+adlere
DIGITAL EXPERTISE

Ansible pour professionnels Linux / Unix

Johan Klotz - jklotz@adlere.fr

+adlere
DIGITAL EXPERTISE

Rôles

Des rôles, pour quoi faire ?

Provisionnement de système

configuration hardware (eg HP iLO)
configuration configuration (vlans, …)
virtualisation
installation OS
utilisateurs
stockage
services
durcissement
[…]

ROLES

Configuration

Provisionnement

Installation d'applications

Durcissement

Remédiation

- Identifier les unités logiques, les rendre ré-utilisables et partageables
- Ils doivent être agnostiques : pas de secrets ou de données spécifiques à un site

Playbook d'origine : sec_settings.yml

- Playbook utilisé dans le provisionnement d'une VM; concerne la sécurité en général

```yaml
---
- name: Various security settings
  hosts: all
  gather_facts: no


  tasks:
    - name: Setting SElinux to enforcing
      ansible.posix.selinux:
        state: enforcing
        policy: targeted


    - name: Install firewalld
      ansible.builtin.package:
        name: firewalld
        state: present


    - name: Disable firewalld
      ansible.builtin.service:
        name: firewalld
        state: stopped
        enabled: false


    - name: System reboot (timeout 300 s)
      ansible.builtin.reboot:
        reboot_timeout: 300
```

SElinux

firewall

divers

sshd

- Pas réutilisable
- susceptible de croissance organique

(suite)

```yaml
    - name: set -o vi
      ansible.builtin.blockinfile:
        insertafter: EOF
        path: /etc/profile
        state: present
        block: |
          set -o vi


    - name: Disable Root Login
      ansible.builtin.lineinfile:
        dest: /etc/ssh/sshd_config
        regexp: '^PermitRootLogin'
        line: "PermitRootLogin no"
        state: present
        backup: yes
      become: yes
      notify:
        - restart ssh


  handlers:
    - name: restart ssh
      systemd:
        name: sshd
        state: restarted
```

Évolution #1 : rôles embarqués dans le projet

- On embarque un répertoire `./roles` dans le projet

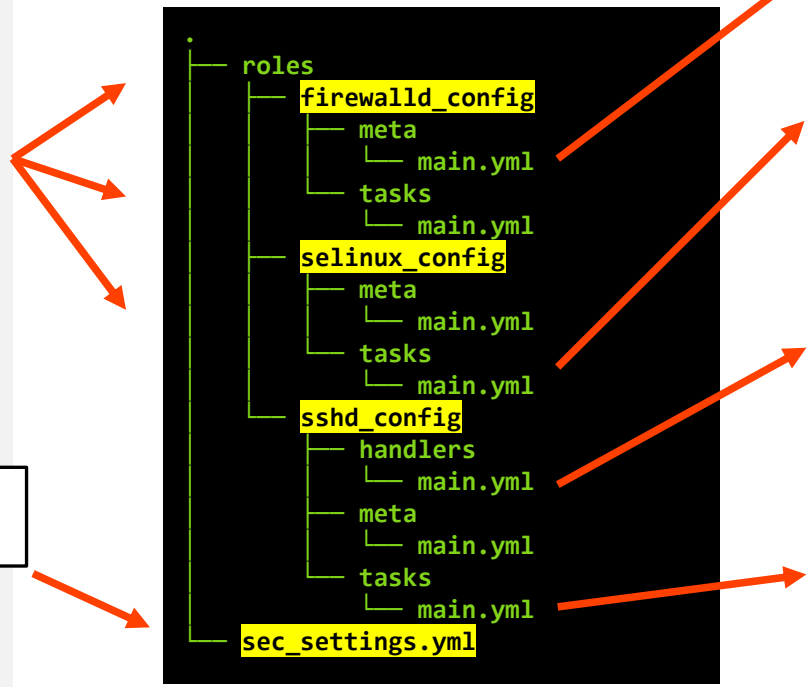
```yaml
---
- name: Various security settings
  hosts: all
  gather_facts: no

  roles:
    - firewalld_config
    - selinux_config
    - sshd_config

  tasks:
    - name: System reboot (timeout 300 s)
      ansible.builtin.reboot:
        reboot_timeout: 300

    - name: set -o vi
      blockinfile:
        insertafter: EOF
        path: /etc/profile
        state: present
        block: |
          set -o vi
```

playbook principal




```yaml
- name: Disable firewalld
  ansible.builtin.service:
    name: firewalld
    state: stopped
    enabled: false
```

```yaml
- name: Setting SElinux to enforcing
  ansible.posix.selinux:
    state: enforcing
    policy: targeted
```

```yaml
- name: restart ssh
  ansible.builtin.systemd:
    name: sshd
    state: restarted
```

```yaml
- name: SSHD ROLE | Enable Root Login
  ansible.builtin.lineinfile:
        dest: /etc/ssh/sshd_config
        regexp: '^PermitRootLogin'
        line: "PermitRootLogin no"
        state: present
        backup: yes
  become: yes
  notify:
    - restart ssh
```

- on aurait pu mettre chaque rôle directement dans le répertoire du projet
- les rôles peuvent croître indépendamment l'un de l'autre et s'enrichir
- meilleure organisation, plus lisible

Évolution #2 : rôles partagés et réutilisables

- Chaque rôle est (dé)placé dans un repository git spécifique

```
.
├── collections.yml
├── README.md
├── roles_requirements.yml
└── sec_settings.yml
```

```
$ cat collections.yml
collections:
  - ansible.posix
```

(ansible.posix nécessité par le rôle selinux)

```
$ cat roles_requirements.yml
---
- src: https://gitlab.com/myrepo/roles/firewalld_config
  scm: git
  name: firewalld_config

- src: https://gitlab.com/myrepo/roles/selinux_config
  scm: git
  name: selinux_config

- src: https://gitlab.com/myrepo/roles/sshd_config
  scm: git
  name: sshd_config
```

```
---
- name: Various security settings
  hosts: all
  gather_facts: no

  roles:
    - firewalld_config
    - selinux_config
    - sshd_config

  tasks:
    - name: System reboot (timeout 300 s)
      ansible.builtin.reboot:
        reboot_timeout: 300

    - name: set -o vi
      blockinfile:
        insertafter: EOF
        path: /etc/profile
        state: present
        block: |
          set -o vi
```

le playbook ne change pas

- rôles et collections sont décrits dans des fichiers spécifiques
- on les installe avec

```
ansible-galaxy collection install -r collections.yml
ansible-galaxy role install -r roles_requirements.yml
```

- Un repository par rôle
- Partageable, réutilisable, bonne lisibilité, peuvent croître indépendamment

Évolution #3 : appel d'un "meta"-rôle et de ses dépendances


```
.
├── collections.yml
├── README.md
├── role_requirement.yml
└── sec_settings.yml
```

```
$ cat collections.yml
collections:
  - ansible.posix
```

(ansible.posix nécessité par le rôle selinux)

```
$ cat role_requirement.yml
---
- src: https://gitlab.com/myrepo/roles/security
  scm: git
  name: security
```

```
---
- name: Various security settings
  hosts: all
  gather_facts: no

  roles:
    - security

  tasks:
    - name: System reboot (timeout 300 s)
      ansible.builtin.reboot:
        reboot_timeout: 300

    - name: set -o vi
      blockinfile:
        insertafter: EOF
        path: /etc/profile
        state: present
        block: |
          set -o vi
```

Le rôle 'security' ,'a qu'un seul fichier `meta/main.yml`, qui liste les dépendances du rôle

```
dependencies:
  - role: sshd_config
    src: https://gitlab.com/myrepo/ansible/roles/sshd_config
    scm: git
  - role: selinux_config
    src: https://gitlab.com/myrepo/ansible/roles/selinux_config
    scm: git
  - role: firewalld_config
    src: https://gitlab.com/myrepo/ansible/roles/firewalld_config
    scm: git
```

le playbook référence juste un rôle

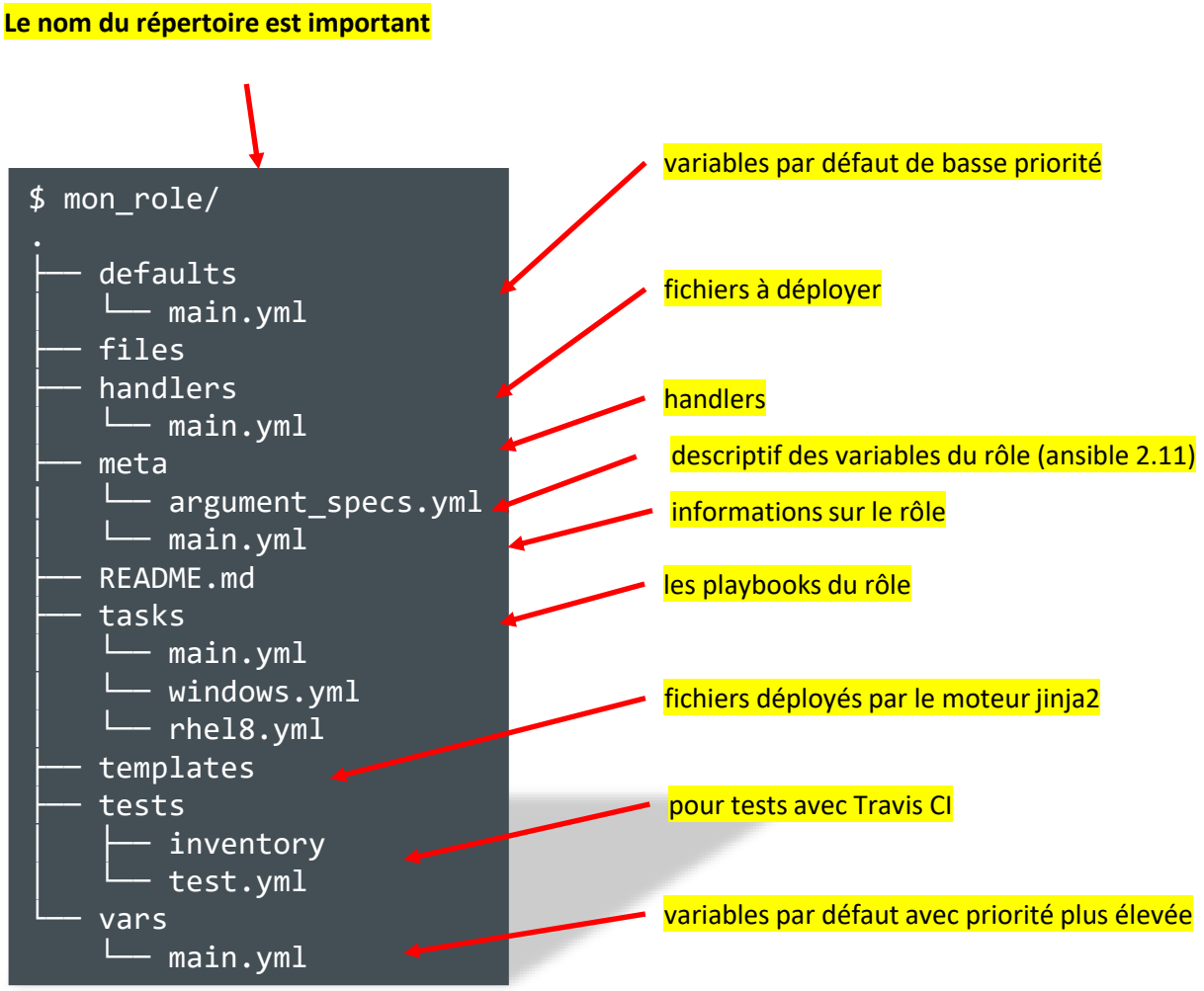
Rôle inclus dans un projet

- les rôles peuvent aller dans un sous-répertoire 'roles' du projet
- ou directement dans le projet
- ce sont des bouts de code réutilisables et partageables
- ils peuvent exister dans d'autres emplacements (chemins spécifiques à définir)

```
mon_projet/
├── ansible.cfg                 # Fichier de configuration
├── inventory/                  # Répertoire de fichiers d'inventaire
├── group_vars/                 # Répertoires des variables de groupe
├── host_vars/                  # Répertoire de variables par système
├── roles/                      # Répertoire des rôles
│   ├── common/                 # Rôle 'common'
│   │   ├── tasks/              # Playbooks du rôle
│   │   │   └── main.yml
│   │   ├── handlers/           # Handlers
│   │   ├── templates/          # Fichier template Jinja
│   │   ├── files/              # Fichiers à recopier
│   │   ├── vars/               # Variables;  internes du rôle
│   │   └── defaults/           # Variables par défaut du rôle
│   └── webserver/              # Rôle 'webserver'
│       ├── […]
├── playbooks/                  # Répertoire de playbooks
├── files/                      # Fichiers à recopier
├── templates/                  # Fichiers pour template Jinja2
└── README.md                   # Documentation
```

Rôles ansible

- Ensemble de playbooks et leurs ressources
- code générique, ré-utilisable, distribuable
- apportent structure et organisation logique aux playbooks
- nécessitent de la réflexion
- appelés à partir d'un playbook
- doivent respecter une structure définie
- `ansible-galaxy [role] init` initialise la structure



https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_reuse_roles.html

Comment créer un rôle

Manuellement de A à Z	Avec ansible-galaxy

`mkdir -p projet/roles; cd projet/roles`
`mkdir mon-role; cd mon-role`
`mkdir -v {meta,tasks}`
	`mkdir -p projet/roles; cd projet/roles`
	`ansible-galaxy role init mon-role`
	`cd mon-role`

	enlever les objets (répertoires) non utilisés
créer un fichier de tâches dans `tasks/main.yml` créer un fichier de description dans `meta/main.yml`	éditer le fichier de tâches dans `tasks/main.yml` éditer le fichier de description dans `meta/main.yml` attention à la licence dans le `README.md`

Initialiser / completer autant que possible le README.md

- nommage du rôle : un périmètre technique / entité / nom de produit, et un verbe à la fin (`sshd_configure`, `nginx_install`, …)
  - attention aux réorganisations qui changent les noms des entités
- Il n'est pas recommandé de mettre des underscores (_) dans un nom de rôle
- on peut mettre des tirets (-)
- le fichier de description est généralement optionnel, obligatoire si on veut publier sur galaxy.ansible.com

Structure d'un rôle : metadonnées


```
$ mon_role/
.
├── defaults
│   └── main.yml
├── files
├── handlers
│   └── main.yml
├── meta
│   └── argument_specs.yml
│   └── main.yml
│   └── requirements.yml
├── README.md
├── tasks
│   └── main.yml
│   └── windows.yml
│   └── rhel8.yml
├── templates
├── tests
│   ├── inventory
│   └── test.yml
└── vars
    └── main.yml
```

Aussi complet que possible SVP

main.yml

```
galaxy_info:
  author: your name
  description: your role description
  company: your company (optional)

  # If the issue tracker for your role is not on github, uncomment the
  # next line and provide a value
  # issue_tracker_url: http://example.com/issue/tracker

  # Choose a valid license ID from https://spdx.org
  license: license (GPL-2.0-or-later, MIT, etc)

  min_ansible_version: 2.15

  galaxy_tags:
    - sshd
    - linux

dependencies: []
```

```
[…]
dependencies:
    - geerlingguy.haproxy
    - name: geerlingguy.ansible
      version: 2.0.2
[…]
```

Autres façons de spécifier les dépendances :

```
---
- geerlingguy.haproxy
- name: geerlingguy.ansible
  version: 2.0.2
[…]
```

requirements.yml

Structure d'un rôle : métadonnées de argument_specs.yml


```
Lorem ipsum
```

```
$ mon_role/
.
├── defaults
│   └── main.yml
├── files
├── handlers
│   └── main.yml
├── meta
│   └── argument_specs.yml
│   └── main.yml
│   └── requirements.yml
├── README.md
├── tasks
│   └── main.yml
│   └── windows.yml
│   └── rhel8.yml
├── templates
├── tests
│   ├── inventory
│   └── test.yml
└── vars
    └── main.yml
```

Structure d'un rôle : variables


```
$ mon_role/
.
├── defaults
│   └── main.yml
├── files
├── handlers
│   └── main.yml
├── meta
│   └── argument_specs.yml
│   └── main.yml
│   └── requirements.yml
├── README.md
├── tasks
│   └── main.yml
│   └── windows.yml
│   └── rhel8.yml
├── templates
├── tests
│   ├── inventory
│   └── test.yml
└── vars
    └── main.yml
```

Variables 'métier', avec une priorité faible

```yaml
---
http_port: 8080
html_dir: /www/html
```

Variables spécifiques au fonctionnement du rôle, de priorité plus élevée.

```yaml
---
debian_package: apache2
rhel_package_name: httpd
```

Exemple #1

```yaml
roles:
  - role: apache_install
    vars:
      http_port: 8080
      debian_package: new-apache2
```

➔ les 2 variables sont redéfinies
"les variables redéfinies dans l'appel d'un rôle ont priorité sur les variables définies dans le rôle"

Exemple #2

```yaml
---
- name: Playbook install Apache
  hosts: web
  vars:
    debian_package: apache3
    http_port: 8042

  tasks:
  - role: apache_install
```

➔ `http_port` est redéfinie, pas `debian_package`
"Les variables définies dans l'en-tête d'un play on priorité sur role/defaults, mais pas sur role/vars"

Structure d'un rôle

Quelque part dans tasks/xxx.yml :

```
$ mon_role/
.
├── defaults
│   └── main.yml
├── files
├── handlers
│   └── main.yml
├── meta
│   └── argument_specs.yml
│   └── main.yml
│   └── requirements.yml
├── README.md
├── tasks
│   └── main.yml
│   └── windows.yml
│   └── rhel8.yml
├── templates
├── tests
│   ├── inventory
│   └── test.yml
└── vars
    └── main.yml
```

Répertoire pour stocker les fichiers manipulés par le module copy

```
---
- name: Relance HTTPD
  ansible.builtin.service:
    name: httpd
    state: restarted
    enabled: true
```

```
---
- name: Copie un fichier de config
  ansible.builtin.template:
    src: httpd.conf.j2
    dest: /etc/httpd/conf.d/ACME.conf
  notify: Relance HTTPD
```

Répertoire pour stocker les fichiers manipulés par le module template

Variables spécifiques au fonctionnement du rôle, non surchargeables lors de l'appel

Structure d'un rôle : fichiers de tâches


```
$ mon_role/
.
├── defaults
│   └── main.yml
├── files
├── handlers
│   └── main.yml
├── meta
│   └── argument_specs.yml
│   └── main.yml
│   └── requirements.yml
├── README.md
├── tasks
│   └── main.yml
│   └── windows.yml
│   └── rhel8.yml
├── templates
├── tests
│   ├── inventory
│   └── test.yml
└── vars
    └── main.yml
```

Fichiers de tâches du rôle
main.yml est chargé par défaut

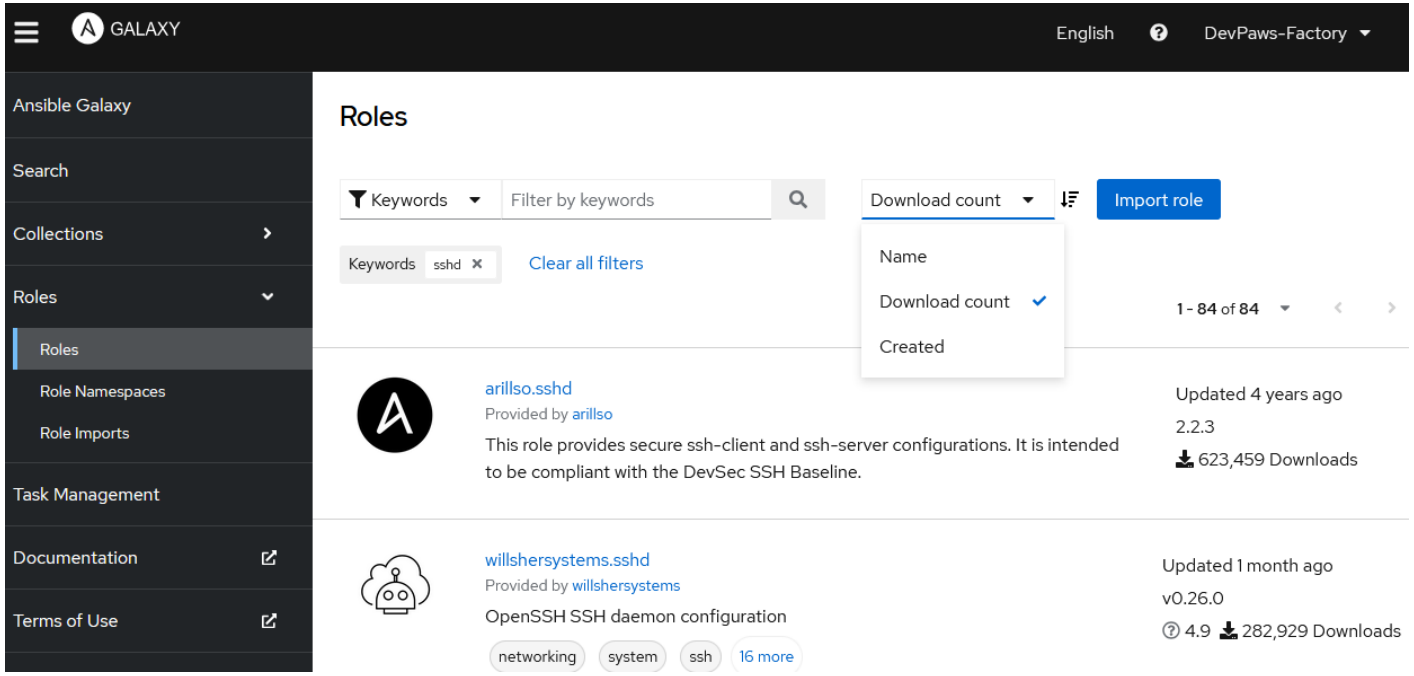
```
---
- name: SSHD_CONFIGURE | Include du fichier de tâches Debian12 ...
  ansible.builtin.import_tasks:
    file: bookworm.yml
  when:
    - ansible_facts['distribution'] == 'Debian'
    - ansible_facts['distribution_major_version'] == '12'

- name: SSHD_CONFIGURE | Include du fichier de tâches RHEL 9 ...
  ansible.builtin.import_tasks:
    file: rhel9.yml
  when:
    - ansible_facts['distribution'] == 'RedHat'
    - ansible_facts['distribution_major_version'] == '9'
```

Répertoire avec les ressources nécessaires pour valider le fonctionnement du rôle

Rôles : installation

- avec la commande ansible-galaxy [role] install
- prend un un nom de rôle en argument , un fichier, une URI
- si nom de rôle, par défaut la recherche se fait sur galaxy.ansible.com



Rôles : installation

Depuis le site galaxy.ansible.com	`ansible-galaxy role install <nom_role>`
Depuis une archive	`ansible-galaxy role install <fichier nom_role.tar.gz>`
Depuis un repo Github	PAT : `ansible-galaxy role install git+https://<PERSONAL ACCESS TOKEN>@github.com/DevPaws-Factory/sshd_harden.git` (marche aussi pour repo public) Clef SSH : `ansible-galaxy role install git+ssh://git@github.com/DevPaws-Factory/sshd_harden`

- Les dépendances de rôle sont résolues à l'installation :

```
$ ansible-galaxy role install sshd_configure.1.0.0.tgz
Starting galaxy role install process
- extracting sshd_configure.1.0.0.tgz to /home/admjkl/.ansible/roles/sshd_configure.1.0.0.tgz
- sshd_configure.1.0.0.tgz was installed successfully
- adding dependency: geerlingguy.haproxy
- adding dependency: geerlingguy.ansible (2.0.2)
- downloading role 'haproxy', owned by geerlingguy
- downloading role from https://github.com/geerlingguy/ansible-role-haproxy/archive/1.3.1.tar.gz
- extracting geerlingguy.haproxy to /home/admjkl/.ansible/roles/geerlingguy.haproxy
- geerlingguy.haproxy (1.3.1) was installed successfully
- downloading role 'ansible', owned by geerlingguy
- downloading role from https://github.com/geerlingguy/ansible-role-ansible/archive/2.0.2.tar.gz
- extracting geerlingguy.ansible to /home/admjkl/.ansible/roles/geerlingguy.ansible
- geerlingguy.ansible (2.0.2) was installed successfully
```

Installation avec un fichier de prérequis

- S'installe avec : `ansible-galaxy role install -r requirements.yml`

```
---
 roles:
 # Installe la dernière version disponible depuis Ansible Galaxy
 - name: geerlingguy.firewall

 # Installe une version spécifique, depuis Ansible Galaxy
 - name: geerlingguy.php
   version: 4.3.1

 # Installe une version spécifique  depuis GitHub
 - src: https://github.com/geerlingguy/ansible-role-passenger
   name: passenger
   version: 2.0.0

 # Installe une archive depuis un serveur web
 - src: https://www.example.com/ansible/roles/my-role-name.tar.gz
   name: my-role
```

Appeler des rôles depuis un playbook

Avec la directive "roles"

```yaml
---
- name: Mon playbook
  hosts: all
  gather_facts: no


  roles:
    - role1
    - role: role2
      vars:
        myvar: '42'
    - role: '/chemin/vers/role3'

  tasks:
    - name: Suite des tâches
```

Import (= statique)

```yaml
---
- name: Mon playbook
- hosts: all
  gather_facts: no


  tasks:
    - name: Import du role1
      ansible.builtin.import_role:
        name: role1
      vars:
        myvar: 'valeur'


    - name: Import du role2
        ansible.builtin.import_role:
          name: role2
```

Include (= dynamique)

```yaml
---
- name: Mon playbook
  hosts: all
  gather_facts: no


  tasks:
    - name: Include du role1
      ansible.builtin.include_role:
        name: role1

    - name: Include du role2
      ansible.builtin.include_role:
        name: role2
```

Emplacements de recherche par défaut

1. Dans les collections

2. dans `./roles/`, relativement au fichier du playbook

```
$ tree -L 3
.
├── ansible.cfg
├── inventory
├── main.yml
└── roles
    └── sshd_harden
        ├── defaults
        ├── files
        ├── handlers
        ├── meta
        ├── README.md
        ├── tasks
        ├── templates
        ├── tests
        └── vars
```

3. dans la directive `roles_path`, par défaut :

```
~/.ansible/roles
/usr/share/ansible/roles
/etc/ansible/roles
```

Personnalisable dans `ansible.cfg` :

```
[defaults]
roles_path = /path/to/roles
```

(ou dans la variable `ANSIBLE_ROLES_PATH`)

4. dans le répertoire du playbook

Débogage de rôle

- `ansible-playbook -vv` affiche l'emplacement du rôle exécuté

```
PLAYBOOK: main.yml ***************************
1 plays in ./main.yml

PLAY [Main playbook] *************************************

TASK [role1 : Play 1, task 1] ****************************
task path: /etc/ansible/roles/role1/tasks/main.yml:2
ok: [localhost] => {
    "msg": "This is play1, task1"
}

TASK [role2 : Play2, task 1] *****************************
task path: /etc/ansible/roles/role2/tasks/main.yml:2
ok: [localhost] => {
    "msg": "This is play2, task 1"
}
```

- Recommandé de nommer de façon explicite les tâches d'un rôle pour faciliter la compréhension à l'exécution

```
---
- name: APACHE RHEL | Installation Apache
  ansible.builtin.apt:
    name:
      - apache2
```

Résumé des commandes

Objet	Commande
Création de la structure de répertoire Créera le sous-répertoire ROLE_NAME avec les fichiers nécessaires. Recommandé : enlever le superflu	`ansible-galaxy [role] init ROLE_NAME`
Préparer un rôle pour distribution. Depuis le répertoire parent, le même où on a fait la commande d'init	`tar czvf ./ROLE_NAME.1.0.0.tar.gz ./ROLE_NAME`

Installer un rôle. Par défaut, va dans `~/.ansible/roles`	`ansible-galaxy install ./ROLE_NAME.tar.gz`
	
	`ansible-galaxy install ROLE_NAME`
	
	`[-p destination_path]`
	`[--server https://my.server.example.com]`

- guide utilisateur `ansible-galaxy` : https://docs.ansible.com/ansible/latest/cli/ansible-galaxy.html

Résumé des commandes

ansible-galaxy role	Description
`list`	Liste les rôles installés sur le système
`install`	Installe un rôle en local, par défaut dans `~/.ansible/roles` Si nom de rôle seul, télécharge depuis Galaxy Ansible ou selon `ansible.cfg`
`init`	`ansible-galaxy role init MON_ROLE`
`remove`	efface un rôle en local
`delete`	efface un rôle de Galaxy Ansible `ansible-galaxy delete github_user github_repo`
`search`	`ansible-galaxy search cyberark`
`import`	Importe un rôle de GitHub vers galaxy.ansible.com (`ansible-galaxy login` d'abord)
`info`	Affiche des informations sur un rôle donné `ansible-galaxy role info geerlingguy.haproxy`


Merci