```yaml
---

- name: "Configuration de MariaDB"
  hosts: database
  gather_facts: no
  tasks:
    - name: "Installation module MySQL-python"
      apt:
        name: "python3-mysqldb"
        state: present
    - name: "Création base de données Wordpress"
      mysql_db:
        name: "wordpress"
        state: present
```

```
sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Playbo
oks/config-mariadb.yml

PLAY [Configuration de MariaDB] ************************************************

TASK [Installation module MySQL-python] ****************************************
changed: [bdd-1]

TASK [Création base de données Wordpress] **************************************
[WARNING]: Support of mysqlcline/MySQLdb connector is deprecated. We'll stop testin
g against it in collection version 4.0.0 and remove the related code in 5.0.0. Use
PyMySQL connector instead.
changed: [bdd-1]

PLAY RECAP *********************************************************************
bdd-1                      : ok=2    changed=2    unreachable=0    failed=0    skip
ped=0    rescued=0    ignored=0

root@Ansible:~#
```

⇨ Création de l'utilisateur SQL « wordpress » et octroi des droits sur les tables de la base de données wordpress à l'utilisateur wordpress : module mysql_user

config-mariadb.yml * — Kate

Fichier Édition Sélection Affichage Aller Projets Client LSP Sessions Outils Configuration Aide

Nouveau Ouvrir Enregistrer Enregistrer sous Annuler Refaire

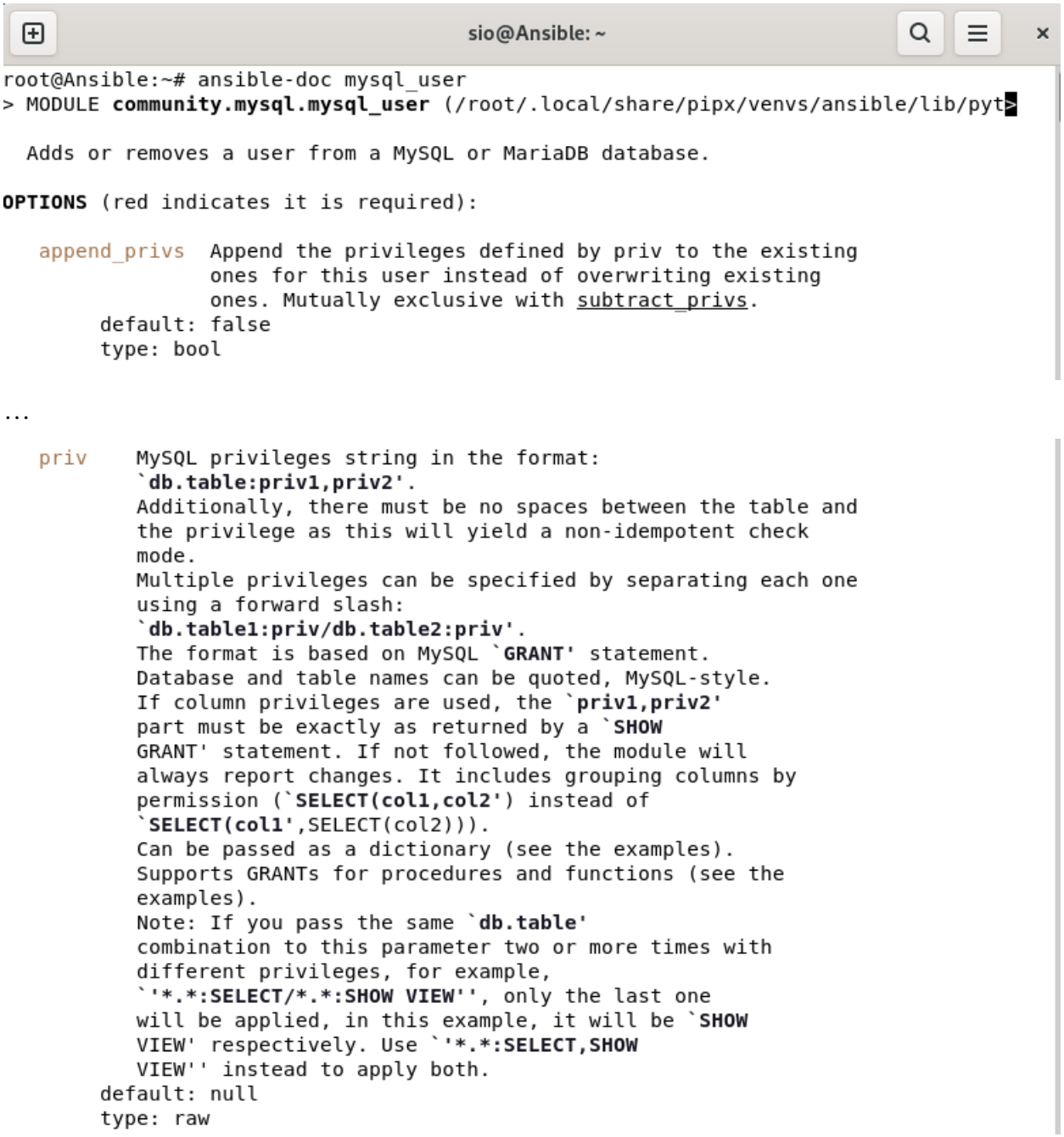
Playbooks
config-mariadb.yml

config-mariadb.yml

home ▸ sio ▸ Documents ▸ Playbooks ▸ config-mariadb.yml

```yaml
---

- name: "Configuration de MariaDB"
  hosts: database
  gather_facts: no
  tasks:
    - name: "Installation module MySQL-python"
      apt:
        name: "python3-mysqldb"
        state: present
    - name: "Création base de données Wordpress"
      mysql_db:
        name: "wordpress"
        state: present
    - name: "Création utilisateur"
      mysql_user:
        name: "wordpress"
        password: "wordpress"
        priv: "wordpress.*:ALL"
        state: present
```

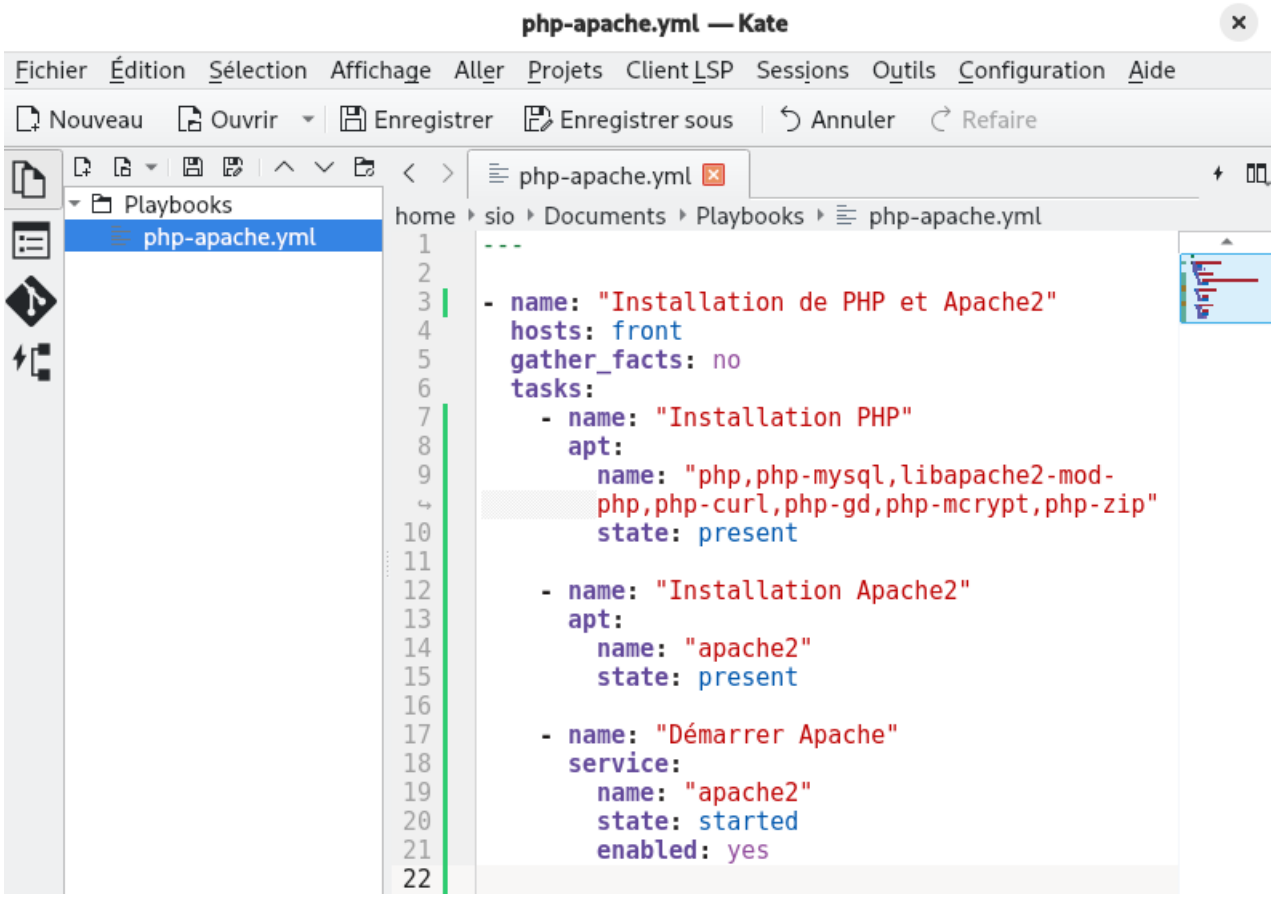
⇨ Documentation sur le module mysql_user (les options) :


sio@Ansible: ~
root@Ansible:~# ansible-doc mysql_user
> MODULE community.mysql.mysql_user (/root/.local/share/pipx/venvs/ansible/lib/pyt
Adds or removes a user from a MySQL or MariaDB database.
OPTIONS (red indicates it is required):
append_privs Append the privileges defined by priv to the existing
ones for this user instead of overwriting existing
ones. Mutually exclusive with subtract_privs.
default: false
type: bool
...
priv MySQL privileges string in the format:
`db.table:priv1,priv2'.
Additionally, there must be no spaces between the table and
the privilege as this will yield a non-idempotent check
mode.
Multiple privileges can be specified by separating each one
using a forward slash:
`db.table1:priv/db.table2:priv'.
The format is based on MySQL `GRANT' statement.
Database and table names can be quoted, MySQL-style.
If column privileges are used, the `priv1,priv2'
part must be exactly as returned by a `SHOW
GRANT' statement. If not followed, the module will
always report changes. It includes grouping columns by
permission (`SELECT(col1,col2') instead of
`SELECT(col1',SELECT(col2))).
Can be passed as a dictionary (see the examples).
Supports GRANTs for procedures and functions (see the
examples).
Note: If you pass the same `db.table'
combination to this parameter two or more times with
different privileges, for example,
`'*.*:SELECT/*.*:SHOW VIEW'', only the last one
will be applied, in this example, it will be `SHOW
VIEW' respectively. Use `'*.*:SELECT,SHOW
VIEW'' instead to apply both.
default: null
type: raw

```
sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Playb
ooks/config-mariadb.yml

PLAY [Configuration de MariaDB] ************************************************

TASK [Installation module MySQL-python] ****************************************
ok: [bdd-1]

TASK [Création base de données Wordpress] **************************************
[WARNING]: Support of mysqlcline/MySQLdb connector is deprecated. We'll stop testi
ng against it in collection version 4.0.0 and remove the related code in 5.0.0. Us
e PyMySQL connector instead.
ok: [bdd-1]

TASK [Création utilisateur] ****************************************************
[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 c
ommunity.mysql 4.0.0.
changed: [bdd-1]

PLAY RECAP *********************************************************************
bdd-1                      : ok=3    changed=1    unreachable=0    failed=0    ski
pped=0    rescued=0    ignored=0

root@Ansible:~#
```

12. Installation d'un serveur PHP

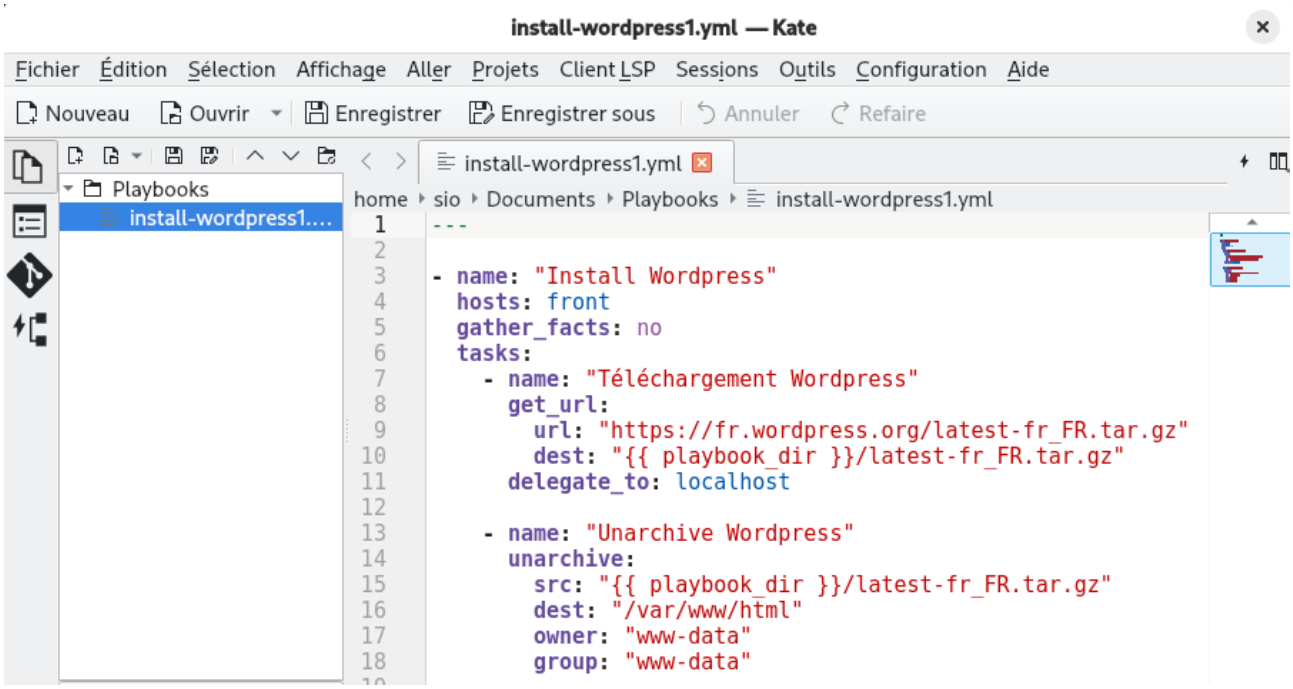
Playbook php.yml : modules apt et service



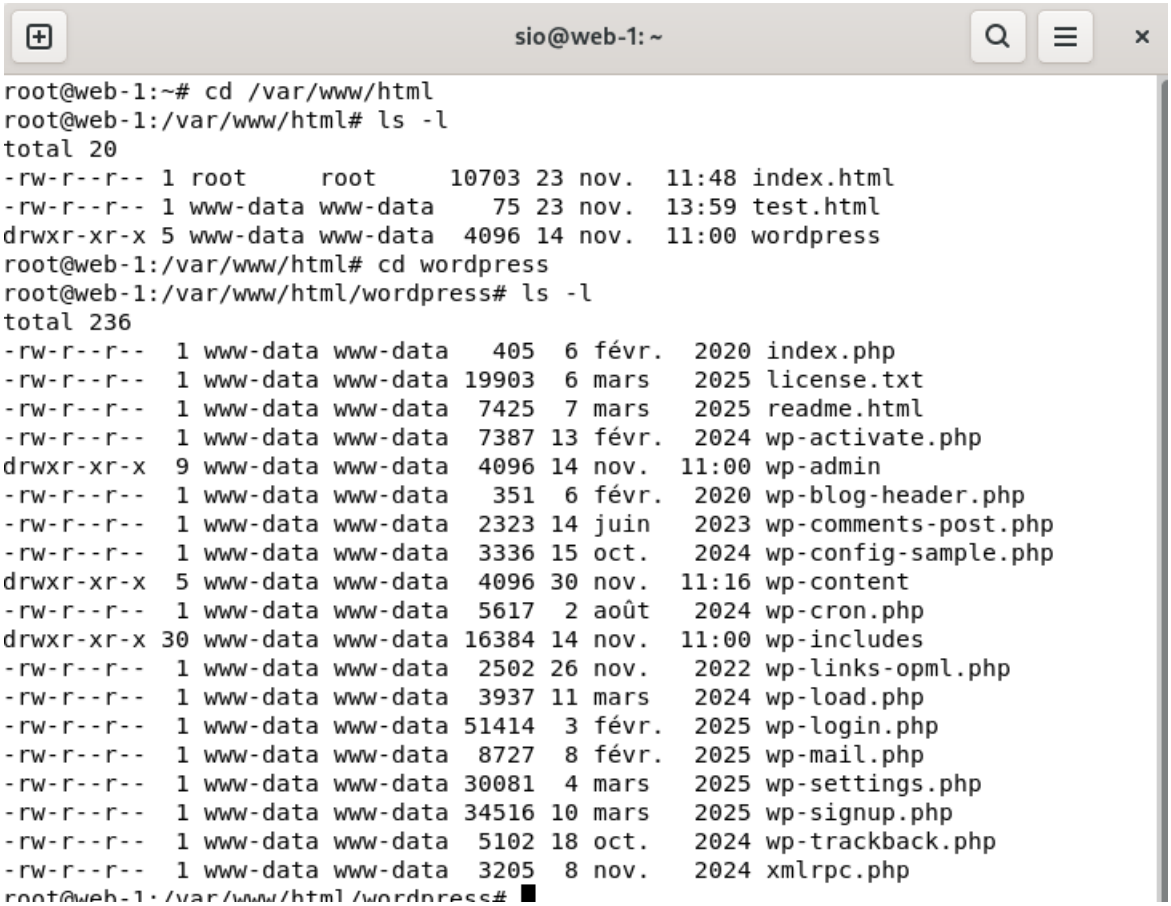
```
sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Pla
ybooks/php-apache.yml

PLAY [Installation de PHP et Apache2] ************************************

TASK [Installation PHP] **************************************************
changed: [web-1]

TASK [Installation Apache2] **********************************************
ok: [web-1]

TASK [Démarrer Apache] ***************************************************
ok: [web-1]

PLAY RECAP ***************************************************************
web-1                      : ok=3    changed=1    unreachable=0    failed=0    s
kipped=0    rescued=0    ignored=0

root@Ansible:~#
```

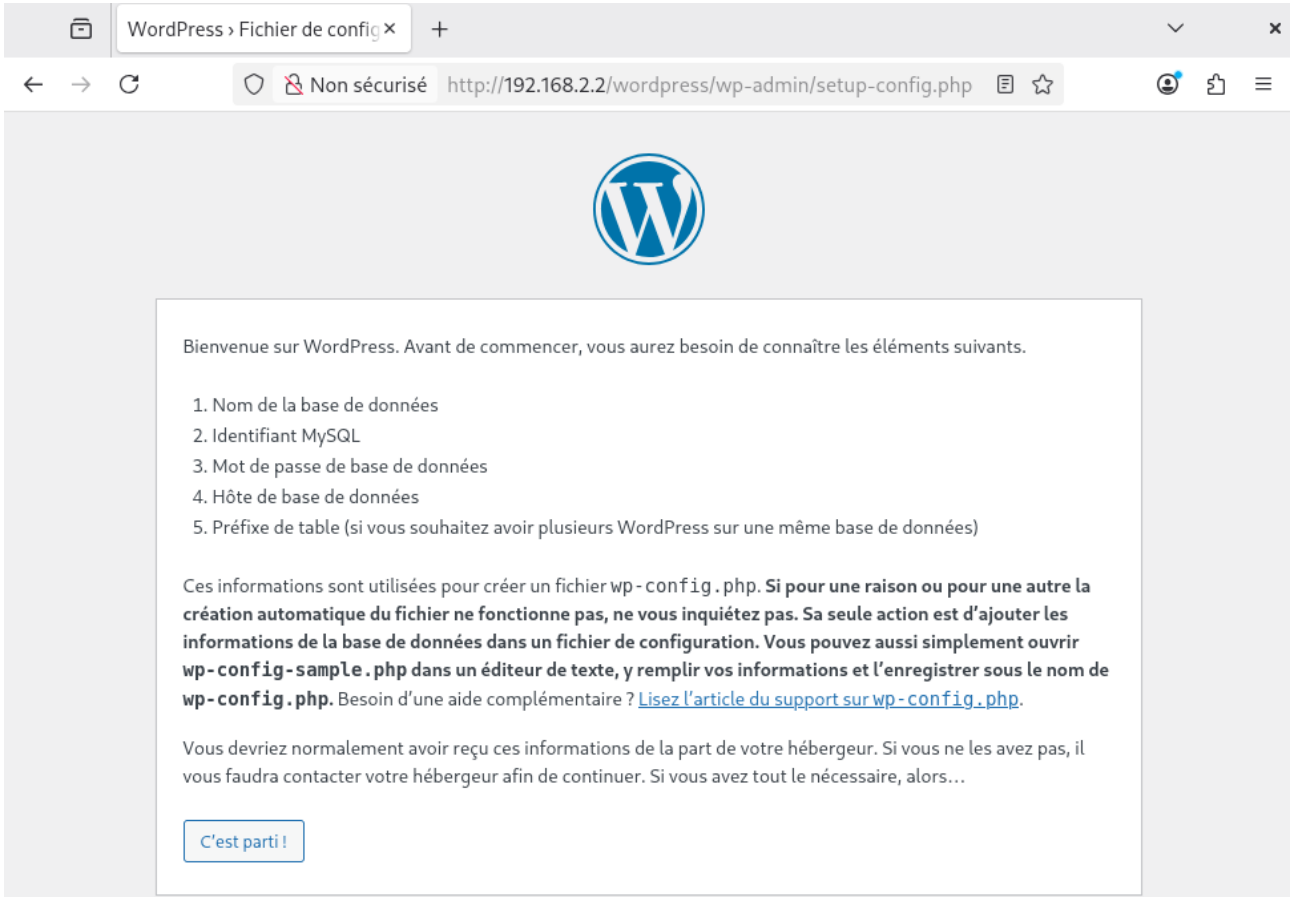
13. Installation de Wordpress

Playbook install-wordpress1.yml : modules get_url et unarchive




sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Pl
aybooks/install-wordpress1.yml
PLAY [Install Wordpress] **
*
TASK [Téléchargement Wordpress] ***
*
ok: [web-1 -> localhost]
TASK [Unarchive Wordpress] **
*
changed: [web-1]
PLAY RECAP **
*
web-1 : ok=2 changed=1 unreachable=0 failed=0
skipped=0 rescued=0 ignored=0
root@Ansible:~#


sio@web-1: ~
root@web-1:~# cd /var/www/html
root@web-1:/var/www/html# ls -l
total 20
-rw-r--r-- 1 root root 10703 23 nov. 11:48 index.html
-rw-r--r-- 1 www-data www-data 75 23 nov. 13:59 test.html
drwxr-xr-x 5 www-data www-data 4096 14 nov. 11:00 wordpress
root@web-1:/var/www/html# cd wordpress
root@web-1:/var/www/html/wordpress# ls -l
total 236
-rw-r--r-- 1 www-data www-data 405 6 févr. 2020 index.php
-rw-r--r-- 1 www-data www-data 19903 6 mars 2025 license.txt
-rw-r--r-- 1 www-data www-data 7425 7 mars 2025 readme.html
-rw-r--r-- 1 www-data www-data 7387 13 févr. 2024 wp-activate.php
drwxr-xr-x 9 www-data www-data 4096 14 nov. 11:00 wp-admin
-rw-r--r-- 1 www-data www-data 351 6 févr. 2020 wp-blog-header.php
-rw-r--r-- 1 www-data www-data 2323 14 juin 2023 wp-comments-post.php
-rw-r--r-- 1 www-data www-data 3336 15 oct. 2024 wp-config-sample.php
drwxr-xr-x 5 www-data www-data 4096 30 nov. 11:16 wp-content
-rw-r--r-- 1 www-data www-data 5617 2 août 2024 wp-cron.php
drwxr-xr-x 30 www-data www-data 16384 14 nov. 11:00 wp-includes
-rw-r--r-- 1 www-data www-data 2502 26 nov. 2022 wp-links-opml.php
-rw-r--r-- 1 www-data www-data 3937 11 mars 2024 wp-load.php
-rw-r--r-- 1 www-data www-data 51414 3 févr. 2025 wp-login.php
-rw-r--r-- 1 www-data www-data 8727 8 févr. 2025 wp-mail.php
-rw-r--r-- 1 www-data www-data 30081 4 mars 2025 wp-settings.php
-rw-r--r-- 1 www-data www-data 34516 10 mars 2025 wp-signup.php
-rw-r--r-- 1 www-data www-data 5102 18 oct. 2024 wp-trackback.php
-rw-r--r-- 1 www-data www-data 3205 8 nov. 2024 xmlrpc.php
root@web-1:/var/www/html/wordpress#



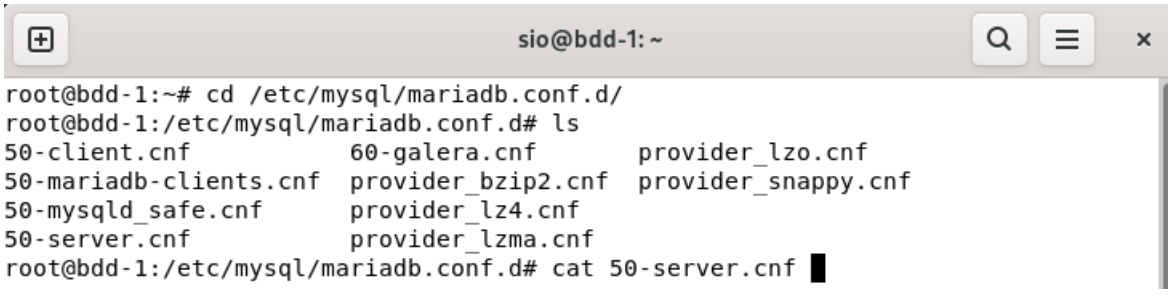
Ne pas poursuivre la création du fichier wp-config.php

Nouveau playbook install-mariadb2.yml : handlers et module lineinfile

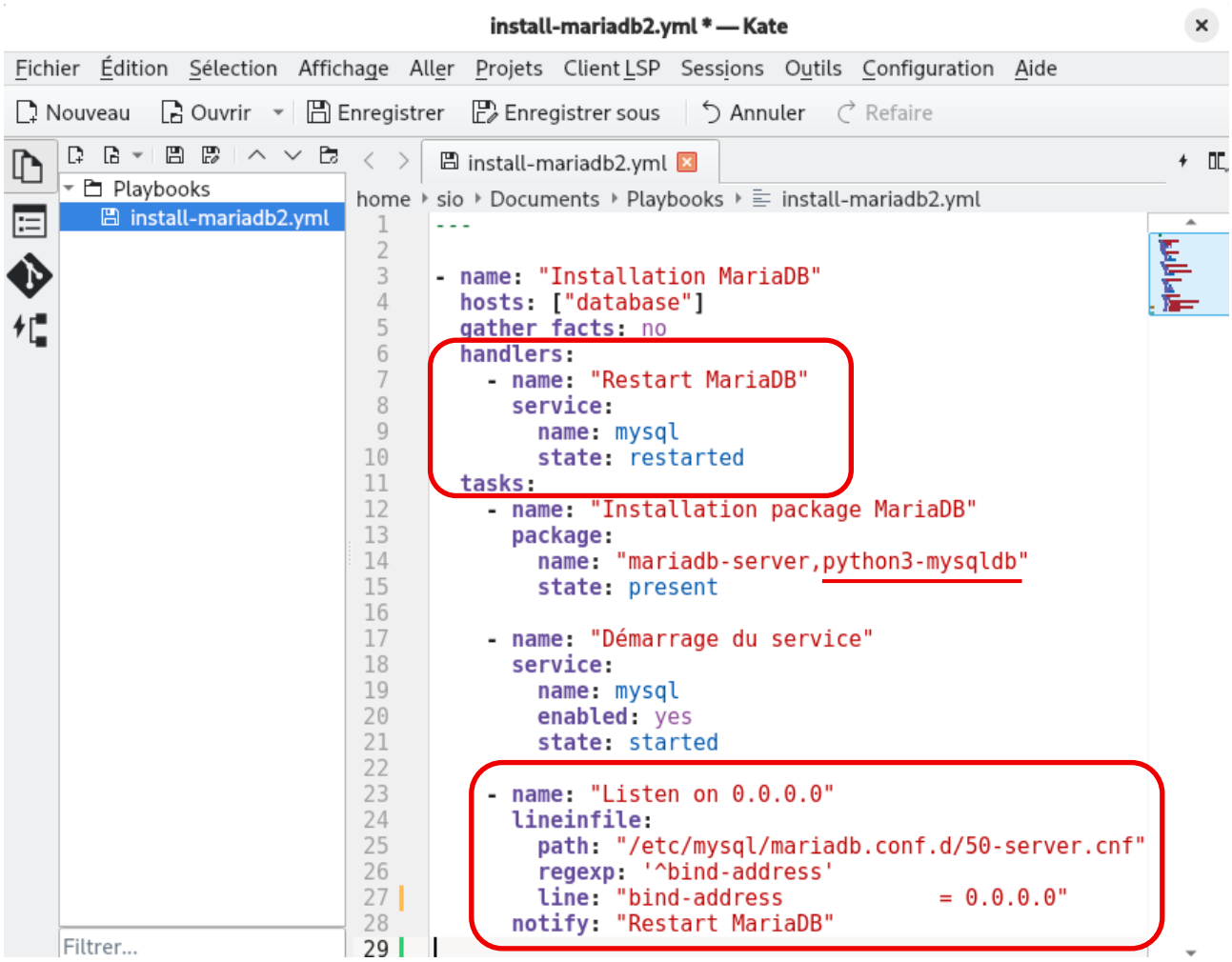
Un **handler** est une tâche qui permet ici de redémarrer le service si une autre tâche modifie le fichier de configuration. La section **handlers** se place au même niveau que **tasks**. Un handler sera appelé avec **notify**. Il n'intervient qu'une seule fois même s'il a été appelé par plusieurs tâches et uniquement en cas de changement.

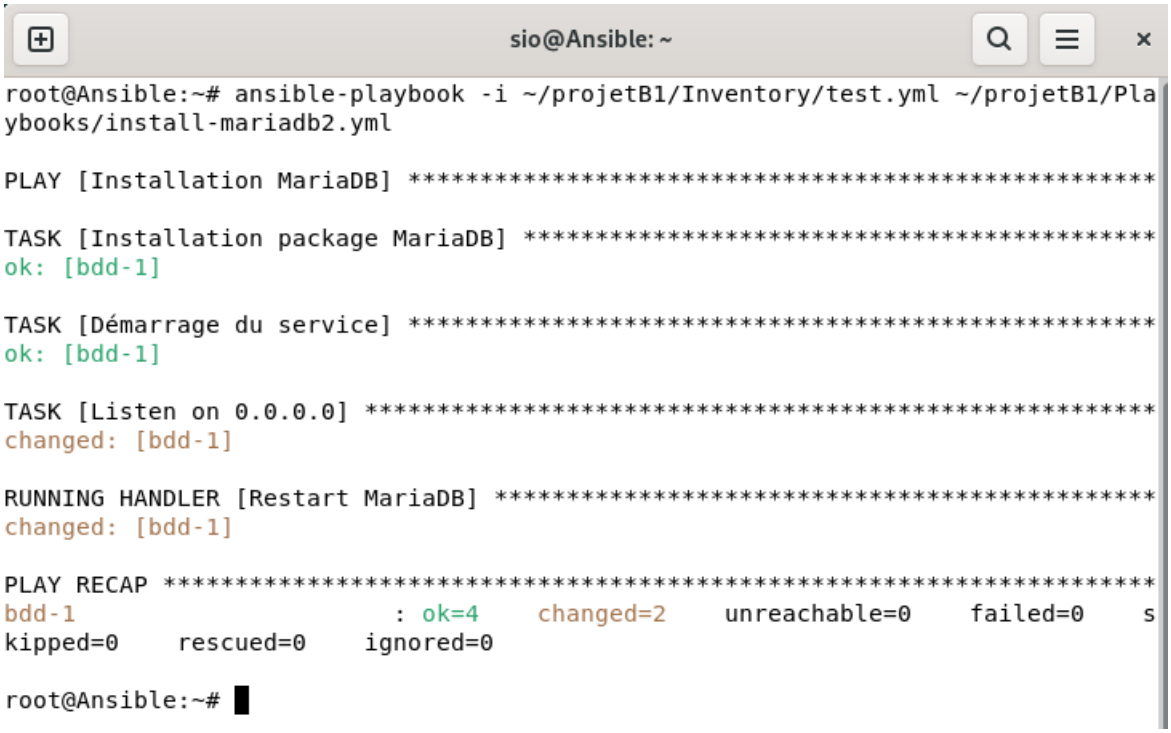
Mariadb répond uniquement par défaut en local host.

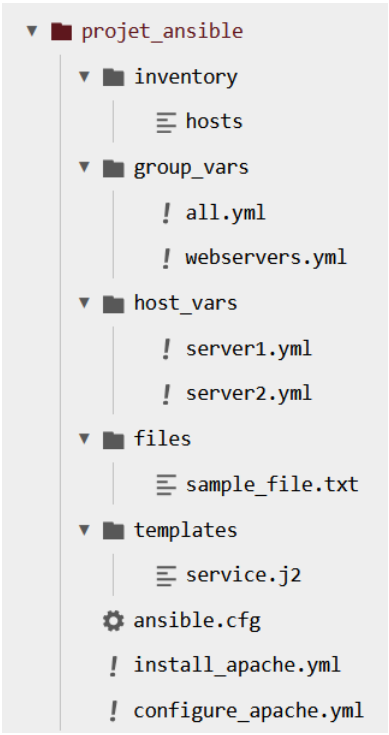
⇨ Faire un **grep bind-address /etc/mysql/mariadb.conf.d/50-server.cnf** sur la machine bdd-1 pour monter que mariadb écoute depuis 127.0.0.1 et non pas depuis toutes les interfaces de la machine. Affichez également le **fichier 50-server.cnf** afin de montrer la ligne bind-address.



Le module lineinfile va permettre de modifier la ligne bind-address.


install-mariadb2.yml * — Kate
Fichier Édition Sélection Affichage Aller Projets Client LSP Sessions Outils Configuration Aide
Nouveau Ouvrir Enregistrer Enregistrer sous Annuler Refaire
Playbooks
install-mariadb2.yml
Filtrer...
install-mariadb2.yml
home ▸ sio ▸ Documents ▸ Playbooks ▸ install-mariadb2.yml
1 ---
2
3 - name: "Installation MariaDB"
4 hosts: ["database"]
5 gather_facts: no
6 handlers:
7 - name: "Restart MariaDB"
8 service:
9 name: mysql
10 state: restarted
11 tasks:
12 - name: "Installation package MariaDB"
13 package:
14 name: "mariadb-server,python3-mysqldb"
15 state: present
16
17 - name: "Démarrage du service"
18 service:
19 name: mysql
20 enabled: yes
21 state: started
22
23 - name: "Listen on 0.0.0.0"
24 lineinfile:
25 path: "/etc/mysql/mariadb.conf.d/50-server.cnf"
26 regexp: '^bind-address'
27 line: "bind-address = 0.0.0.0"
28 notify: "Restart MariaDB"
29

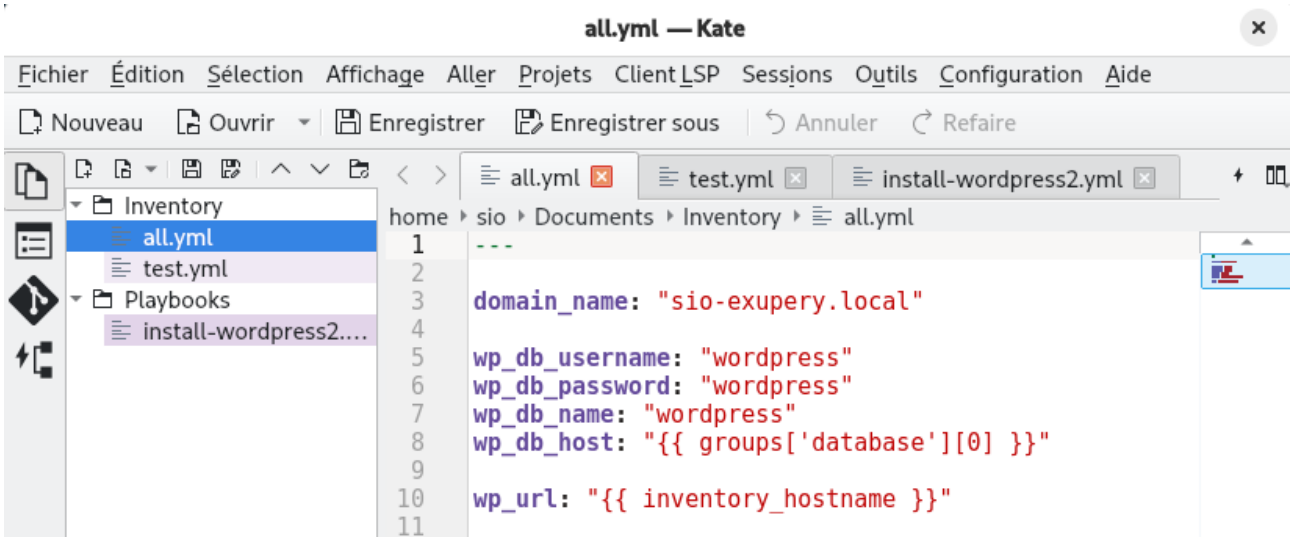

sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Pla
ybooks/install-mariadb2.yml
PLAY [Installation MariaDB] **
TASK [Installation package MariaDB] **
ok: [bdd-1]
TASK [Démarrage du service] **
ok: [bdd-1]
TASK [Listen on 0.0.0.0] ***
changed: [bdd-1]
RUNNING HANDLER [Restart MariaDB] **
changed: [bdd-1]
PLAY RECAP ***
bdd-1 : ok=4 changed=2 unreachable=0 failed=0 s
kipped=0 rescued=0 ignored=0
root@Ansible:~#



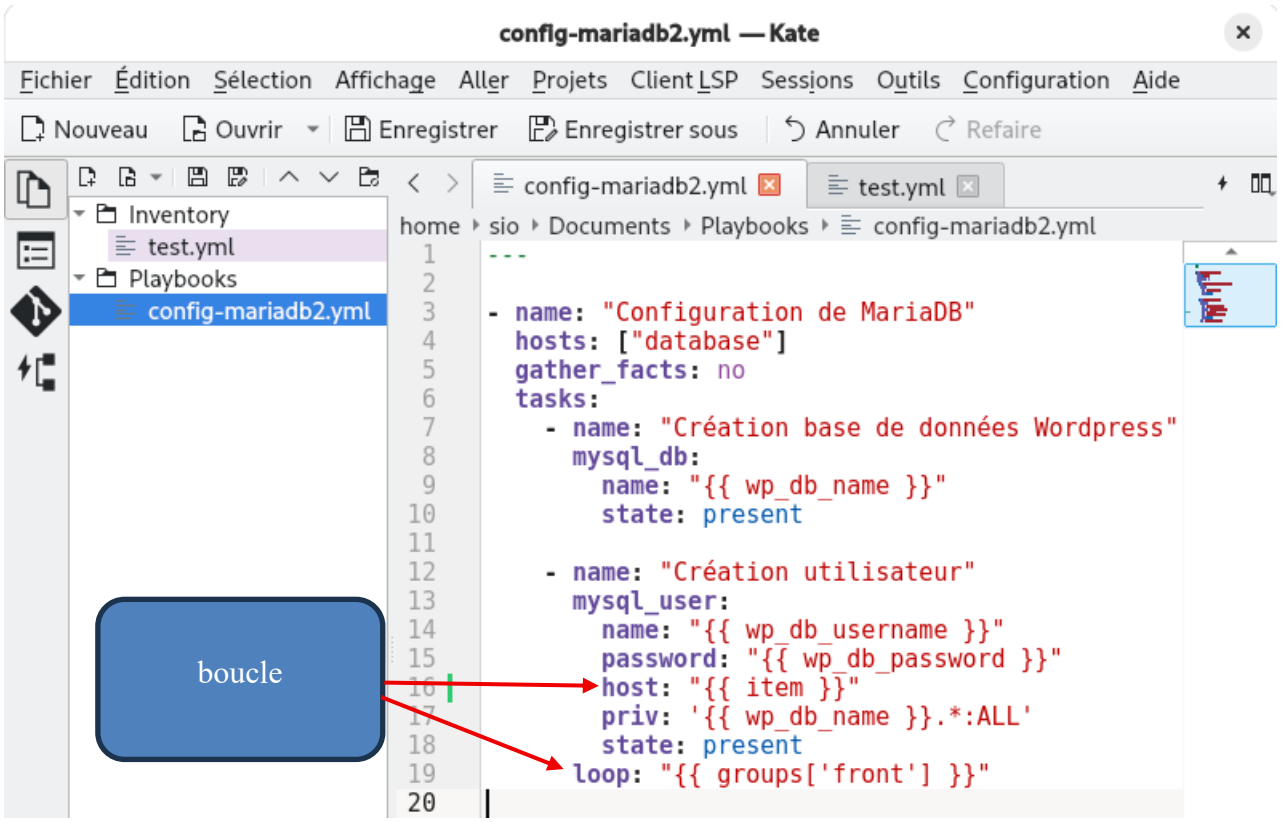
Cf. https://blog.stephane-robert.info/docs/infra-as-code/gestion-de-configuration/ansible/variables/

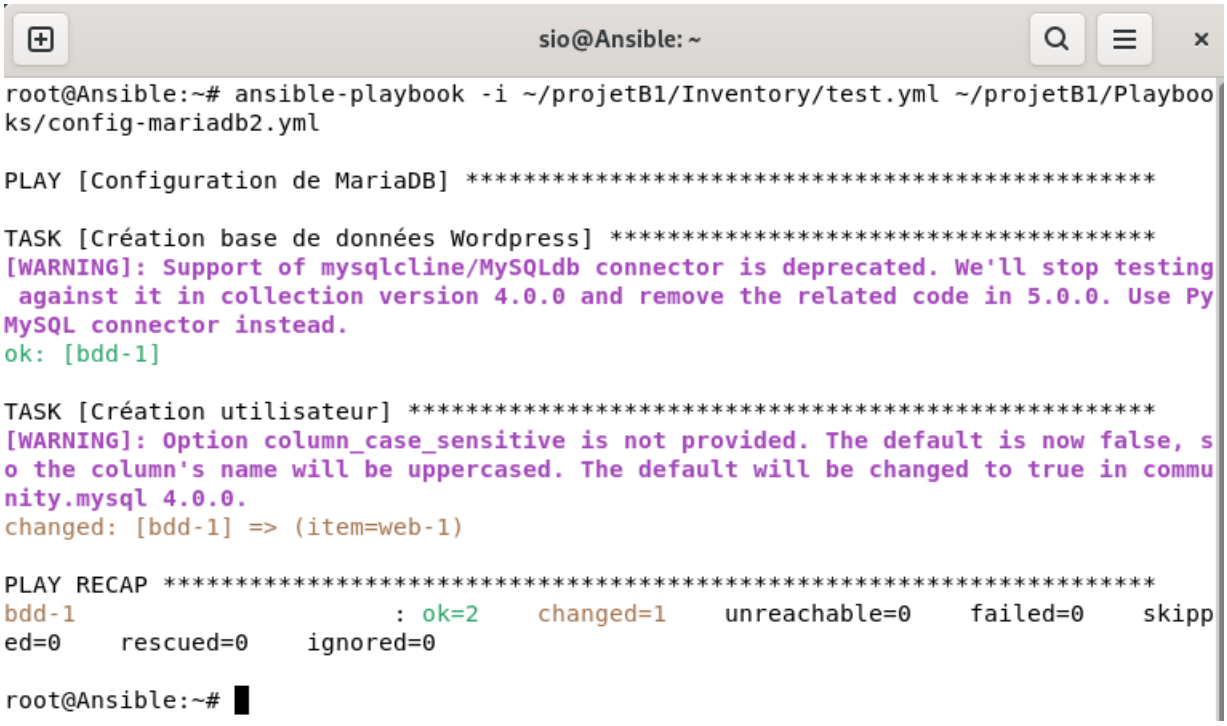
Créez le répertoire **group_vars** dans le répertoire Inventory :

Créez, dans le répertoire group_vars, le fichier **all.yml** contenant les variables qui seront utilisées dans les playbooks **config-mariadb2.yml et install-wordpress2.yml :**

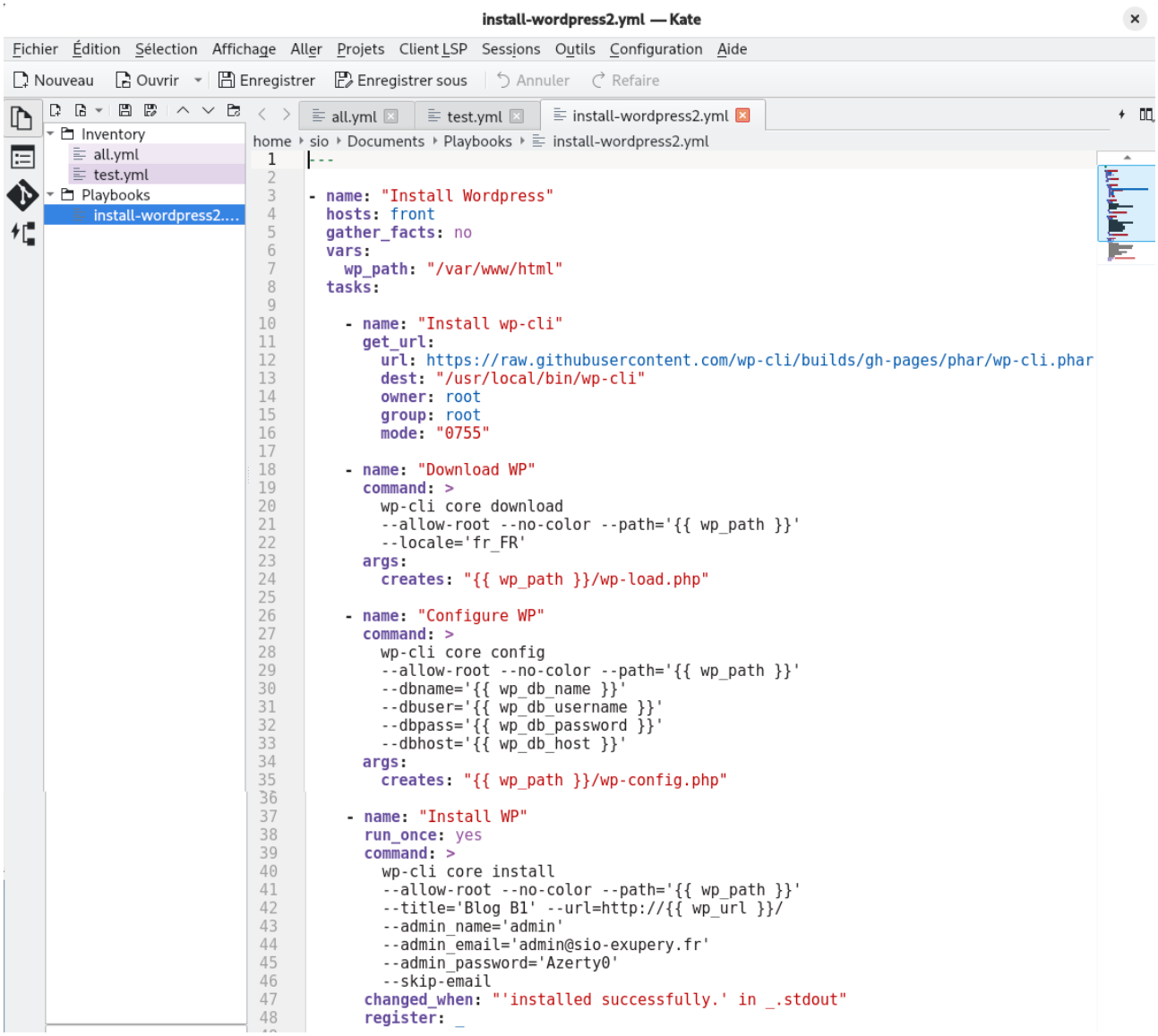


Playbook config-mariadb2.yml : création de la base de données et de l'utilisateur SQL avec les modules mysql_db et mysql_user pour chaque machine du groupe database (cf. fichier initial page 35 en comparaison)

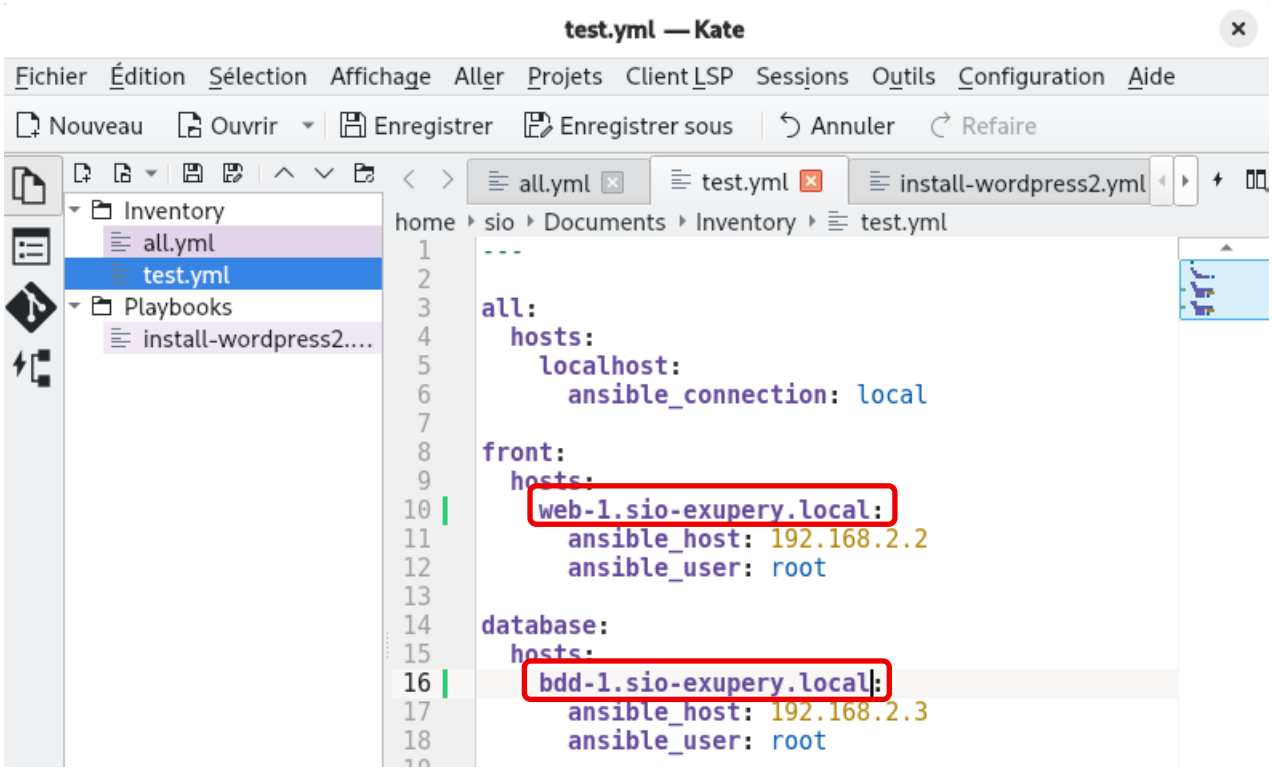




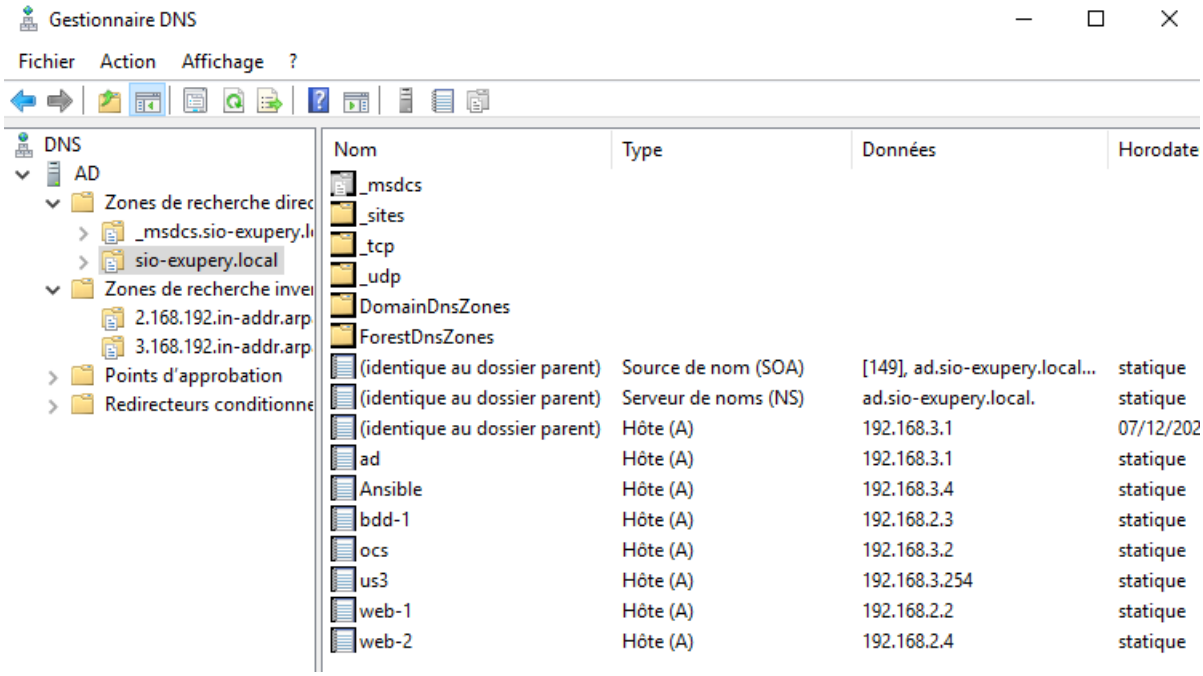
Playbook **install-wordpress2.yml** destiné à automatiser la configuration (cf. pages 38 à 40 en comparaison) : **wp-cli** téléchargé avec le module **get_url** et **module command** pour télécharger les binaires de wordpress puis initialiser la base de données.

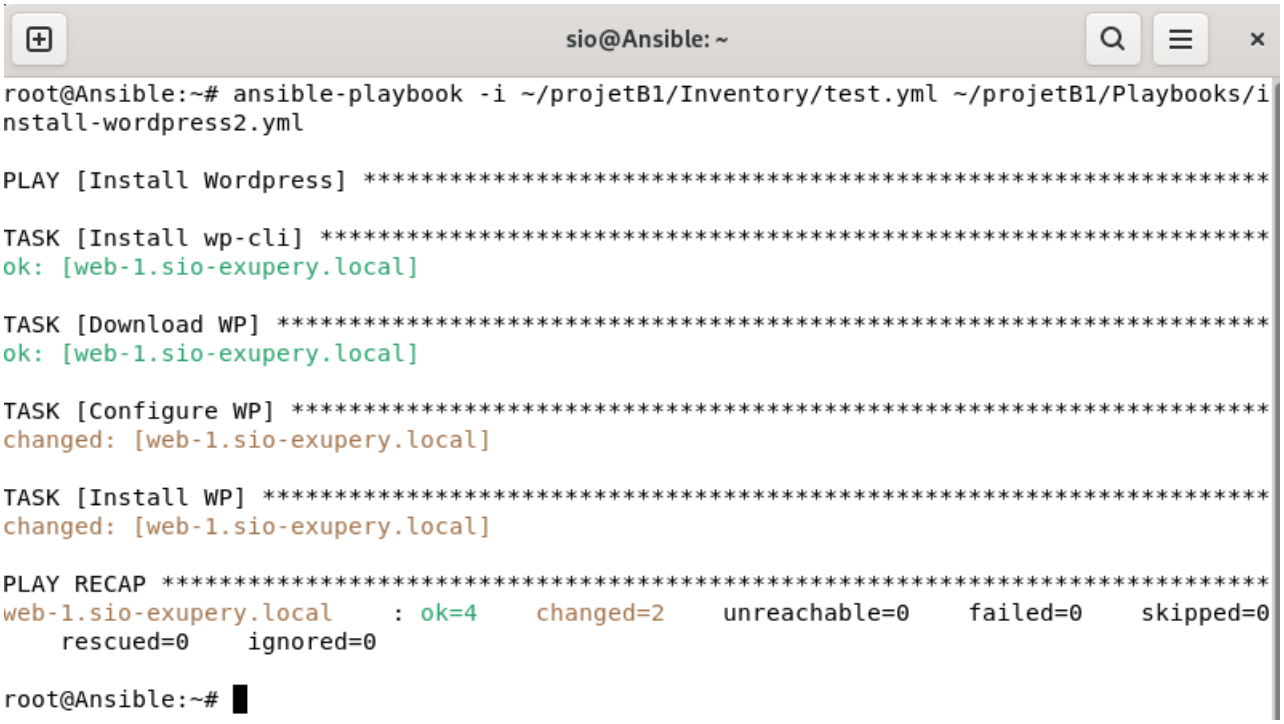


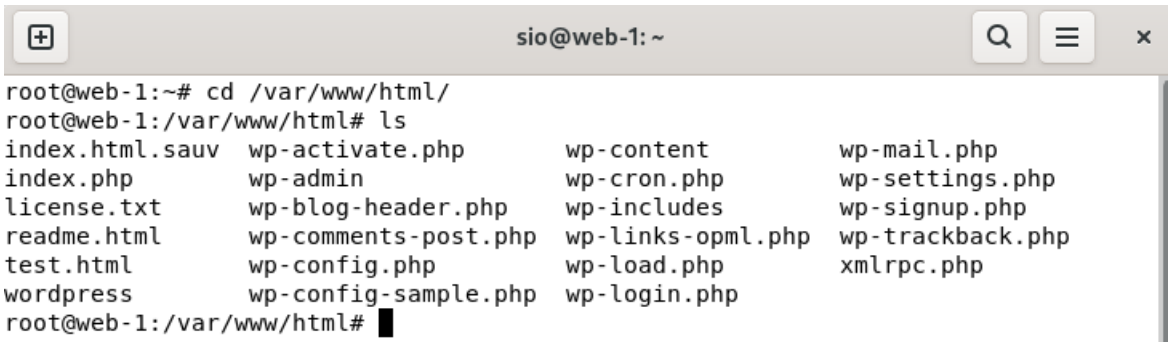
Modifiez le fichier d'inventaire :

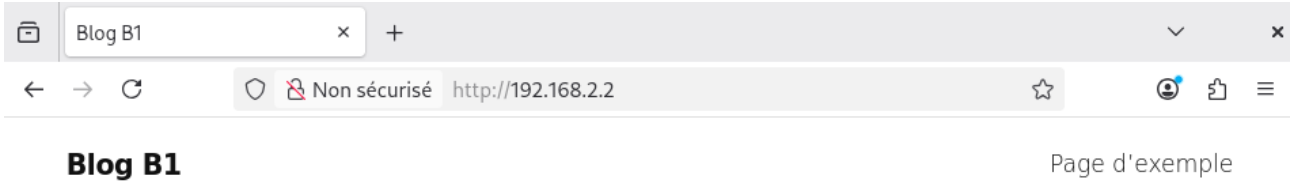


Créez les enregistrements DNS dans la zone sio-exupery.local :




sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Playbooks/install-wordpress2.yml
PLAY [Install Wordpress] **
TASK [Install wp-cli] **
ok: [web-1.sio-exupery.local]
TASK [Download WP] **
ok: [web-1.sio-exupery.local]
TASK [Configure WP] **
changed: [web-1.sio-exupery.local]
TASK [Install WP] **
changed: [web-1.sio-exupery.local]
PLAY RECAP **
web-1.sio-exupery.local : ok=4 changed=2 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0
root@Ansible:~#


sio@web-1: ~
root@web-1:~# cd /var/www/html/
root@web-1:/var/www/html# ls
index.html.sauv wp-activate.php wp-content wp-mail.php
index.php wp-admin wp-cron.php wp-settings.php
license.txt wp-blog-header.php wp-includes wp-signup.php
readme.html wp-comments-post.php wp-links-opml.php wp-trackback.php
test.html wp-config.php wp-load.php xmlrpc.php
wordpress wp-config-sample.php wp-login.php
root@web-1:/var/www/html#


Blog B1
Non sécurisé
http://192.168.2.2
Blog B1
Page d'exemple
Blog
Bonjour tout le monde !
Bienvenue sur WordPress. Ceci est votre premier article. Modifiez-le ou supprimez-le, puis commencez à écrire !

14. Installation d'un serveur HAproxy

Vérification US3 :

```
  GNU nano 7.2                                  /etc/netplan/50-cloud-init.yaml
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.1.101/24]
      routes:
          - to: default
            via: 192.168.1.1
      nameservers:
            addresses: [192.168.1.1]
    enp0s8:
        addresses: [192.168.2.254/24]
        dhcp4: no
    enp0s9:
        addresses: [192.168.3.254/24]
        dhcp4: no
```

GW : 172.17.250.3

192.168.3.1

```
root@US3:/etc/netplan# netplan apply
root@US3:/etc/netplan# _
```

```
root@us3:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere
root@us3:~#
```

Translation

```
  GNU nano 7.2                                                  /etc/sysctl.conf
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#

#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

##############################################################3
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1

# Uncomment the next line to enable packet forwarding for IPv6
#  Enabling this option disables Stateless Address Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

Routage

```
root@us3:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:09:e5:3f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.101/24 brd 192.168.1.255 scope global enp0s3
       valid_lft forever preferred_lft forever
    inet6 2a01:cb1d:79a:4c00:a00:27ff:fe09:e53f/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86379sec preferred_lft 579sec
    inet6 fe80::a00:27ff:fe09:e53f/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c6:ad:f9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.254/24 brd 192.168.2.255 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec6:adf9/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6c:13:10 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.254/24 brd 192.168.3.255 scope global enp0s9
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe6c:1310/64 scope link
       valid_lft forever preferred_lft forever
root@us3:~# ip r
default via 192.168.1.1 dev enp0s3 proto static
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.101
192.168.2.0/24 dev enp0s8 proto kernel scope link src 192.168.2.254
192.168.3.0/24 dev enp0s9 proto kernel scope link src 192.168.3.254
root@us3:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=20.2 ms
^C
--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 20.231/20.231/20.231/0.000 ms
root@us3:~#
```

```
root@us3:~# cd /run/systemd/resolve
root@us3:/run/systemd/resolve# ls -l
total 8
srw-rw-rw- 1 systemd-resolve systemd-resolve   0 déc.   7 12:52 io.systemd.Resolve
srw------- 1 systemd-resolve systemd-resolve   0 déc.   7 12:52 io.systemd.Resolve.Monitor
-rw-r--r-- 1 systemd-resolve systemd-resolve 878 déc.   7 12:53 resolv.conf
-rw-r--r-- 1 systemd-resolve systemd-resolve 923 déc.   7 12:53 stub-resolv.conf
root@us3:/run/systemd/resolve# cat resolv.conf
# This is /run/systemd/resolve/resolv.conf managed by man:systemd-resolved(8).
# Do not edit.
#
# This file might be symlinked as /etc/resolv.conf. If you're looking at
# /etc/resolv.conf and seeing this text, you have followed the symlink.
#
# This is a dynamic resolv.conf file for connecting local clients directly to
# all known uplink DNS servers. This file lists all configured search domains.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 192.168.1.1
```

192.168.3.1

Si problème résolution DNS : https://www.linuxtricks.fr/wiki/systemd-la-resolution-de-nom-avec-systemd-resolved

```
 GNU nano 7.2                                                /etc/ssh/sshd_config

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
```

US3 serveur SSH (redémarrer ensuite le service sshd)

Transfert de la clé publique du client SSH Ansible vers le fichier authorized_keys du serveur SSH US3 :

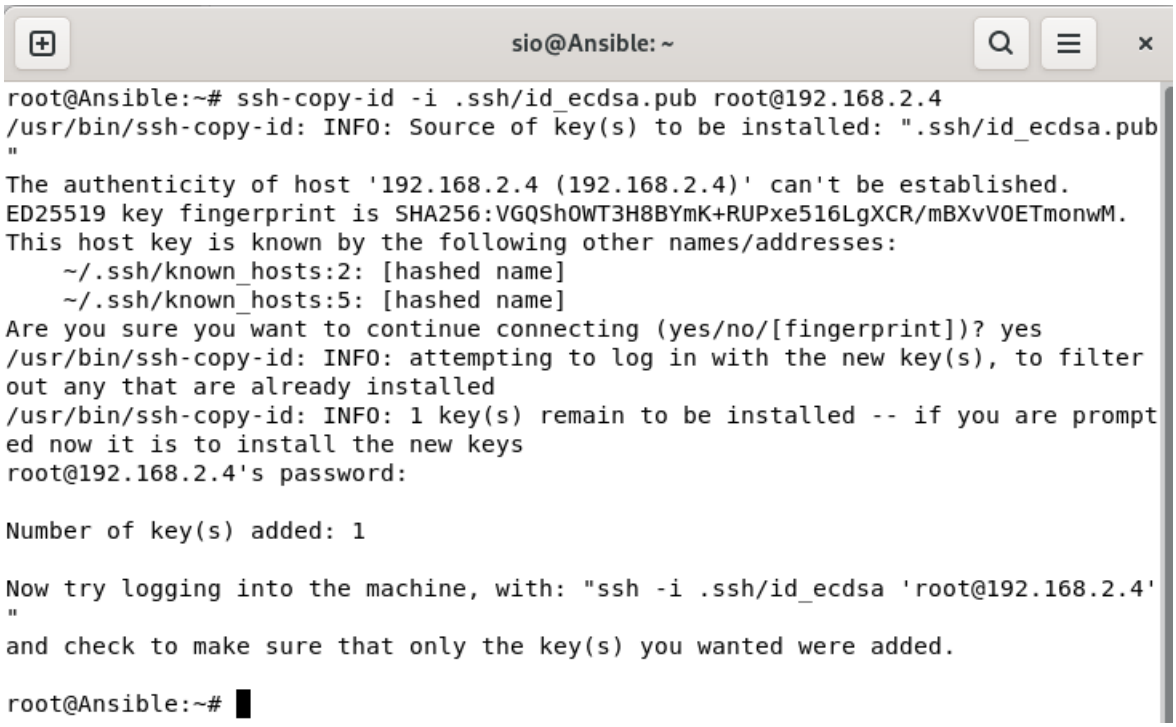
```
sio@Ansible: ~
root@Ansible:~# ssh-copy-id root@192.168.3.254
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: ssh-add -L
The authenticity of host '192.168.3.254 (192.168.3.254)' can't be established.
ED25519 key fingerprint is SHA256:py+96UF1wsAeOT7r/Fonwhl2Eqq7piD3XorNCf4ubvI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 2 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
root@192.168.3.254's password:

Number of key(s) added: 2

Now try logging into the machine, with: "ssh 'root@192.168.3.254'"
and check to make sure that only the key(s) you wanted were added.

root@Ansible:~#
```

```
sio@Web-2: ~
 GNU nano 8.4                    /etc/ssh/sshd_config

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
AuthorizedKeysFile      .ssh/authorized_keys .ssh/authorized_keys2
```

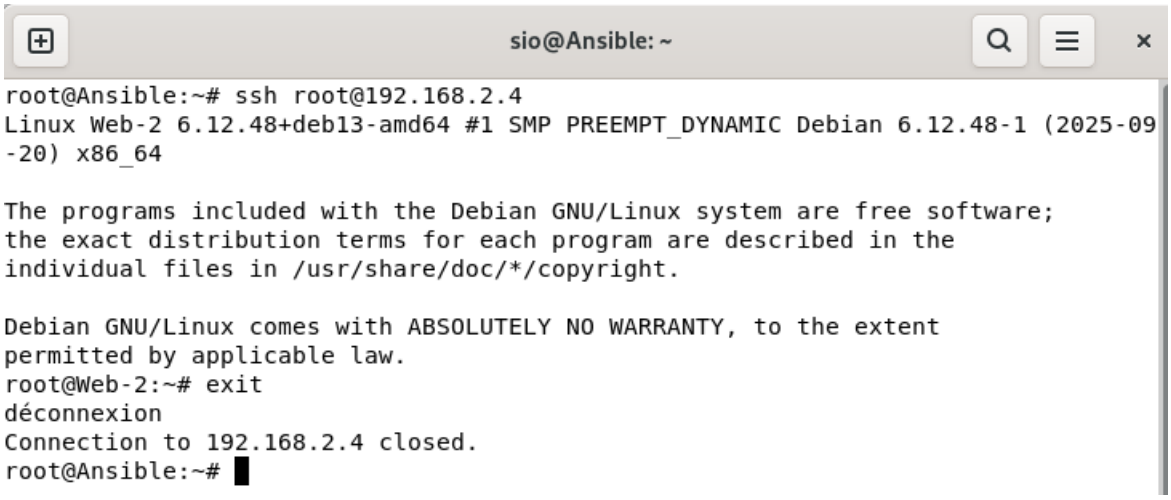
Serveur SSH web-2

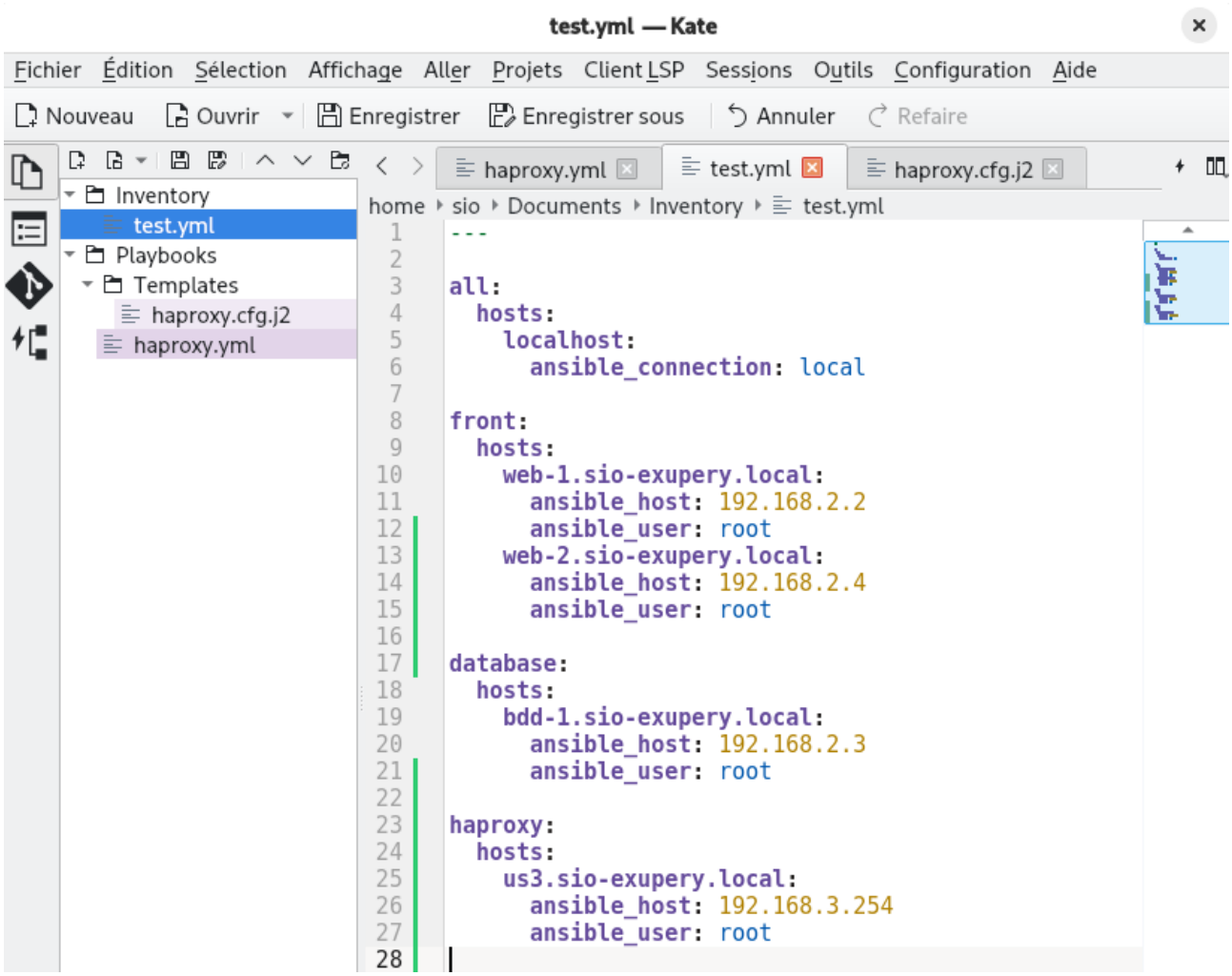
```
sio@Web-2: ~
root@Web-2:~# systemctl restart sshd
root@Web-2:~#
```

Transfert de la clé publique du client SSH Ansible vers le fichier authorized_keys du serveur SSH web-2 :



Test accès SSH au serveur web-2 :





Installation PHP et Apache sur web-2 :

```
sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Playbooks/php-apache.yml

PLAY [Installation de PHP et Apache2] ******************************************************************

TASK [Installation PHP] ********************************************************************************
ok: [web-1.sio-exupery.local]
changed: [web-2.sio-exupery.local]

TASK [Installation Apache2] ****************************************************************************
ok: [web-1.sio-exupery.local]
ok: [web-2.sio-exupery.local]

TASK [Démarrer Apache] *********************************************************************************
ok: [web-1.sio-exupery.local]
ok: [web-2.sio-exupery.local]

PLAY RECAP *********************************************************************************************
web-1.sio-exupery.local    : ok=3    changed=0    unreachable=0    failed=0    skipped=0    rescued=0
 ignored=0
web-2.sio-exupery.local    : ok=3    changed=1    unreachable=0    failed=0    skipped=0    rescued=0
 ignored=0

root@Ansible:~#
```

Modification Création de l'utilisateur SQL sur bdd-1 (pour web-2) :

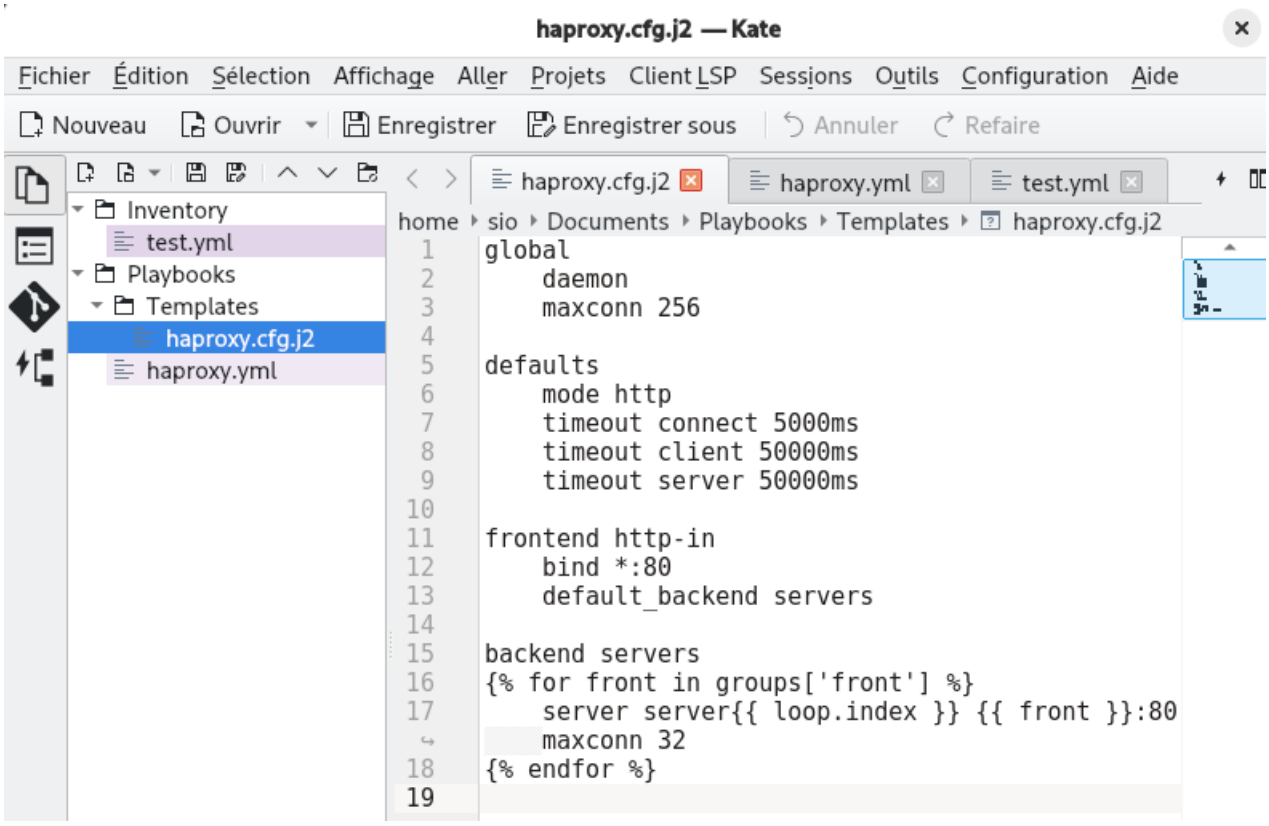
```
sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Pla
ybooks/config-mariadb2.yml

PLAY [Configuration de MariaDB] ************************************************

TASK [Création base de données Wordpress] **************************************
[WARNING]: Support of mysqlcline/MySQLdb connector is deprecated. We'll stop tes
ting against it in collection version 4.0.0 and remove the related code in 5.0.0
. Use PyMySQL connector instead.
ok: [bdd-1.sio-exupery.local]

TASK [Création utilisateur] ****************************************************
[WARNING]: Option column_case_sensitive is not provided. The default is now fals
e, so the column's name will be uppercased. The default will be changed to true
in community.mysql 4.0.0.
ok: [bdd-1.sio-exupery.local] => (item=web-1.sio-exupery.local)
changed: [bdd-1.sio-exupery.local] => (item=web-2.sio-exupery.local)

PLAY RECAP *********************************************************************
bdd-1.sio-exupery.local    : ok=2    changed=1    unreachable=0    failed=0    s
kipped=0    rescued=0    ignored=0

root@Ansible:~#
```

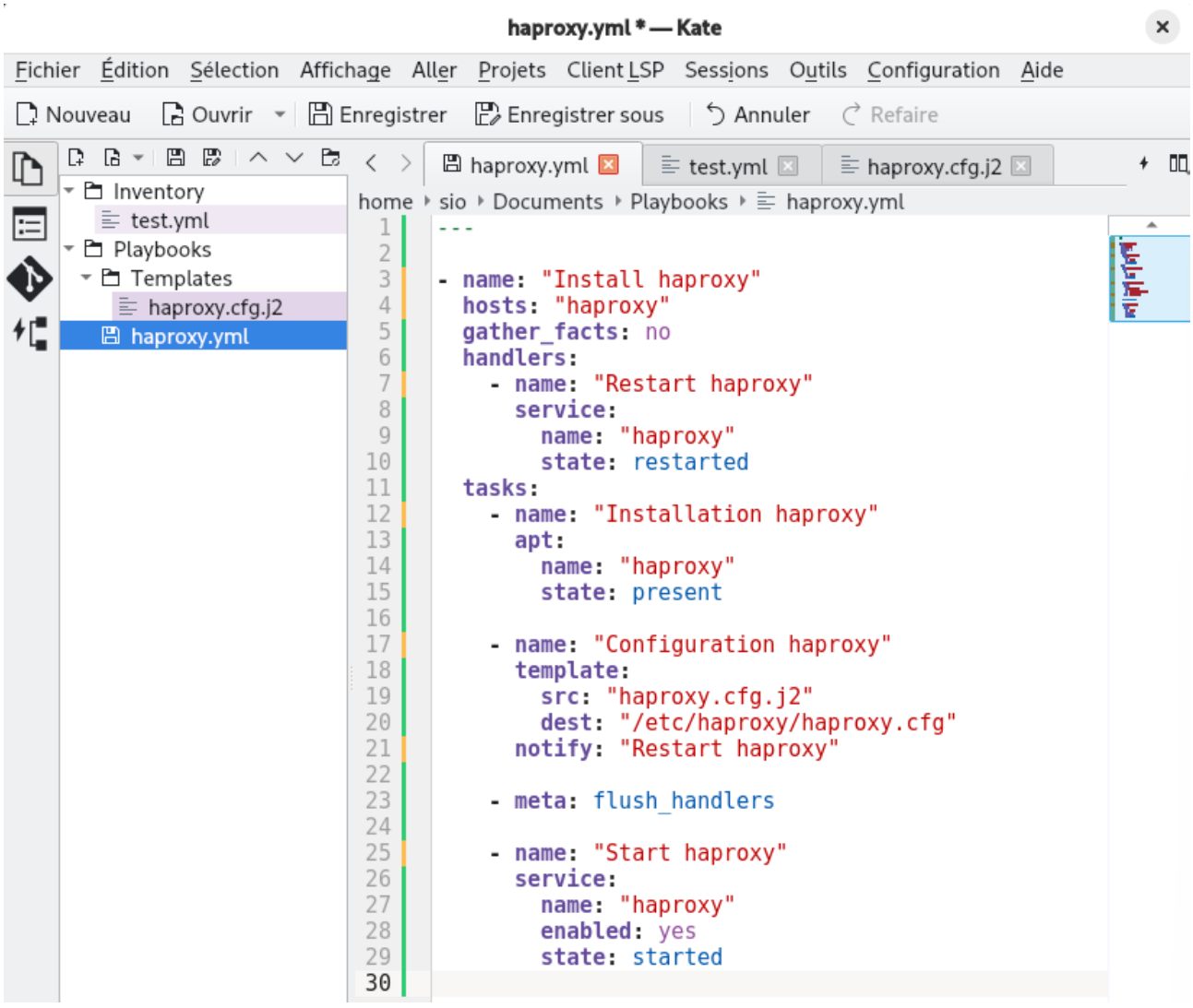
Installation de wordpress sur web-2 :

```
sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Playbooks/inst
all-wordpress2.yml -e wp_url=us3.sio-exupery.local

PLAY [Install Wordpress] *******************************************************

TASK [Install wp-cli] **********************************************************
changed: [web-2.sio-exupery.local]
ok: [web-1.sio-exupery.local]

TASK [Download WP] *************************************************************
ok: [web-1.sio-exupery.local]
changed: [web-2.sio-exupery.local]

TASK [Configure WP] ************************************************************
ok: [web-1.sio-exupery.local]
changed: [web-2.sio-exupery.local]

TASK [Install WP] **************************************************************
ok: [web-1.sio-exupery.local]

PLAY RECAP *********************************************************************
web-1.sio-exupery.local    : ok=4    changed=0    unreachable=0    failed=0    skipped=0    rescued=0
 ignored=0
web-2.sio-exupery.local    : ok=3    changed=1    unreachable=0    failed=0    skipped=0    rescued=0
 ignored=0

root@Ansible:~#
```

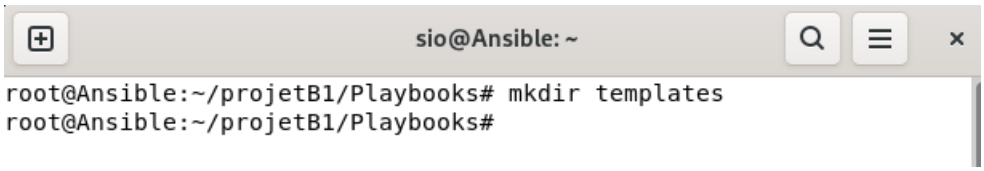
Module **template** et moteur de template **Jinja** pour modifier dynamiquement un fichier de configuration :

```
sio@Ansible: ~
root@Ansible:~/projetB1/Playbooks# mkdir templates
root@Ansible:~/projetB1/Playbooks#
```


haproxy.cfg.j2 — Kate
Fichier Édition Sélection Affichage Aller Projets Client LSP Sessions Outils Configuration Aide
Nouveau Ouvrir Enregistrer Enregistrer sous Annuler Refaire
Inventory
test.yml
Playbooks
Templates
haproxy.cfg.j2
haproxy.yml
haproxy.cfg.j2
haproxy.yml
test.yml
home sio Documents Playbooks Templates haproxy.cfg.j2
1 global
2 daemon
3 maxconn 256
4
5 defaults
6 mode http
7 timeout connect 5000ms
8 timeout client 50000ms
9 timeout server 50000ms
10
11 frontend http-in
12 bind *:80
13 default_backend servers
14
15 backend servers
16 {% for front in groups['front'] %}
17 server server{{ loop.index }} {{ front }}:80
maxconn 32
18 {% endfor %}
19

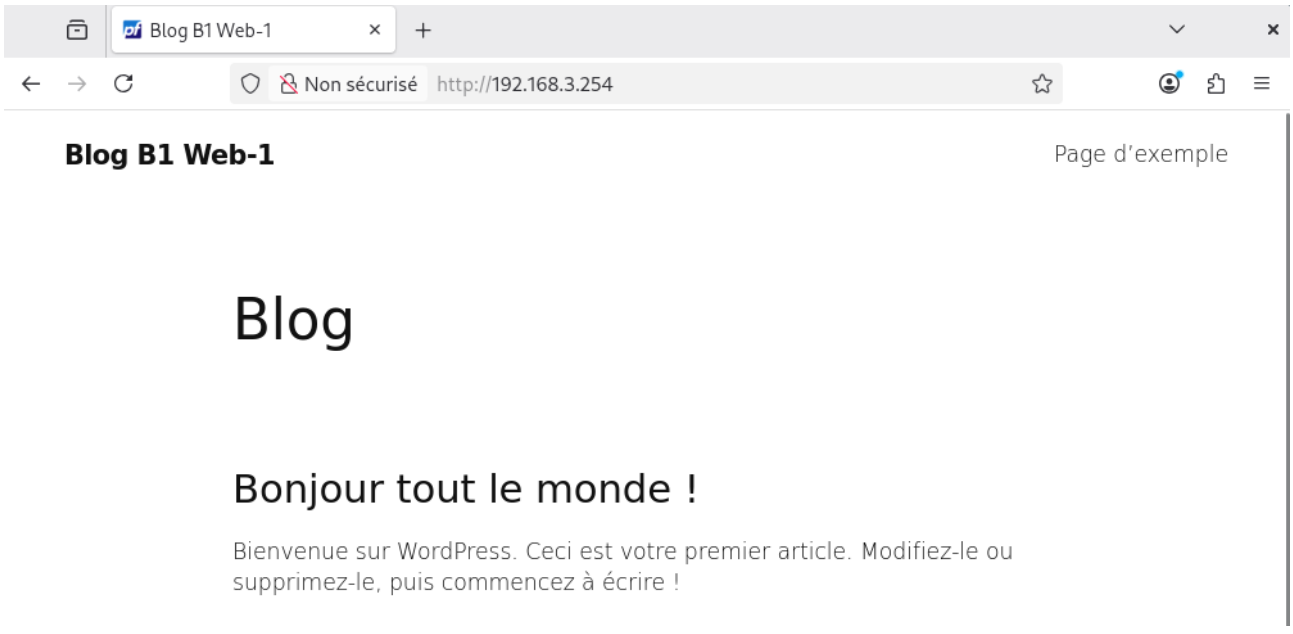

haproxy.yml * — Kate
Fichier Édition Sélection Affichage Aller Projets Client LSP Sessions Outils Configuration Aide
Nouveau Ouvrir Enregistrer Enregistrer sous Annuler Refaire
Inventory
test.yml
Playbooks
Templates
haproxy.cfg.j2
haproxy.yml
haproxy.yml
test.yml
haproxy.cfg.j2
home sio Documents Playbooks haproxy.yml

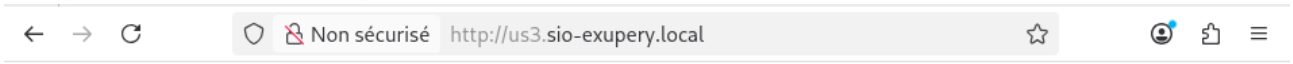
- name: "Install haproxy"
hosts: "haproxy"
gather_facts: no
handlers:
- name: "Restart haproxy"
service:
name: "haproxy"
state: restarted
tasks:
- name: "Installation haproxy"
apt:
name: "haproxy"
state: present
- name: "Configuration haproxy"
template:
src: "haproxy.cfg.j2"
dest: "/etc/haproxy/haproxy.cfg"
notify: "Restart haproxy"
- meta: flush_handlers
- name: "Start haproxy"
service:
name: "haproxy"
enabled: yes
state: started


sio@Ansible: ~
root@Ansible:~/projetB1/Playbooks# mkdir templates
root@Ansible:~/projetB1/Playbooks#

```
sio@Ansible: ~
root@Ansible:~# ansible-playbook -i ~/projetB1/Inventory/test.yml ~/projetB1/Playbooks/haproxy.yml

PLAY [Install haproxy] *********************************************************

TASK [Installation haproxy] ****************************************************
ok: [us3.sio-exupery.local]

TASK [Configuration haproxy] ***************************************************
ok: [us3.sio-exupery.local]

TASK [meta] ********************************************************************

TASK [Start haproxy] ***********************************************************
changed: [us3.sio-exupery.local]

PLAY RECAP *********************************************************************
us3.sio-exupery.local      : ok=3    changed=1    unreachable=0    failed=0    skipped=0
    rescued=0    ignored=0

root@Ansible:~#
```

```
root@us3:~# cat /etc/haproxy/haproxy.cfg
global
    daemon
    maxconn 256

defaults
    mode http
    timeout connect 5000ms
    timeout client 50000ms
    timeout server 50000ms

frontend http-in
    bind *:80
    default_backend servers

backend servers
    server server1 web-1.sio-exupery.local:80 maxconn 32
    server server2 web-2.sio-exupery.local:80 maxconn 32
root@us3:~#
```





Blog B1 Web-1 Page d'exemple

Blog

Bonjour tout le monde !

Bienvenue sur WordPress. Ceci est votre premier article. Modifiez-le ou supprimez-le, puis commencez à écrire !