Version : **2023.02**.

Dernière mise-à-jour : 2023/08/25 01:25

LCF801 - Installation d'Ansible

Contenu du Module

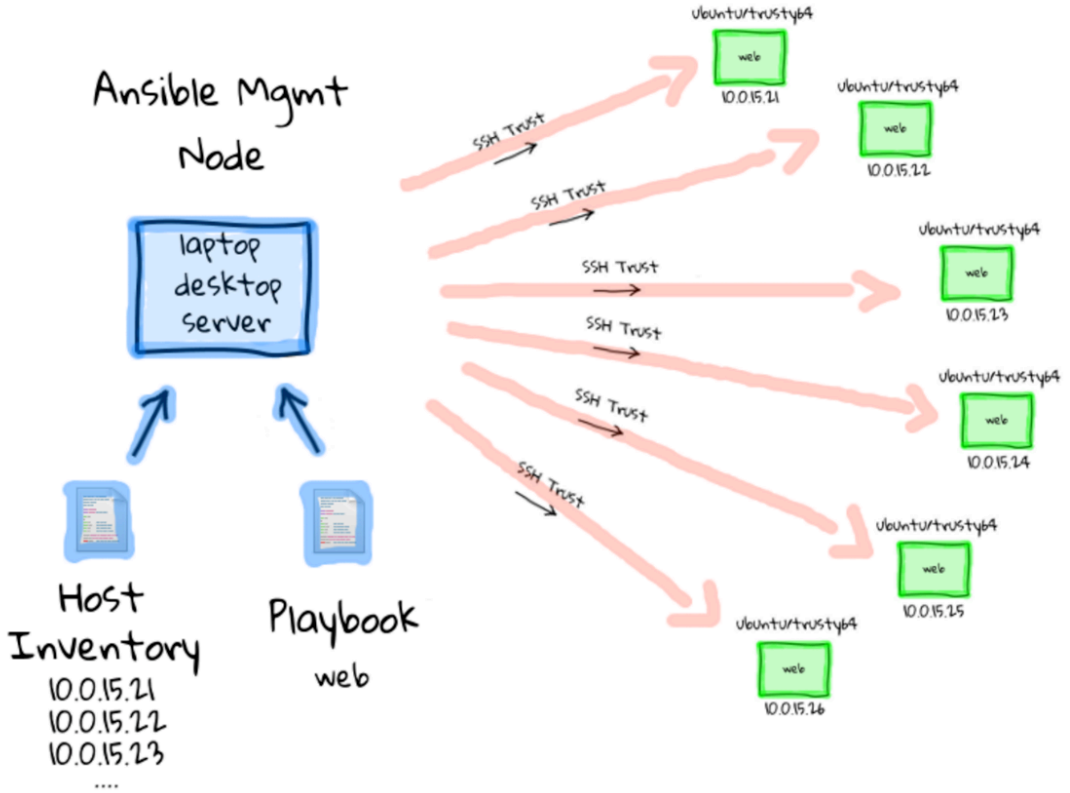
- **LCF801 - Installation d'Ansible**
  - Contenu du Module
  - Qu'est-ce Ansible ?
  - LAB #1 - Installation d'Ansible
  - LAB #2 - Configuration de ssh et de sudo
    - 2.1 - ssh
    - 2.2 - sudo

Qu'est-ce Ansible ?

Ansible est un outil d'automatisation qui permet d'automatiser les installations et les configurations répétitives de logiciels de manière fiable en utilisant une bibliothèque ré-utilisable d'instructions.

Ansible :

- est installé sur un **contrôleur** qui communique avec les machines cibles en utilisant le protocole **SSH**,
- ne nécessite ni l'utilisation d'un agent ni l'utilisation d'un service sur les cibles,
- utilise le langage **YAML** (**Y**et **A**other **M**arkup **L**anguage), plus simple que JSON, le code Ruby utilisé par **Chef** et le langage propriétaire de **Puppet**.



LAB #1 - Installation d'Ansible

Connectez-vous à la à **centos8** à partir de votre gateway dans notre cloud :

```
trainee@traineeXX:~$ ssh -l trainee 10.0.2.45
The authenticity of host '10.0.2.45 (10.0.2.45)' can't be established.
ECDSA key fingerprint is SHA256:Q7T/CP0SLiMbMAIgVzTuEHegYS/spPE5zzQchCHD5Vw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.2.45' (ECDSA) to the list of known hosts.
trainee@10.0.2.45's password:
Activate the web console with: systemctl enable --now cockpit.socket
```

```
Last login: Sun Mar  6 12:00:35 2022 from 10.0.2.1
[trainee@centos8 ~]$
```

Pour obtenir la dernière version d'Ansible, il convient d'utiliser **python3-pip**. Installez python3-pip avec la commande **dnf** :

```
[trainee@centos8 ~]$ su -
Password: fenestros

[root@centos8 ~]# dnf update
Last metadata expiration check: 0:19:03 ago on Tue 08 Mar 2022 10:30:01 EST.
Dependencies resolved.
Nothing to do.
Complete!

[root@centos8 ~]# dnf -y install python3-pip
Last metadata expiration check: 0:19:29 ago on Tue 08 Mar 2022 10:30:01 EST.
Package python3-pip-9.0.3-20.el8.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!

[root@centos8 ~]# pip3 -V
pip 9.0.3 from /usr/lib/python3.6/site-packages (python 3.6)

[root@centos8 ~]# pip3 list
DEPRECATION: The default format will switch to columns in the future. You can use --format=(legacy|columns) (or
define a format=(legacy|columns) in your pip.conf under the [list] section) to disable this warning.
blivet (3.4.0)
Brlapi (0.6.7)
chardet (3.0.4)
chrome-gnome-shell (0.0.0)
configobj (5.0.6)
cupshelpers (1.0)
```

```
dasbus (1.2)
dbus-python (1.2.4)
decorator (4.2.1)
docutils (0.14)
ethtool (0.14)
gpg (1.13.1)
html5lib (0.999999999)
idna (2.5)
iniparse (0.4)
initial-setup (0.3.81.7)
isc (2.0)
langtable (0.0.51)
libcomps (0.1.16)
lxml (4.2.3)
nftables (0.1)
ntplib (0.3.3)
ordered-set (2.0.2)
perf (0.1)
pexpect (4.3.1)
pid (2.1.1)
pip (9.0.3)
ply (3.9)
productmd (1.11)
psutil (5.4.3)
ptyprocess (0.5.2)
pwquality (1.4.4)
pycairo (1.16.3)
pycups (1.9.72)
pycurl (7.43.0.2)
pydbus (0.6.0)
pyenchant (2.0.0)
pygobject (3.28.3)
pyinotify (0.9.6)
pykickstart (3.16.14)
```

```
pyparsing (2.1.10)
pyparted (3.11.7)
PySocks (1.6.8)
python-dateutil (2.6.1)
python-dmidecode (3.12.2)
python-linux-procfs (0.6.3)
python-meh (0.47.2)
pytz (2017.2)
pyudev (0.21.0)
pyxdg (0.25)
PyYAML (3.12)
requests (2.20.0)
requests-file (1.4.3)
requests-ftp (0.3.1)
rpm (4.14.3)
schedutils (0.6)
selinux (2.9)
sepolicy (1.1)
setools (4.3.0)
setroubleshoot (1.1)
setuptools (39.2.0)
simpleline (1.1.1)
six (1.11.0)
slip (0.6.4)
slip.dbus (0.6.4)
sos (4.1)
SSSDConfig (2.5.2)
subscription-manager (1.28.21)
syspurpose (1.28.21)
systemd-python (234)
urllib3 (1.24.2)
webencodings (0.5.1)

[root@centos8 ~]# python3 -m pip install --upgrade pip
```

```
WARNING: Running pip install with root privileges is generally not a good idea. Try `__main__.py install --user` instead.
Collecting pip
  Downloading https://files.pythonhosted.org/packages/a4/6d/6463d49a933f547439d6b5b98b46af8742cc03ae83543e4d7688c2420f8b/pip-21.3.1-py3-none-any.whl (1.7MB)
    100% |████████████████████████████████| 1.7MB 747kB/s
Installing collected packages: pip
Successfully installed pip-21.3.1
```

Dernièrement, mettez à jour Python vers la version 3.8 :

```
[root@centos8 ~]# dnf module -y install python38
```

> **Important** : Pip3 est le gestionnaire des paquets pour Python 3.5. La commande est disponible en tant que pip3 ou pip sous Linux, Mac et Windows®.

> **Important** : Notez que le mot de passe **fenestros** ne sera pas en clair.

Utilisez ensuite pip3 pour installer Ansible en tant que **trainee** :

```
[trainee@centos8 ~]$ pip3 install ansible
```

Consultez la version d'Ansible que vous avez installé :

```
[trainee@centos8 ~]$ ansible --version
ansible [core 2.11.9]
  config file = None
```

```
  configured module search path = ['/home/trainee/.ansible/plugins/modules',
'/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/local/lib/python3.6/site-packages/ansible
  ansible collection location = /home/trainee/.ansible/collections:/usr/share/ansible/collections
  executable location = /usr/local/bin/ansible
  python version = 3.6.8 (default, Sep 10 2021, 09:13:53) [GCC 8.5.0 20210514 (Red Hat 8.5.0-3)]
  jinja version = 3.0.3
  libyaml = True
```

LAB #2 - Configuration de ssh et de sudo

2.1 - ssh

Ansible a besoin d'une configuration par clef asymétrique avec la machine **targeta** afin de fonctionner correctement. Dans cette configuration :

- La machine **centos8** envoie à la machine **targeta** une requête d'authentification par clé asymétrique qui contient le module de la clé à utiliser,
- La machine **targeta** recherche une correspondance pour ce module dans le fichier des clés autorisés **~/.ssh/authorized_keys**,
  - Dans le cas où une correspondance n'est pas trouvée, la machine **targeta** met fin à la communication,
  - Dans le cas contraire la machine **targeta** génère une chaîne aléatoire de 256 bits appelée un **challenge** et la chiffre avec la **clé publique de la machine centos8**,
- La machine **centos8** reçoit le challenge et le décrypte avec la partie privée de sa clé. Il combine le challenge avec l'identifiant de session et chiffre le résultat. Ensuite il envoie le résultat chiffré à la machine **targeta**.
- La machine **targeta** génère le même haché et le compare avec celui reçu de la machine **centos8**. Si les deux hachés sont identiques, l'authentification est réussie.

Saisissez maintenant les commandes suivantes en tant que **trainee** dans la machine **centos8** :

> **Important** - Lors de la génération des clefs, la passphrase doit être **vide**.

```
[trainee@centos8 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_rsa.
Your public key has been saved in /home/trainee/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:mgCPKDg5NBf68IbtjUqbvCVLrDf4nw2C6QdIQRgF/aY trainee@centos8.ittraining.loc
The key's randomart image is:
+---[RSA 3072]----+
|=*..             |
|..o .            |
| =oo             |
|o+O+o            |
|X..Bo   S        |
|+*E o. o         |
|o*o+..o          |
|B Xo +           |
|.@+oo .          |
+----[SHA256]-----+
[trainee@centos8 ~]$ ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ecdsa.
Your public key has been saved in /home/trainee/.ssh/id_ecdsa.pub.
The key fingerprint is:
SHA256:X2O1yKIbbCmNcIrnB9vYd2Tn8S8zISf/lbdlP9/Rtvc trainee@centos8.ittraining.loc
The key's randomart image is:
+---[ECDSA 256]---+
|                 |
|                 |
```

```
|             .  |
|          . o . |
|    . . S . * .  |
|   ..+ + +o+=.o o|
|  . o*o Bo.o B +B|
|   oo +o.o. . *+@|
|    .. ...     OE|
+----[SHA256]-----+
[trainee@centos8 ~]$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ed25519.
Your public key has been saved in /home/trainee/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:nLP4esR7UmNsc6dAqmDUufS8ORxCCI+LpaE04sXAwZw trainee@centos8.ittraining.loc
The key's randomart image is:
+--[ED25519 256]--+
|+.o              |
| E.              |
|  o+ o .         |
|oooo+ =. ..      |
|==oo o =S+       |
|+.. o o.BoO . .  |
|   . ..=.O = o   |
|      ..O . .    |
|      .o.+       |
+----[SHA256]-----+
```

Important - Les clés générées seront placées dans le répertoire **~/.ssh/**.

Créez ensuite le fichier **~/.ssh/authorized_keys** :

```
[trainee@centos8 ~]$ cat .ssh/id_rsa.pub >> .ssh/authorized_keys
[trainee@centos8 ~]$ cat .ssh/id_ecdsa.pub >> .ssh/authorized_keys
[trainee@centos8 ~]$ cat .ssh/id_ed25519.pub >> .ssh/authorized_keys
[trainee@centos8 ~]$ cat .ssh/authorized_keys
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDDKmSGaSKZ427gtXkTfzJAuOjhZYtR4nLU5j3OP8K7nTIKY7ounDVhl3vRBrgEqGJdO60DLtPSXbS32GopQ
mPcKttf7qYVb7IRUzhBntIiaEvs4dDiu86NEV1CVzQF3vYw0yEKC0jYOVuIQ/OpGjP7D8EoSMwuWozXBnR1bVVhbtS/5MQwBo6iW2kKZ+7XNWDVMm
ZkAE4Qy5D6yMMFXFio4ceAwmnid5SSNTZaMAKoUxckGPfdgBzvrWkPExHo91rk6cbmz5JDLLBweE/Ml5zLFBFLC1pAszRTXfDtDnOjC257Y0ZZlr5
4uitRofTvWOuzeDc1iYD/t7zyXBm5fizY21d5MyESgzDSaGzrfKTCYt0GarwDBs+P+PBNPodNGsEU2OUzz5kg4+gh9tGUoTRO1t0PJfd+i+1nlBTX
Hnp7K4cy/DdAYUr4siaVkAuih/EKRUF7EZVSmgy4WN2OgUDbOizeKMrLycm2WO6BvA7cNCSmo+n5Zpz154nl/xFVH48=
trainee@centos8.ittraining.loc
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCxg+k9SSk32zbrNnNTZqv8joQLTbWpoHYU6ggNRRu1Z4Nclag1rkIdwFGgHa
m6RnHX9N3fE+zie58IWYDGYOlk= trainee@centos8.ittraining.loc
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIGST4moeGWfP+y3olo5D8hntztUMSKvR/xk21Zq1BIz trainee@centos8.ittraining.loc
```

Il convient maintenant de se connecter sur la machine **targeta** en utilisant ssh et de créer le répertoire ~/.ssh :

```
[trainee@centos8 ~]$ ssh -l trainee 10.0.2.52
The authenticity of host '10.0.2.52 (10.0.2.52)' can't be established.
ECDSA key fingerprint is SHA256:sEfHBv9azmK60cjqF/aJgUc9jg56slNaZQdAUcvBOvE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.52' (ECDSA) to the list of known hosts.
Debian GNU/Linux 9
trainee@10.0.2.52's password:
Linux targeta.i2tch.loc 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
```

```
permitted by applicable law.
Last login: Sun Mar 21 08:47:45 2021 from 10.0.2.10

trainee@targeta:~$ ls -la | grep .ssh
drwx------  2 trainee trainee  4096 janv. 28  2019 .ssh

trainee@targeta:~$ exit
déconnexion
Connection to 10.0.2.52 closed.
```

Important : Notez que le mot de passe **trainee** ne sera pas en clair.

Important - Si le dossier distant .ssh n'existe pas dans le répertoire personnel de l'utilisateur connecté, il faut le créer avec des permissions de 700.

Ensuite, il convient de transférer le fichier **.ssh/authorized_keys** de la machine **centos8** vers la machine **targeta** :

```
[trainee@centos8 ~]$ scp .ssh/authorized_keys trainee@10.0.2.52:/home/trainee/.ssh/authorized_keys
Debian GNU/Linux 9
trainee@10.0.2.52's password: trainee
authorized_keys
100%  888     1.5MB/s   00:00
```

Important : Notez que le mot de passe **trainee** ne sera pas en clair.

Connectez-vous via ssh de la machine **centos8** à la machine **targeta** :

```
[trainee@centos8 ~]$ ssh -l trainee 10.0.2.52
Debian GNU/Linux 9
Linux targeta.i2tch.loc 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Mar  8 17:15:18 2022 from 10.0.2.45
trainee@targeta:~$
```

Important : Notez que l'authentification a utilisé le couple de clefs asymétrique et aucun mot de passe n'a été requis.

2.2 - sudo

La commande **sudo** permet à un utilisateur autorisé d'exécuter une commande en tant que **root** ou en tant qu'un autre utilisateur. Lors de l'exécution de la commande, l'UID et le GID effectifs et réels sont ceux de l'identité de l'utilisateur cible. L'utilisation de la commande **sudo** est une façon simple de déléguer des tâches administratives à d'autres utilisateurs sans communiquer le mot de passe de **root** et sans placer un SUID bit sur l'exécutable. La commande **sudo** est configurée grâce au fichier **/etc/sudoers**.

Consultez ensuite le fichier **/etc/sudoers** :

```
trainee@targeta:~$ su -
Mot de passe : fenestros
root@targeta:~# cat /etc/sudoers
#
```

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

Important : Notez la présence de la ligne **%sudo ALL=(ALL) ALL**. Cette ligne possède le format **Qui Où = (En tant que qui) Quoi**. La ligne implique donc que les membres du groupe **sudo** peuvent exécuter à partir de n'importe quel hôte et en tant que n'importe quel utilisateur, toutes les commandes du système. Dans ce fichier donc, un groupe est référencé par un **%**. Un nom sans ce caractère est forcément un utilisateur. Pour éditer le fichier **/etc/sudoers**, il est **nécessaire** d'utiliser la commande **visudo**.

Vérifez le contenu du fichier **/etc/sudoers.d/ansible_users** dans la VM **targeta** qui permettra à **trainee** d'utiliser la commande sudo **sans** entrer son mot de passe :

```
root@targeta:~# cat /etc/sudoers.d/ansible_users
trainee ALL=(ALL)       NOPASSWD:ALL
root@targeta:~# ls -l /etc/sudoers.d/ansible_users
-r--r----- 1 root root 31 janv. 29  2019 /etc/sudoers.d/ansible_users
```

Testez la prise en compte de vore configuration :

```
trainee@targeta:~$ sudo su -
root@targeta:~# exit
déconnexion
trainee@targeta:~$ exit
déconnexion
Connection to 10.0.2.52 closed.
[trainee@centos8 ~]$
```

Important : Notez que trainee a pu exécuter la commande **su -** via sudo sans saisir son mot de passe.
