Ansible

Marc Baudoin

Hybrix

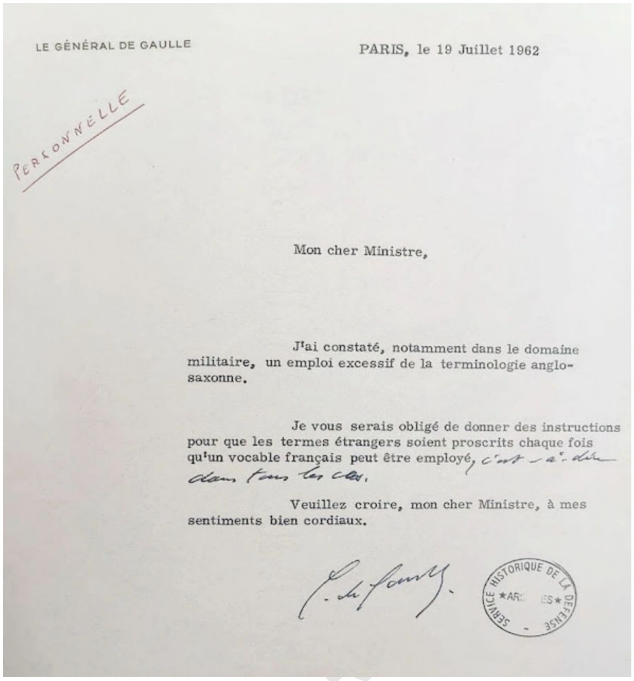
IGPDE — 19 – 20 juin 2025

Ici, c'est du fait maison, sans aucun artifice d'intelligence

Figure – https://www.uqac.ca/ressourcespedago/iag/

Figure – https://ai-label.org/

Ici, on s'exprime en français (pas en franglais)



LE GÉNÉRAL DE GAULLE

PARIS, le 19 Juillet 1962

PERSONNELLE

Mon cher Ministre,

J'ai constaté, notamment dans le domaine militaire, un emploi excessif de la terminologie anglo-saxonne.

Je vous serais obligé de donner des instructions pour que les termes étrangers soient proscrits chaque fois qu'un vocable français peut être employé, c'est-à-dire dans tous les cas.

Veuillez croire, mon cher Ministre, à mes sentiments bien cordiaux.

SERVICE HISTORIQUE DE LA DÉFENSE

Figure – https://www.fix-dessinateur.com/

Sommaire

Sommaire

IaC

- Signifie : *infrastructure as code*.
- L'IaC consiste à gérer un système informatique (l'*infrastructure*) au moyen de fichiers de définition (le *code*) plutôt que grâce à de nombreuses opérations manuelles — idéalement regroupées dans des scripts afin d'atteindre un certain niveau d'automatisation — effectuées par des administrateurs.

`https://fr.wikipedia.org/wiki/Infrastructure_as_code`
`https://infrastructure-as-code.com/`

Gestion de configuration

Problématique

- Dans des temps pas si anciens, un gros centre informatique se composait au plus de quelques dizaines de serveurs, souvent hétérogènes.
- Aujourd'hui, un gros centre informatique se compose de plusieurs centaines de serveurs virtualisés, souvent organisés en groupes de serveurs identiques pour des raisons de redondance.
- Comment assurer la gestion de ces serveurs, de manière cohérente, simple et la plus automatisée possible ?

Gestion de configuration

De quoi s'agit-il ?

- La gestion de configuration a pour objectifs :
  - de décrire la configuration d'un système informatique ;
  - de l'appliquer de manière automatique.
- La configuration du système informatique est contenue dans un ensemble de fichiers appelé CMDB (*configuration management database*).
- Outre son utilité pour la gestion de configuration, la CMDB a également d'indéniables qualités documentaires.
- En corollaire, la gestion de configuration permet également :
  - de conserver l'historique des configurations successives (en mettant la CMDB sous contrôle de versions) ;
  - de détecter et de corriger les configurations non conformes.
- Attention : il est illusoire d'espérer utiliser de la gestion de configuration sans savoir au préalable réaliser manuellement les mêmes opérations.

https://fr.wikipedia.org/wiki/Gestion_de_configuration
https://fr.wikipedia.org/wiki/Configuration_management_database
https://cfgmgmtcamp.org/

Gestion de configuration

Idempotence

- Le concept d'*idempotence* est fondamental en gestion de configuration.
- En mathématiques, une application f est dite *idempotente* si et seulement si :

$$f \circ f = f \qquad \text{(le symbole } \circ \text{ se dit } \textit{rond}\text{, il s'agit de la composition)}$$

c'est-à-dire si et seulement si :

$$\forall x \; f(f(x)) = f(x)$$

- Une opération est donc idempotente si elle a le même effet lorsqu'on l'effectue une fois ou deux fois de suite et ainsi, par récurrence, plusieurs fois de suite.

https://fr.wikipedia.org/wiki/Composition_de_fonctions
https://fr.wikipedia.org/wiki/Idempotence

Gestion de configuration

Quels logiciels peut-on utiliser ?

Ansible
- pas d'agent sur les machines à gérer (mais il y a des prérequis)
- la communication avec les machines à gérer se fait au moyen de leur protocole natif (SSH, WinRM, REST...)
- écrit en Python

CFEngine
- modèle agent-serveur
- écrit en C
- utilise un langage de description complexe

Chef
- modèle agent-serveur
- écrit en Ruby

Puppet
- modèle agent-serveur (sauf Bolt)
- écrit en Ruby

Salt
- modèle agent-serveur
- écrit en Python

https://en.wikipedia.org/wiki/Comparison_of_open-source_configuration_management_software

Ansible

Principe

- Ansible est simple et léger à mettre en œuvre.
- Ansible fonctionne sans agent sur les machines à gérer.
- Ansible utilise le protocole de communication habituel des machines à gérer.
- Ansible utilise des fichiers de description (la CMDB) au format YAML.
- Ansible a été créé par Michael DeHaan.

https://www.ansible.com/
https://docs.ansible.com/
https://forum.ansible.com/
https://fr.wikipedia.org/wiki/Ansible_(logiciel)
https://www.reddit.com/r/ansible/
https://stackoverflow.com/questions/tagged/ansible
https://www.youtube.com/c/AnsibleAutomation
https://www.learnlinux.tv/getting-started-with-ansible/

Ansible

Catégories de machines

- Ansible distingue deux catégories de machines :
  - la machine de contrôle (*control node*), sur laquelle Ansible est installé (cette machine ne peut pas fonctionner sous Windows)
  - les machines à gérer (*managed nodes*), sur lesquelles l'installation d'un agent spécifique n'est pas nécessaire
- La machine de contrôle communique avec les machines à gérer en utilisant :

  SSH pour les machines à gérer fonctionnant sous UNIX
  WinRM pour les machines à gérer fonctionnant sous Windows
- Les actions sur les machines à gérer sont effectuées au moyen de :

  Python pour les machines à gérer fonctionnant sous UNIX
  PowerShell pour les machines à gérer fonctionnant sous Windows

https://docs.ansible.com/ansible/latest/getting_started/basic_concepts.html#control-node
https://docs.ansible.com/ansible/latest/getting_started/basic_concepts.html#managed-nodes

Ansible

Cycle de vie

- Ansible a été restructuré à partir du début de 2021 et, depuis, est composé de deux parties complémentaires :
  - `ansible-core` (nommé au départ `ansible-base`)
    - contient les outils et les modules élémentaires
    - les trois versions les plus récentes (l'actuelle et les deux précédentes) bénéficient de correctifs (toutes les trois semaines)
  - `ansible`
    - contient de nombreuses collections gérées par la communauté
    - seule la version actuelle bénéficie de correctifs (toutes les trois semaines)
    - une nouvelle version majeure tous les six mois, peu après la sortie de la nouvelle version d'`ansible-core`
    - suit les règles de gestion sémantique de version

https://docs.ansible.com/ansible/latest/reference_appendices/release_and_maintenance.html
https://groups.google.com/g/ansible-announce
https://semver.org/lang/fr/

Ansible

Cycle de vie

ansible-base 2.10.0	2020-08-13	ansible 3.0.0	2021-02-18
ansible-core 2.11.0	2021-04-26	ansible 4.0.0	2021-05-18
ansible-core 2.12.0	2021-11-08	ansible 5.0.0	2021-11-30
ansible-core 2.13.0	2022-05-16	ansible 6.0.0	2022-06-21
ansible-core 2.14.0	2022-11-07	ansible 7.0.0	2022-11-22
ansible-core 2.15.0	2023-05-15	ansible 8.0.0	2023-05-30
ansible-core 2.16.0	2023-11-06	ansible 9.0.0	2023-11-21
ansible-core 2.17.0	2024-05-20	ansible 10.0.0	2024-06-04
ansible-core 2.18.0	2024-11-04	ansible 11.0.0	2024-11-19
ansible-core 2.19.0	2025-07-21	ansible 12.0.0	2025-08-05
ansible-core 2.20.0	2025-11-??	ansible 13.0.0	2025-11-??

Table – *Correspondances entre versions d'*`ansible-core` *et d'*`ansible`

https://docs.ansible.com/ansible/devel/roadmap/ansible_core_roadmap_index.html
https://docs.ansible.com/ansible/devel/roadmap/ansible_roadmap_index.html
https://docs.ansible.com/ansible/latest/porting_guides/porting_guides.html

Ansible

Certification Red Hat

- Les plus intrépides peuvent tenter l'examen de certification EX294 (anciennement EX407) proposé par Red Hat :
  - l'inscription coûte 530 € HT
  - l'examen dure 4 h
  - la certification est valable pendant 3 ans

https://www.redhat.com/fr/services/training/ex294-red-hat-certified-engineer-rhce-exam-red-hat-enterprise-linux-9

Ansible

Interfaces Web

- Plusieurs interfaces Web permettent de faire fonctionner Ansible :

  Automation controller (anciennement Ansible Tower) est un logiciel commercialisé par Red Hat

  AWX est le logiciel libre parrainé par Red Hat dont certaines versions sont utilisées pour concevoir Automation controller

  Semaphore UI est un logiciel libre offrant une solution extérieure à Red Hat

- Attention, ces logiciels permettent d'exécuter Ansible — et ils offrent des possibilités intéressantes dont Ansible ne dispose pas — mais ils ne dispensent en aucun cas d'avoir à mettre au point les fichiers de la CMDB.

https://www.redhat.com/fr/technologies/management/ansible/automation-controller
https://www.ansible.com/community/awx-project
https://www.ansible-semaphore.com/
https://www.learnlinux.tv/complete-ansible-semaphore-tutorial-from-installation-to-automation/

Sommaire

Installation sur la machine de contrôle

BSD

- Paquet `py311-ansible` sur FreeBSD :

```
# pkg install py311-ansible
```

  On peut aussi utiliser les ports.

- Paquet `ansible`[1] sur NetBSD :

```
# pkgin install ansible
```

  On peut aussi utiliser pkgsrc.

- Paquet `ansible` sur OpenBSD :

```
# pkg_add ansible
```

  On peut aussi utiliser les ports.

1. `https://cdn.netbsd.org/pub/pkgsrc/current/pkgsrc/sysutils/ansible/`

Installation sur la machine de contrôle

Linux

- Paquet `ansible` sur Red Hat Enterprise Linux (dans le dépôt EPEL [2]) et Fedora [3] :

```
# dnf install epel-release
# dnf install ansible
```


2. https://docs.ansible.com/ansible/latest/installation_guide/installation_distros.html#installing-ansible-from-epel
3. https://docs.ansible.com/ansible/latest/installation_guide/installation_distros.html#installing-ansible-on-fedora-linux
   https://www.theurbanpenguin.com/ansible-rhce-the-new-system-administration-3/
   https://www.youtube.com/watch?v=9eHtelvVi6o

Installation sur la machine de contrôle

Linux

- Paquet `ansible` sur Debian [4] et Ubuntu [5] :

```
# apt install ansible
```

- Sur Ubuntu, il est possible d'installer une version d'Ansible plus récente que celle du dépôt Ubuntu en utilisant un dépôt PPA [6] (*Personal Package Archives*) :

```
$ sudo add-apt-repository -P ppa:ansible/ansible
$ sudo apt install ansible
```


4. https://docs.ansible.com/ansible/latest/installation_guide/installation_distros.html#installing-ansible-on-debian
5. https://docs.ansible.com/ansible/latest/installation_guide/installation_distros.html#installing-ansible-on-ubuntu
6. https://launchpad.net/~ansible
   https://www.youtube.com/watch?v=pJjUkogMtpE

Sommaire

Fichiers de configuration

- Les fichiers de configuration d'Ansible se trouvent dans le répertoire `/etc/ansible` :

  `/etc/ansible/ansible.cfg` paramétrage
  `/etc/ansible/hosts` inventaire
  `/etc/ansible/roles` répertoire contenant les rôles

- Ces fichiers ne sont généralement pas utilisés parce qu'il est possible de placer des fichiers équivalents dans la CMDB, ce qui offre plus de souplesse.

Paramétrage d'Ansible

- Le fichier `/etc/ansible/ansible.cfg` contient les paramètres de fonctionnement d'Ansible.
- Il s'agit d'un fichier au format INI.
- Plus généralement, Ansible obtient son paramétrage, dans cet ordre, depuis le premier des fichiers suivants qui existe (les suivants, s'ils existent également, sont ignorés) :
  1. le fichier dont le chemin d'accès absolu est indiqué par la variable d'environnement `ANSIBLE_CONFIG`
  2. `./ansible.cfg`
  3. `~/.ansible.cfg`
  4. `/etc/ansible/ansible.cfg`

---

https://docs.ansible.com/ansible/latest/installation_guide/intro_configuration.html

https://www.youtube.com/watch?v=7zT0j2S6I2w

https://www.youtube.com/watch?v=RM7dguUv21A

https://fr.wikipedia.org/wiki/Fichier_INI

La commande `ansible-config`

- La commande `ansible-config` permet d'afficher le paramétrage d'Ansible :

`init` affiche le paramétrage exhaustif avec des commentaires et la valeur par défaut de chaque paramètre :

```
$ ansible-config init > ansible.cfg
```

avec l'option `--disabled`, les paramètres sont commentés :

```
$ ansible-config init --disabled > ansible.cfg
```

`view` affiche le paramétrage actuel :

```
$ ansible-config view
```

---

https://docs.ansible.com/ansible/latest/cli/ansible-config.html

Inventaire

Inventaire statique

- L'inventaire répertorie les machines gérées par Ansible :

hosts

```
[test]
test1.example.com
test2.example.com

[web]
www.example.com
www-dev.example.com
```

- Le format d'inventaire le plus utilisé est le format INI :
  - les groupes (dont les noms choisis arbitrement sont entre crochets) rassemblent les machines devant subir le même traitement
  - les machines peuvent être indiquées par nom (FQDN) ou adresse IP
- Le chemin d'accès de l'inventaire est indiqué par le paramètre de configuration `inventory` ou l'une des options `-i`, `--inventory` et `--inventory-file`.

https://docs.ansible.com/ansible/latest/inventory_guide/intro_inventory.html
https://www.theurbanpenguin.com/ansible-inventory/
https://www.youtube.com/watch?v=qyFw0nR4eaw
https://fr.wikipedia.org/wiki/Fichier_INI

Inventaire

Inventaire statique

- Il est aussi possible d'indiquer, pour chaque machine, un alias (un nom symbolique) couplé à la variable `ansible_host`, dont la valeur indique le nom ou l'adresse IP de la machine :

hosts

```
[test]
test1   ansible_host=test1.example.com
test2   ansible_host=198.51.100.2
```

Inventaire

Inventaire dynamique

- Si le fichier d'inventaire est exécutable — on parle alors de *script d'inventaire* —, il est exécuté et sa sortie standard — qui doit être au format JSON (*JavaScript Object Notation*) — fournit l'inventaire :

```
{
        "test": {
                "hosts": [ "test1.example.com" , "test2.example.com" ]
        }
}
```

- Un script d'inventaire est censé accepter les options :

`--list` pour afficher tout l'inventaire

`--host <nom d'hôte>` pour n'afficher que les variables de l'hôte indiqué

https://docs.ansible.com/ansible/latest/dev_guide/developing_inventory.html
https://www.json.org/
https://fr.wikipedia.org/wiki/JavaScript_Object_Notation

Inventaire

Répertoire d'inventaire

- Il est aussi possible d'indiquer un répertoire en tant qu'inventaire.
- Ce répertoire doit contenir des fichiers dont le contenu est :
  - soit un inventaire statique
  - soit un inventaire dynamique
- Dans ce cas, l'ensemble cumulé des fichiers contenus dans ce répertoire est utilisé comme inventaire.

https://docs.ansible.com/ansible/latest/inventory_guide/intro_inventory.html#organizing-inventory-in-a-directory

La commande ansible-inventory

- La commande ansible-inventory permet d'afficher l'inventaire (par défaut au format JSON) :

`--list` affiche l'inventaire complet :

```
$ ansible-inventory --list
[...]
```

`--graph` affiche l'inventaire sous la forme d'un arbre :

```
$ ansible-inventory --graph
@all:
  |--@ungrouped:
  |--@test:
  |  |--test1.example.com
  |  |--test2.example.com
```

https://docs.ansible.com/ansible/latest/cli/ansible-inventory.html

Organisation des fichiers

- Ansible n'impose aucune structure particulière pour les fichiers de la CMDB mais il est courant de les organiser en ayant un répertoire par projet, contenant :

`ansible.cfg` configuration du projet
`hosts` inventaire du projet
`roles` rôles du projet
`*.yml` livrets du projet

```
<projet>/
├── ansible.cfg
├── hosts
├── roles/
├── livret-1.yml
├── livret-2.yml
└── ...
```

ansible.cfg

```
[defaults]
inventory = hosts
```

Sommaire

Communication entre machines

- Ansible utilise SSH pour communiquer avec les machines à gérer fonctionnant sous UNIX.
- Quel compte peut-on utiliser pour se connecter aux machines distantes ?
- Deux approches sont acceptables en matière de sécurité :
  - `root` avec authentification par clé
  - compte non privilégié puis utilisation de `sudo` pour effectuer une élévation de privilèges

La deuxième approche permet une meilleure traçabilité des actions de `root` sur les machines distantes lorsqu'on travaille directement en ligne de commande sur les machines à gérer mais elle est plus limitée dans le cadre de l'utilisation d'Ansible puisque la seule commande qu'il exécute est `python` et que `sudo` journalise uniquement la ligne de commande exécutée et pas le contenu du script que `python` interprète.

Clés SSH

- Création d'un couple de clés sur la machine de contrôle :

```
$ ssh-keygen -t ed25519
```

- Transfert de la clé publique depuis la machine de contrôle vers une machine à gérer :
  - en utilisant un compte utilisateur identique à celui de la machine de contrôle :

```
$ ssh-copy-id test1.example.com
```

  - en utilisant un compte utilisateur différent de celui de la machine de contrôle :

```
$ ssh-copy-id root@test1.example.com
```

---

https://www.theurbanpenguin.com/up-and-running-with-ansible-configuration-management/

Clés SSH

- Afin d'éviter d'avoir à saisir de manière répétée la phrase de passe de la clé privée, il est préférable de l'enregistrer en mémoire.
- Pour cela, il faut lancer l'agent SSH s'il ne l'est pas déjà :

```
$ eval `ssh-agent`
Agent pid 1664
```

```
$ eval $(ssh-agent)
Agent pid 1664
```

- Puis on peut mémoriser la clé privée et sa phrase de passe :

```
$ ssh-add
[...]
```

Tests de communication

- Le module `ansible.builtin.ping` permet de savoir si la communication avec les machines indiquées dans l'inventaire se fait correctement :

```
$ ansible -m ansible.builtin.ping all
test1.example.com | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
test2.example.com | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```


Tests de communication

- S'il est nécessaire de se connecter sous l'identité d'un utilisateur différent de celui qui exécute la commande `ansible`, il faut utiliser l'option `-u` suivie de l'identifiant de cet utilisateur :

```
$ ansible -m ansible.builtin.ping -u root all
[...]
```

Tests de communication

- Le module `ansible.builtin.setup` récupère et affiche de nombreuses informations factuelles (*facts*) stockées par Ansible dans des variables :

```
$ ansible -m ansible.builtin.setup all
test1.example.com | SUCCESS => {
    "ansible_facts": {
        "ansible_all_ipv4_addresses": [
            "198.51.100.33"
        ],
        "ansible_all_ipv6_addresses": [
            "2001:db8:1234:5678:cafe:abba:d0d0:c0c0",
            "fe80::cafe:abba:d0d0:c0c0"
        ],
[...]
```

https://www.youtube.com/watch?v=dGjId7RSLek

Commande *ad hoc*

- Cette façon d'utiliser un module au moyen de la commande `ansible` constitue une commande *ad hoc* (pour cela).
- Une commande *ad hoc* permet d'effectuer une action ponctuelle au moyen d'un des modules d'Ansible sans utiliser la CMDB.
- Par conséquent, une commande *ad hoc* n'a pas vocation à être réutilisable.

https://docs.ansible.com/ansible/latest/command_guide/intro_adhoc.html
https://www.youtube.com/watch?v=-ytUl6sl9Bw

Sommaire

YAML

- YAML signifie : *YAML Ain't Markup Language* (acronyme récursif).
- Il s'agit d'un format général de représentation de données.
- YAML est le format utilisé par Ansible pour représenter la CMDB.
- La commande `yamllint` (paquet `yamllint` sur toutes les distributions) permet de vérifier la syntaxe d'un fichier au format YAML.

---

https://yaml.org/
https://fr.wikipedia.org/wiki/YAML
https://yaml-multiline.info/
https://docs.ansible.com/ansible/latest/reference_appendices/YAMLSyntax.html
https://github.com/adrienverge/yamllint
https://www.redhat.com/sysadmin/check-yaml-yamllint

Exemple

coquillettes.yml

```
---
recette: coquillettes au beurre
convives: 1
ingrédients:
  - ingrédient: coquillettes
    quantité: 70g
  - ingrédient: beurre
    quantité: 15g
étapes:
  - faire bouillir l'eau
  - faire cuire les coquillettes dedans
  - les égoutter
  - mettre du beurre
# en variante, ajouter du fromage
```

- Un fichier YAML a généralement une extension `.yml`.
- Un fichier YAML est censé commencer par une ligne contenant trois tirets. Ce n'est plus indispensable pour Ansible mais c'est une habitude qu'on a tendance à respecter.
- Les commentaires commencent par un croisillon `#` et se poursuivent jusqu'à la fin de la ligne.

Collections

- Un fichier YAML peut contenir deux types de structures de données (qu'on appelle *collections* en terminologie YAML) :

  des *séquences* contenant des éléments ordonnés :

```
- faire bouillir l'eau
- faire cuire les coquillettes dedans
- les égoutter
- mettre du beurre
```

  des *correspondances* (*mappings*) contenant des éléments (leur ordre est sans importance) composés d'une clé (unique) et d'une valeur :

```
recette: coquillettes au beurre
convives: 1
```

Style des collections

- Les collections peuvent s'écrire selon deux styles :

  le *style en bloc* (*block style*)

```
- entrée
- plat
- dessert
```

```
manger: choucroute
boire: bière
```

  le *style en flux* (*flow style*)

```
[ entrée , plat , dessert ]
```

```
{ manger: choucroute , boire: bière }
```


Imbrication des collections

- Les collections peuvent être imbriquées.
- L'indentation — généralement de deux espaces — est importante car elle traduit l'imbrication des collections.
- Il faut utiliser des espaces pour l'indentation, pas des tabulations (si l'on utilise `vi` ou Vim, la commande `:set list` permet de matérialiser visuellement les tabulations et les fins de ligne).
- Ici, par exemple, la valeur de l'élément de correspondance est une séquence dont chaque élément est une correspondance :

```
ingrédients:
  - ingrédient: coquillettes
    quantité: 70g
  - ingrédient: beurre
    quantité: 15g
```

- Toutes les combinaisons possibles sont autorisées.

Éditeurs de texte

Vim

- Le format YAML impose un respect très strict de l'alignement vertical des éléments de même niveau hiérarchique.
- L'option `cursorcolumn` (ou sa forme abrégée `cuc`) permet de matérialiser visuellement la ligne verticale sur laquelle se trouve le curseur, ce qui facilite l'alignement vertical des éléments. Ceci peut se faire :
  - ponctuellement, pour la session en cours :

```
:set cursorcolumn
```

```
:set cuc
```

  - de manière systématique, dans le fichier de configuration de Vim :

~/.vimrc
```
set cursorcolumn
```

~/.vimrc
```
set cuc
```

---

http://vimdoc.sourceforge.net/htmldoc/options.html#'cursorcolumn'

Éditeurs de texte

Les autres

- D'autres éditeurs de texte disposent d'un mécanisme de matérialisation de la ligne verticale sur laquelle se trouve le curseur.
- GNU nano gère — enfin — la coloration syntaxique de fichiers au format YAML depuis la version 6.0 (2021-12-15).

Sommaire

Sommaire

Généralités

Les livrets

- Les livrets (*playbooks*) sont les fichiers élémentaires constituant la CMDB d'Ansible.
- Les livrets sont des fichiers au format YAML.

- D'après le Wiktionnaire anglophone, le mot *playbook* signifie :
  1. *A book containing the text of a play or plays.*
  2. *A book of games and amusements for children.*
  3. *(US, American football) A book of strategies (plays) for use in American football (and by extension other sports or disciplines).*
  4. *(US, figurative) A set of commonly employed tactics and strategies.*

https://docs.ansible.com/ansible/latest/playbook_guide/playbooks.html
https://en.wiktionary.org/wiki/playbook

Généralités

Exemple

principes.yml

```
---
- name: Premier livret tout simple
  hosts: test
  tasks:
    - name: Commande id
      ansible.builtin.command:
        cmd: id
    - name: Commande uname -a
      ansible.builtin.command:
        cmd: uname -a
```

- Structure générale :
  - `name` description du livret ou de la tâche
  - `hosts` groupe (ou machine) concerné dans l'inventaire
  - `tasks` liste des tâches (traitements) à effectuer
- Et le plus important :

  `ansible.builtin.command` module à utiliser suivi de ses paramètres

  Il existe de nombreux autres modules, chacun ayant une fonction spécifique.

https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_intro.html
https://www.youtube.com/watch?v=h3EcXPGmR7g

La commande ansible-playbook

- Pour faire en sorte d'appliquer le contenu d'un livret aux machines concernées, on utilise la commande ansible-playbook :

```
$ ansible-playbook -v principes.yml
```

- L'option -v permet d'afficher le détail des tâches. On peut augmenter le nombre de v (-vv, -vvv, -vvvv, -vvvvv) pour afficher encore plus d'informations.
- Il n'y a aucune raison d'exécuter la commande ansible-playbook sous l'identité du super-utilisateur (root) sur la machine de contrôle. La commande ansible-playbook doit toujours être exécutée sous l'identité d'un utilisateur non privilégié.
- La commande ansible-playbook dispose de nombreuses options. Pour en afficher la liste :

```
$ ansible-playbook -h
```

https://docs.ansible.com/ansible/latest/cli/ansible-playbook.html

La commande ansible-playbook

- L'une des options de la commande ansible-playbook les plus utiles est l'option -C (ou --check) qui permet d'afficher ce qui se produirait en l'absence de cette option sans effectuer aucune modification sur les machines à gérer (*dry run*) :

```
$ ansible-playbook -vC livret.yml
```

- Cette option fonctionne correctement avec la majorité des modules mais certains, en raison de leur mode de fonctionnement, ne donneront pas un résultat fiable.

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

Généralités

remote_user

principes-remote_user.yml

```
---
- name: Connexion sous l'identité d'un utilisateur spécifique
  hosts: test
  remote_user: root
  tasks:
    - name: Commande id
      ansible.builtin.command:
        cmd: id
    - name: Commande uname -a
      ansible.builtin.command:
        cmd: uname -a
```

`remote_user` identifiant à utiliser pour se connecter par SSH

Généralités

become

principes-become-1.yml

```
---
- name: Changement d'identité
  hosts: test
  remote_user: ansible
  become: true
  #become_user: root
  #become_method: sudo
  tasks:
    - name: Commande id
      ansible.builtin.command:
        cmd: id
    - name: Commande uname -a
      ansible.builtin.command:
        cmd: uname -a
```

`become` indique qu'il faut changer d'identité

`become_user` identifiant de l'utilisateur qu'il faut devenir (`root` par défaut)

`become_method` méthode à utiliser pour le changement d'identité (`sudo` par défaut)

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

Généralités

become

- L'option `-K` (ou `--ask-become-pass`) de la commande `ansible-playbook` permet la saisie du mot de passe destiné à `sudo` :

```
$ ansible-playbook -vK principes-become-1.yml
```


Généralités

become

- Il est possible de changer d'identité au niveau d'une seule tâche, en application du *principe de moindre privilège*.

principes-become-2.yml

```
---
- name: Changement d'identité
  hosts: test
  tasks:
    - name: Commande id normale
      ansible.builtin.command:
        cmd: id
    - name: Commande id privilégiée
      ansible.builtin.command:
        cmd: id
      become: true
    - name: Commande id normale
      ansible.builtin.command:
        cmd: id
```


https://fr.wikipedia.org/wiki/Principe_de_moindre_privilège

Sommaire

Les variables

Principe

- La documentation d'Ansible recense pas moins de 22 façons différentes de définir des variables.
- Pour rester simple, les façons les plus utilisées de définir des variables sont (dans l'ordre de priorité) :
  1. sur la ligne de commande
  2. dans le livret
  3. par Ansible
  4. dans l'inventaire

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

Les variables

Variables définies sur la ligne de commande

```
$ ansible-playbook -v -e var=toto variables-lignecom.yml
```

```
$ ansible-playbook -v --extra-vars var=toto variables-lignecom.yml
```

variables-lignecom.yml

```
---
- name: Variables définies sur la ligne de commande
  hosts: test
  tasks:
    - name: Affichage de la variable var
      ansible.builtin.debug:
        msg: 'La variable var contient : {{ var }}'
```

https://www.theurbanpenguin.com/passing-ansible-variables-from-the-command-line/

Les variables

Variables définies dans le livret et variables définies par Ansible

variables-livret-ansible.yml

```
---
- name: Variables définies dans le livret et variables définies par Ansible
  hosts: test
  become: true
  vars:
    fichier: gopher
    version: 1.0
  tasks:
    - name: Copie du fichier de configuration
      ansible.builtin.copy:
        src: test-{{ fichier }}-{{ version }}-{{ ansible_os_family }}.conf
        dest: /etc/{{ fichier }}.conf
        owner: root
        group: root
        mode: '444'
```

Les variables

Variables définies dans l'inventaire

/etc/ansible/hosts

```
[test]
test1.example.com var=test1
test2.example.com var=test2
```

variables-inventaire.yml

```
---
- name: Variables définies dans l'inventaire
  hosts: test
  tasks:
    - name: Affichage de la variable var
      ansible.builtin.debug:
        msg: 'La variable var contient : {{ var }}'
```

/etc/ansible/hosts

```
[test]
test1.example.com
test2.example.com

[test:vars]
ansible_user=ansible
ansible_become_pass=toto
```

https://www.theurbanpenguin.com/using-ansible-variables-in-inventory-files/

Les variables

Guillemets

- Toute valeur d'un élément de collection YAML (séquence ou correspondance) qui commence par une variable doit être placée entre guillemets :

variables-guillemets.yml

```
---
- name: Variables et guillemets
  hosts: test
  vars:
    srv: mr-fabulous
    clt: blues-brothers
  tasks:
    - name: Test avec des guillemets
      ansible.builtin.debug:
        msg: "{{ item }}.example.com"
      loop:
        - "{{ srv }}"
        - "{{ clt }}"
```

https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_variables.html#when-to-quote-variables-a-yaml-gotcha

Les variables

Filtres

- Les *filtres* permettent d'effectuer des traitements sur le contenu des variables lors de leur utilisation (le contenu des variables n'est pas modifié) :

variables-filtres.yml

```
---
- name: Variables et filtres
  hosts: test
  vars:
    test: GRAND
  tasks:
    - name: Sans filtre
      ansible.builtin.debug:
        msg: "{{ test }}"
    - name: Avec filtre
      ansible.builtin.debug:
        msg: "{{ test | lower }}"
```

https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_filters.html
https://jinja.palletsprojects.com/en/3.1.x/templates/#builtin-filters

Sommaire

Les conditions

- Une tâche peut n'être exécutée que si une condition est vérifiée.
- La condition est indiquée par l'instruction when.

Attention

La syntaxe de l'instruction when est inhabituelle :

- les variables ne doivent pas être utilisées entre des paires d'accolades
- les chaînes de caractères doivent être entourées par des apostrophes

when.yml

```
---
- name: Conditions
  hosts: test
  become: true
  tasks:
    - name: Paquet apache2 sur debianoïde
      ansible.builtin.package:
        name: apache2
        state: present
      when: ansible_os_family == 'Debian'
    - name: Paquet httpd sur redhatoïde
      ansible.builtin.package:
        name: httpd
        state: present
      when: ansible_os_family == 'RedHat'
```

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

https://jinja.palletsprojects.com/en/3.1.x/templates/#builtin-tests

https://www.youtube.com/watch?v=x-sQpE1S9kQ

Sommaire

Les boucles

Principe

- Il est possible d'exécuter plusieurs fois le même module avec certains paramètres différents au moyen d'une *boucle*.
- Dans la boucle, la variable `item` prendra successivement les valeurs de la séquence suivant l'instruction `loop`.
- Cette instruction `loop` a été ajoutée dans la version 2.5 d'Ansible, sortie en mars 2018. Auparavant, on utilisait — et on peut toujours utiiser aujourd'hui — une dizaine de syntaxes `with_<type>`, avec un `<type>` différent pour chaque type de boucle possible.

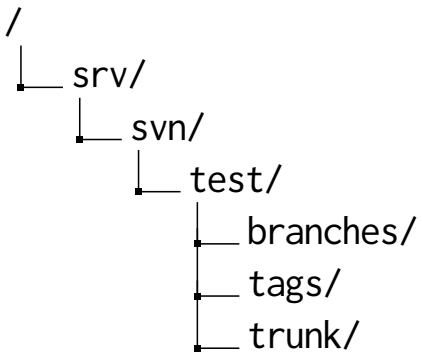
https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_loops.html

Les boucles

Exemple de boucle simple

boucle-simple.yml

```
---
- name: Boucle simple
  hosts: test
  become: true
  vars:
    projet_svn: test
  tasks:
    - name: Répertoires standards SVN
      ansible.builtin.file:
        path: /srv/svn/{{ projet_svn }}/{{ item }}
        state: directory
        owner: root
        group: root
        mode: '755'
      loop: [ branches, tags, trunk ]
```



Les boucles

Exemple de boucle sur une correspondance

boucle-correspondance.yml

```
---
- name: Boucle sur une correspondance
  hosts: test
  become: true
  vars:
    crt: /etc/pki/tls/certs/{{ inventory_hostname }}-crt.pem
    key: /etc/pki/tls/private/{{ inventory_hostname }}-key.pem
  tasks:
    - name: Droits d'accès sur la clé privée et le certificat TLS
      ansible.builtin.file: path={{ item.path }} mode={{ item.mode }}
      loop:
        - { path: "{{ crt }}" , mode: '444' } # noqa: yaml[commas]
        - { path: "{{ key }}" , mode: '400' } # noqa: yaml[commas]
```


Sommaire

Les modèles

Principe

- Les modèles (*templates*) sont des fichiers situés sur la machine de contrôle dans lesquels Ansible effectue diverses transformations avant de transférer le résultat sur les machines à gérer.
- Ansible utilise à cet effet une bibliothèque pour le langage de programmation Python appelée Jinja2.

---

https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_templating.html
https://palletsprojects.com/p/jinja/
https://fr.wikipedia.org/wiki/Jinja_(moteur_de_template)
https://jpmens.net/2020/09/29/using-ansible-managed/
https://www.youtube.com/watch?v=vjxVko4Y56E

Les modèles

Exemple de modèle

nginx-vhost.conf.j2

```
# {{ ansible_managed }}

server
{
        listen 80 ;
        listen [::]:80 ;

        server_name {{ inventory_hostname }} ;

        root /srv/www/{{ inventory_hostname }} ;
        index index.xhtml ;

        access_log      /var/log/nginx/{{ inventory_hostname }}-access_log ;
        error_log       /var/log/nginx/{{ inventory_hostname }}-error_log ;
}
```

Les modèles

Exemple de livret

template1.yml

```
---
- name: Modèle 1
  hosts: test
  become: true
  tasks:
    - name: Configuration hôte virtuel
      ansible.builtin.template:
        src: nginx-vhost.conf.j2
        dest: /etc/nginx/conf.d/{{ inventory_hostname }}.conf
        owner: root
        group: root
        mode: '444'
```


Les modèles

Exemple de livret

template2.yml

```
---
- name: Modèle 2
  hosts: test
  become: true
  vars:
    ethers:
      - { fqdn: test1.example.com, ethernet: 11:00:aa:11:22:33 }
      - { fqdn: test2.example.com, ethernet: 9c:93:e4:44:55:66 }
      - { fqdn: test3.example.com, ethernet: e0:cb:1d:77:88:99 }
  tasks:
    - name: Configuration DHCP
      ansible.builtin.template:
        src: dhcpd.conf.j2
        dest: /srv/dhcp/dhcpd.conf
        owner: root
        group: root
        mode: '444'
```

Les modèles

Exemple de modèle et résultat

dhcpd.conf.j2

```
# {{ ansible_managed }}
{% for host in ethers %}

host {{ host.fqdn }}
{
        option host-name "{{ host.fqdn }}" ;
        fixed-address {{ host.fqdn }} ;
        hardware ethernet {{ host.ethernet }} ;
}
{% endfor %}
```

/srv/dhcp/dhcpd.conf

```
# Ansible managed

host test1.example.com
{
        option host-name "test1.example.com" ;
        fixed-address test1.example.com ;
        hardware ethernet 11:00:aa:11:22:33 ;
}

host test2.example.com
{
        option host-name "test2.example.com" ;
        fixed-address test2.example.com ;
        hardware ethernet 9c:93:e4:44:55:66 ;
}

host test3.example.com
{
        option host-name "test3.example.com" ;
        fixed-address test3.example.com ;
        hardware ethernet e0:cb:1d:77:88:99 ;
}
```


Sommaire

Les gestionnaires

Principe

- Les gestionnaires (*handlers*) permettent de déclencher certaines actions après la fin du traitement des tâches.
- Une tâche peut déclencher un ou plusieurs gestionnaires.
- Chaque gestionnaire est associé à une ou plusieurs tâches.
- Un gestionnaire n'est déclenché que si au moins l'une de ses tâches associées a effectué une action (c'est-à-dire s'il n'y a pas eu idempotence).
- Les gestionnaires sont exécutés dans l'ordre dans lequel ils sont définis dans la section `handlers`.
- Le même gestionnaire peut être associé à plusieurs tâches mais il ne sera exécuté qu'une seule fois.

```
tasks:
  - name: tâche 1
    ansible.builtin.module:
      [...]
    notify:
      - g2
  - name: tâche 2
    ansible.builtin.module:
      [...]
    notify:
      - g1
  - name: tâche 3
    ansible.builtin.module:
      [...]
    notify:
      - g2
handlers:
  - name: g1
    ansible.builtin.module:
      [...]
  - name: g2
    ansible.builtin.module:
      [...]
```

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

Les gestionnaires

Exemples

`handlers-listen.yml` (syntaxe moderne)

```
---
- name: Gestionnaire
  hosts: test
  become: true
  tasks:
    - name: Configuration syslog
      ansible.builtin.copy:
        src: openldap.conf
        dest: /etc/rsyslog.d/openldap.conf
        owner: root
        group: root
        mode: '444'
      notify:
        - restart rsyslog
  handlers:
    - name: Redémarrage de rsyslog
      ansible.builtin.service:
        name: rsyslog
        state: restarted
      listen: restart rsyslog
```

`handlers-name.yml` (syntaxe historique)

```
---
- name: Gestionnaire
  hosts: test
  become: true
  tasks:
    - name: Configuration syslog
      ansible.builtin.copy:
        src: openldap.conf
        dest: /etc/rsyslog.d/openldap.conf
        owner: root
        group: root
        mode: '444'
      notify:
        - restart rsyslog
  handlers:
    - name: restart rsyslog # noqa: name[casing]
      ansible.builtin.service:
        name: rsyslog
        state: restarted
```

https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_handlers.html#naming-handlers

Sommaire

Principe

- Les livrets peuvent vite atteindre une taille importante et comporter entre eux des parties redondantes. Aussi est-il possible d'organiser la CMDB sous forme de *rôles*.
- L'objectif des rôles est d'éliminer les redondances dans la CMDB en la rendant modulaire, de faciliter la réutilisation du code et de le rendre plus générique.
- Un rôle est simplement le résultat de la décomposition des différentes parties d'un livret mettant en œuvre une fonction précise en organisant ces parties dans un ensemble de répertoires et de fichiers.

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

`https://www.youtube.com/watch?v=kjQWzRX9tB0`

Structure

```
roles/
└── <nom du rôle>/
    ├── defaults/
    │   └── main.yml
    ├── files/
    ├── handlers/
    │   └── main.yml
    ├── meta/
    │   └── main.yml
    ├── tasks/
    │   └── main.yml
    ├── templates/
    └── vars/
        └── main.yml
```

- Le nom d'un rôle (et donc le répertoire correspondant) ne peut contenir que des caractères alphanumériques bas de casse et des tirets bas et doit commencer par une lettre.
- Les répertoires `defaults`, `handlers`, `meta`, `tasks` et `vars` peuvent contenir un fichier `main.yml`, qui sera automatiquement pris en compte.
- Les fichiers utilisés par le module `ansible.builtin.copy` sont recherchés dans le répertoire `files`.
- Les fichiers utilisés par le module `ansible.builtin.template` sont recherchés dans le répertoire `templates`.

Utilisation

- Lorqu'on utilise un ou plusieurs rôles, la commande `ansible-playbook` est exécutée avec en argument un livret plutôt simple faisant la liaison entre l'inventaire et le ou les rôles à appliquer aux machines.
- Ce livret, dont le nom est indifférent, ne fait pas partie du rôle et doit donc être placé à l'extérieur du répertoire `roles`.

livret-roles.yml

```
---
- name: Rôles
  hosts: test
  become: true
  roles:
    - nginx
    - postgresql
```

Exemple

roles/nginx/tasks/main.yml (1/3)

```
---

- name: Installation de nginx
  ansible.builtin.package:
    name: nginx
    state: present
  notify:
    - nginx_enable_start
```


Exemple

roles/nginx/tasks/main.yml (2/3)

```
- name: Création de la clé privée et du certificat TLS
  ansible.builtin.command: openssl req -newkey rsa:2048
                           -nodes -x509 -days 365
                           -subj /CN={{ inventory_hostname }}
                           -keyout {{ nginx_key }}
                           -out {{ nginx_crt }}
  args:
    creates: "{{ nginx_crt }}"
```

Exemple

roles/nginx/tasks/main.yml (3/3)

```
- name: Droits d'accès sur la clé privée et le certificat TLS
  ansible.builtin.file: path={{ item.path }} mode={{ item.mode }}
  loop:
    - { path: "{{ nginx_crt }}", mode: '444' }
    - { path: "{{ nginx_key }}", mode: '400' }

- name: Hôte virtuel TLS
  ansible.builtin.template:
    src: nginx-vhost-tls.conf.j2
    dest: /etc/nginx/conf.d/{{ inventory_hostname }}-tls.conf
    owner: root
    group: root
    mode: '444'
```


Exemple

roles/nginx/vars/main.yml

```
---

nginx_crt: /etc/pki/tls/certs/{{ inventory_hostname }}-crt.pem
nginx_key: /etc/pki/tls/private/{{ inventory_hostname }}-key.pem
```

roles/nginx/handlers/main.yml

```
---

- name: nginx_enable_start # noqa: name[casing]
  ansible.builtin.service:
    name: nginx
    enabled: true
    state: started
```

Utiliser d'autres fichiers

- Les rôles peuvent faire appel à d'autres fichiers que `main.yml`, en les référençant explicitement depuis le fichier `tasks/main.yml` :

`roles/apache/tasks/main.yml`

```
---

- name: Inclusion des variables
  ansible.builtin.include_vars: "{{ ansible_os_family }}.yml"

- name: Import des tâches d'installation
  ansible.builtin.import_tasks: installation.yml
```

https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_reuse.html
https://docs.ansible.com/ansible/latest/modules/include_vars_module.html
https://docs.ansible.com/ansible/latest/modules/import_tasks_module.html

Utiliser d'autres fichiers

`roles/apache/vars/Debian.yml`

```
---

apache_paquet: apache2
```

`roles/apache/vars/RedHat.yml`

```
---

apache_paquet: httpd
```

`roles/apache/tasks/installation.yml`

```
---

- name: Installation d'Apache
  ansible.builtin.package:
    name: "{{ apache_paquet }}"
    state: present
```

Sommaire

Principe

- Une *collection* permet de regrouper des fichiers (livrets, rôles, etc.) pour Ansible.

```
<espace de nommage>/
└── <nom de la collection>/
    ├── docs/
    ├── galaxy.yml
    ├── plugins/
    ├── README.md
    ├── roles/
    │   ├── role1/
    │   ├── role2/
    │   └── .../
    ├── playbooks/
    └── tests/
```


https://docs.ansible.com/ansible/latest/dev_guide/developing_collections.html
https://docs.ansible.com/ansible/latest/collections_guide/

Sommaire

Principe

- Galaxy est un site Web permettant le téléchargement et le télédépôt de rôles et de collections réalisés par la communauté.

`https://galaxy.ansible.com/`
`https://docs.ansible.com/ansible/latest/galaxy/user_guide.html`

La commande ansible-galaxy

Principe

- La commande ansible-galaxy permet la gestion (recherche, téléchargement, télédépôt, etc.) des rôles et des collections depuis Galaxy.
- Elle s'utilise suivie d'un type, d'une action et, au besoin, d'options :

```
$ ansible-galaxy [type] <action> [options]
```

- Le type peut être :

  `collection` pour gérer les collections

  `role` pour gérer les rôles

  En l'absence de type, `role` est utilisé implicitement.

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

La commande ansible-galaxy

Gestion des rôles

`init` crée le squelette d'un nouveau rôle dont le nom est en argument :

```
$ ansible-galaxy role init nom_role
```

`search` effectue une recherche parmi les rôles disponibles :

```
$ ansible-galaxy role search nginx
```

`info` affiche les informations du rôle en argument :

```
$ ansible-galaxy role info bennojoy.nginx
```

La commande ansible-galaxy

Gestion des rôles

`install` télécharge et installe les rôles en arguments :

```
$ ansible-galaxy role install bennojoy.nginx
```

Les rôles sont installés dans le premier répertoire accessible en écriture dans ceux spécifiés par le paramètre `roles_path`. Il est possible d'indiquer explicitement le répertoire d'installation au moyen de l'option `-p` :

```
$ ansible-galaxy role install -p [...] bennojoy.nginx
```


La commande ansible-galaxy

Gestion des rôles

`list` affiche la liste des rôles installés :

```
$ ansible-galaxy role list
```

L'option `-p` permet d'indiquer le répertoire contenant les rôles.

`remove` supprime les rôles en arguments :

```
$ ansible-galaxy role remove bennojoy.nginx
```

L'option `-p` permet d'indiquer le répertoire contenant les rôles.

La commande ansible-galaxy

Gestion des collections

`init` crée le squelette d'une nouvelle collection dont le nom qualifié est en argument :

```
$ ansible-galaxy collection init espace_de_nommage.nom_collection
```

`install` télécharge et installe les collections en arguments :

```
$ ansible-galaxy collection install icinga.icinga
```

Les collections sont installées dans le premier répertoire accessible en écriture dans ceux spécifiés par le paramètre `collections_paths`. Il est possible d'indiquer explicitement le répertoire d'installation au moyen de l'option `-p` :

```
$ ansible-galaxy collection install -p [...] icinga.icinga
```


Sommaire

Sommaire

Les étiquettes

Principe

- Les étiquettes (*tags*) sont des chaînes de caractères arbitraires associées à des structures d'Ansible — principalement des tâches ou des rôles — et permettant leur exécution sélective.
- Lors d'une exécution sélective au moyen d'étiquettes, les gestionnaires associés aux tâches exécutées sont déclenchés.

`https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_tags.html`
`https://www.youtube.com/watch?v=mPi6SwC4SJ8`

Les étiquettes

Exemples

tags.yml (1/3)

```
---
- name: Étiquettes
  hosts: test
  become: true
  tasks:
    - name: Install. nginx
      ansible.builtin.package:
        name: nginx
        state: present
      tags:
        - installation
```

tags.yml (2/3)

```
    - name: Config. nginx
      ansible.builtin.copy:
        src: nginx.conf
        dest: /etc/nginx/nginx.conf
        owner: root
        group: root
        mode: '444'
      tags:
        - configuration
```


Les étiquettes

Exemples

tags.yml (3/3)

```
    - name: Restart nginx
      ansible.builtin.service:
        name: nginx
        state: restarted
      tags:
        - service
```

tags-role.yml

```
---
- name: Étiquettes avec rôle
  hosts: test
  become: true
  roles:
    - role: nginx
      tags:
        - nginx_configuration
```

Les étiquettes

Utilisation

- La commande `ansible-playbook` dispose d' options permettant de sélectionner les tâches à exécuter — ou à ne pas exécuter — en fonction des étiquettes indiquées :
  - L'option `-t` (ou `--tags`) permet d'exécuter les tâches correspondant aux étiquettes indiquées (les autres ne le sont pas) :

```
$ ansible-playbook -v -t installation tags.yml
```

```
$ ansible-playbook -v -t configuration,service tags.yml
```

  - L'option `--skip-tags` permet de ne pas exécuter les tâches correspondant aux étiquettes indiquées (les autres le sont) :

```
$ ansible-playbook -v --skip-tags installation tags.yml
```


Les étiquettes

Étiquettes spéciales

- Certaines étiquettes ont une signification spéciale :

`always` fait en sorte que les tâches correspondantes soient toujours exécutées, sauf si l'étiquette est explicitement ignorée :

```
$ ansible-playbook -v --skip-tags always tags.yml
```

`never` fait en sorte que les tâches correspondantes ne soient jamais exécutées, sauf si l'étiquette est explicitement sélectionnée :

```
$ ansible-playbook -v -t never tags.yml
```

Sommaire

Enregistrer le résultat d'une tâche dans une variable

- L'instruction `register` permet d'enregistrer le résultat d'une tâche dans une variable afin de le réutiliser dans une autre tâche :

register.yml

```
---
- name: Enregistrement du résultat
  hosts: test
  tasks:
    - name: Fichier temporaire
      ansible.builtin.tempfile:
      register: temp
    - name: Droits d'accès
      ansible.builtin.file:
        path: "{{ temp.path }}"
        mode: '644'
```

https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_variables.html#registering-variables

Enregistrer le résultat d'une tâche dans une variable

- Le contenu exact de la variable créée par l'instruction `register` varie selon le module auquel elle s'applique.
- Le module `debug` permet d'en afficher le contenu.

register-debug.yml

```
---
- name: Enregistrement puis affichage
  hosts: test
  tasks:
    - name: Fichier temporaire
      ansible.builtin.tempfile:
      register: temp
    - name: Variable temp
      ansible.builtin.debug:
        var: temp
```

```
$ ansible-playbook -v register-debug.yml
[...]
TASK [Variable temp] ************************
ok: [test1.example.com] => {
    "temp": {
        "changed": true,
        "failed": false,
        "gid": 3351,
        "group": "beatles",
        "mode": "0600",
        "owner": "lennon",
        "path": "/tmp/ansible.zq8ba2xm",
        "size": 0,
        "state": "file",
        "uid": 1664
    }
}
[...]
```


Enregistrer le résultat d'une tâche dans une variable

- Utilisée avec une boucle, l'instruction `register` enregistre le résultat de toutes les tâches de la boucle dans la variable indiquée :

register-loop.yml

```
---
- name: Enregistrement et boucle
  hosts: test
  tasks:
    - name: Fichier temporaire
      ansible.builtin.tempfile:
      loop: [ 1, 2, 3 ]
      register: temp
    - name: Droits d'accès
      ansible.builtin.file:
        path: "{{ item.path }}"
        mode: '644'
      loop: "{{ temp.results }}"
```

https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_loops.html#registering-variables-with-a-loop

Enregistrer le résultat d'une tâche dans une variable

- Certains modules génèrent directement un ensemble de données sans avoir besoin d'une boucle mais une boucle est nécessaire afin de pouvoir traiter ces données.

register-menage.yml

```
---
- name: Ménage de la salle de cours
  hosts: test
  become: true
  tasks:
    - name: Détection des fichiers LDIF
      ansible.builtin.find:
        paths: [ /home/user, /root, /tmp ]
        patterns: '*.ldif'
        recurse: true
      register: ldif
    - name: Suppression des fichiers LDIF
      ansible.builtin.file:
        path: "{{ item.path }}"
        state: absent
      loop: "{{ ldif.files }}"
```


Sommaire

Gestion des erreurs

- En cas d'erreur lors de l'application d'une tâche, le traitement s'arrête sur la machine correspondante (mais il continue sur les autres) en application du principe de précaution.
- Plusieurs approches sont possible pour éviter cela.

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

ignore_errors

- Il est possible d'ignorer sciemment les erreurs lorsqu'on sait qu'une erreur dans une tâche ne compromet pas la suite de l'exécution.

ignore_errors.yml

```
---
- name: Ignorer les erreurs
  hosts: test
  become: true
  tasks:
    - name: Installation d'un paquet inexistant
      ansible.builtin.package:
        name: glub
        state: present
      ignore_errors: true
    - name: Mais on continue quand même
      ansible.builtin.debug:
        msg: nananère
```


https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_error_handling.html#ignoring-failed-commands

Les blocs

- Les blocs permettent de grouper des tâches et de gérer les erreurs :
  - `block` tâches principales
  - `rescue` tâches à exécuter en cas d'erreur
  - `always` tâches à exécuter dans tous les cas

block.yml

```
---
- name: Blocs
  hosts: test
  become: true
  tasks:
    - name: Test de bloc
      block:
        - name: Installation d'un paquet inexistant
          ansible.builtin.package:
            name: glub
            state: present
      rescue:
        - name: Rescue
          ansible.builtin.debug:
            msg: 'cette partie est exécutée en cas d''erreur'
      always:
        - name: Always
          ansible.builtin.debug:
            msg: 'cette partie est toujours exécutée'
```

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

Sommaire

Ansible vault

Principe

- Ansible vault est une fonctionnalité d'Ansible permettant de chiffrer les fichiers dont le contenu doit rester confidentiel.
- Ces fichiers doivent être gérés au moyen de la commande `ansible-vault`.
- Pour utiliser ensuite des fichiers chiffrés, la commande `ansible-playbook` doit être appelée avec l'une des options `--ask-vault-password` ou `--ask-vault-pass` (qu'on peut — enfin — abréger en `-J` à partir de la version 2.16.0 d'`ansible-core`) :

```
$ ansible-playbook -vJ vault.yml
Vault password:
[...]
```

https://docs.ansible.com/ansible/latest/vault_guide/

Ansible vault

La commande `ansible-vault`

- La commande `ansible-vault` permet de gérer des fichiers chiffrés. Elle s'utilise selon la syntaxe suivante :

```
$ ansible-vault <action> [options] fichier.yml
```

- Certaines des actions de la commande `ansible-vault` exécutent un éditeur de texte. Celui-ci peut être personnalisé au moyen de la variable d'environnement `EDITOR`.

https://docs.ansible.com/ansible/latest/cli/ansible-vault.html

Ansible vault

La commande ansible-vault

`create` création d'un nouveau fichier chiffré :

```
$ ansible-vault create vault.yml
New Vault password:
Confirm New Vault password:
```

`encrypt` chiffrement d'un fichier existant :

```
$ ansible-vault encrypt vault.yml
New Vault password:
Confirm New Vault password:
Encryption successful
```


Ansible vault

La commande ansible-vault

`edit` édition d'un fichier chiffré :

```
$ ansible-vault edit vault.yml
Vault password:
```

`view` affichage d'un fichier chiffré :

```
$ ansible-vault view vault.yml
Vault password:
```

Sommaire

La commande ansible-lint

- La commande ansible-lint permet de vérifier le respect d'un certain nombre de bonnes pratiques dans des fichiers YAML pour Ansible.
- Elle s'utilise avec un ou plusieurs arguments, dont chacun peut être :
  - un livret, auquel cas les rôles utilisés par ce livret sont également vérifiés
  - un nom de rôle, auquel cas les tâches et les gestionnaires sont vérifiés
- Installation :
  - paquet ansible-lint sur toutes les distributions Linux
- Exemple :

```
$ ansible-lint livret.yml
[...]
name[casing]: All names should start with an uppercase letter. (warning)
livret.yml:2
[...]
```

https://ansible.readthedocs.io/projects/lint/
https://www.redhat.com/sysadmin/ansible-lint-YAML
https://www.youtube.com/watch?v=8-M66pCzVTQ

Sommaire

Les modules

- Les *modules* sont les composants d'Ansible qui effectuent les actions sur les machines distantes.
- Ansible propose de très nombreux modules.
- Depuis la version 2.9 d'Ansible, les modules ont été réorganisés sous forme de *collections*. La collection `ansible.builtin` regroupe les modules les plus utilisés. Il est désormais recommandé d'écrire les noms de modules dans la CMDB au moyen de leur FQCN (*fully qualified collection name*).
- Il n'est pas utile détailler tous les modules ici — la documentation d'Ansible est très claire et il est préférable de toujours s'y reporter pour avoir une description à jour des modules — mais nous allons en survoler quelques uns.

---

https://docs.ansible.com/ansible/latest/module_plugin_guide/index.html
https://docs.ansible.com/ansible/latest/collections/
https://docs.ansible.com/ansible/latest/collections/index_module.html
https://www.ansible.com/blog/migrating-to-ansible-collections-webinar-qa

Le module ansible.builtin.assert

module-ansible.builtin.assert.yml

```
---
- name: Module ansible.builtin.assert
  hosts: test
  become: true
  tasks:
    - name: Vérification du système hôte
      ansible.builtin.assert:
        that:
          - ansible_os_family == 'RedHat'
          - ansible_distribution_major_version == '7'
        fail_msg: >-
          Il n'est possible d'effectuer ceci que sur
          une distribution Linux de la famille Red Hat
          et de version 7. Or la distribution est :
          {{ ansible_os_family }} version
          {{ ansible_distribution_major_version }}.
```

- Le module ansible.builtin.assert s'assure qu'une ou plusieurs expressions (avec la même syntaxe que l'instruction when) sont vérifiées et échoue dans le cas contraire.
- Les conditions de la séquence suivant le paramètre that doivent toutes être vérifiées pour que le module ansible.builtin.assert réussisse.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/assert_module.html

Le module ansible.builtin.command

module-ansible.builtin.command.yml

```
---
- name: Module ansible.builtin.command
  hosts: test
  become: true
  tasks:
    - name: Création clé rndc
      ansible.builtin.command:
        cmd: rndc-confgen -a
        creates: /etc/rndc.key
```

- Le module ansible.builtin.command permet d'exécuter une commande en spécifiant ses conditions d'exécution (répertoire courant, exécution ou pas en fonction de la présence ou de l'absence d'un fichier).

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/command_module.html

Le module ansible.builtin.copy

module-ansible.builtin.copy.yml

```
---
- name: Module ansible.builtin.copy
  hosts: test
  become: true
  tasks:
    - name: Config. syslog
      ansible.builtin.copy:
        src: openldap.conf
        dest: /etc/rsyslog.d/openldap.conf
        owner: root
        group: root
        mode: '444'
      notify:
        - restart rsyslog
  handlers:
    - name: restart rsyslog # noqa: name[casing]
      ansible.builtin.service:
        name: rsyslog
        state: restarted
```

- Le module ansible.builtin.copy recopie à l'identique un fichier depuis la machine de contrôle vers les machines à gérer.
- La copie n'est effectuée que si l'état du fichier (contenu, caractéristiques) est différent de celui spécifié.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/copy_module.html

Le module ansible.builtin.cron

module-ansible.builtin.cron.yml

```
---
- name: Module ansible.builtin.cron
  hosts: test
  become: true
  tasks:
    - name: Sauvegarde
      ansible.builtin.cron:
        name: sauvegarde
        cron_file: svg
        minute: 0
        hour: 1
        weekday: 7
        user: root
        job: /usr/local/bin/svg
```

- Le module ansible.builtin.cron permet de manipuler des tâches à faire exécuter par cron.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/cron_module.html

Le module ansible.builtin.debug

module-ansible.builtin.debug.yml

```
---
- name: Module ansible.builtin.debug
  hosts: test
  tasks:
    - name: Affichage message
      ansible.builtin.debug:
        msg: 'ceci est un test'
    - name: Affichage variable
      ansible.builtin.debug:
        var: ansible_date_time
```

- Le module ansible.builtin.debug permet d'afficher un message (paramètre msg) ou le contenu d'une variable (paramètre var).
- Les paramètres msg et var sont mutuellement exclusifs.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/debug_module.html

Le module ansible.builtin.file

module-ansible.builtin.file.yml

```
---
- name: Module ansible.builtin.file
  hosts: test
  become: true
  tasks:
    - name: Vérif. /srv/www
      ansible.builtin.file:
        path: /srv/www
        state: directory
        owner: root
        group: root
        mode: '755'
```

- Le module ansible.builtin.file permet de positionner divers attributs sur des fichiers.
- Le module ansible.builtin.file partage de nombreuses options avec les modules ansible.builtin.copy et ansible.builtin.template.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/file_module.html

Le module ansible.builtin.get_url

module-ansible.builtin.get_url.yml

```
---
- name: Module ansible.builtin.get_url
  hosts: test
  become: true
  tasks:
    - name: Téléchargement
      ansible.builtin.get_url:
        url: http://www.example.com/test.tar.gz
        dest: /tmp/test.tar.gz
        owner: root
        group: root
        mode: '644'
```

- Le module ansible.builtin.get_url télécharge un fichier depuis les machines à gérer au moyen des protocoles HTTP, HTTPS ou FTP.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/get_url_module.html

Le module ansible.builtin.lineinfile

module-ansible.builtin.lineinfile.yml

```
---
- name: Module ansible.builtin.lineinfile
  hosts: test
  become: true
  tasks:
    - name: Modif. /etc/hosts
      ansible.builtin.lineinfile:
        path: /etc/hosts
        line: '198.51.100.33    test.example.com'
        regexp: '^198\.51\.100\.33'
```

- Le module ansible.builtin.lineinfile ajoute ou remplace une ligne dans un fichier.
- L'expression rationnelle spécifiée par le paramètre regexp permet d'identifier une ligne similaire afin de la remplacer.
- Il existe aussi un module ansible.builtin.blockinfile, qui permet de manipuler un bloc (plusieurs lignes) de texte dans un fichier.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/lineinfile_module.html

Le module ansible.builtin.package

module-ansible.builtin.package.yml

```
---
- name: Module ansible.builtin.package
  hosts: test
  become: true
  tasks:
    - name: Install. nginx
      ansible.builtin.package:
        name: nginx
        state: present
```

- Le module ansible.builtin.package est un module générique permettant d'installer, de mettre à jour ou de supprimer des paquets logiciels.
- Il existe également des modules ne fonctionnant que sur certaines distributions Linux (ansible.builtin.apt, ansible.builtin.dnf, ansible.builtin.yum, etc.) mais disposant de plus d'options.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/package_module.html

Le module ansible.builtin.replace

module-ansible.builtin.replace.yml

```
---
- name: Module ansible.builtin.replace
  hosts: test
  become: true
  tasks:
    - name: Activation de postscreen
      ansible.builtin.replace:
        path: /etc/postfix/master.cf
        regexp: '^#(smtp.*postscreen)$'
        replace: '\1'
```

- Le module ansible.builtin.replace effectue des remplacements dans un fichier au moyen d'une expression rationnelle avec laquelle on peut mémoriser des chaînes de caractères — entourées par des parenthèses — dans la ligne d'origine puis les réutiliser dans la nouvelle ligne : \1 pour le contenu du premier couple de parenthèses, \2 pour celui du deuxième, etc.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/replace_module.html

Le module ansible.builtin.service

module-ansible.builtin.service.yml

```
---
- name: Module ansible.builtin.service
  hosts: test
  become: true
  tasks:
    - name: Installation de nginx
      ansible.builtin.package:
        name: nginx
        state: present
      notify:
        - enable_start_nginx
  handlers:
    - name: enable_start_nginx # noqa: name[casing]
      ansible.builtin.service:
        name: nginx
        enabled: true
        state: started
```

- Le module ansible.builtin.service est un module générique permettant la gestion des daemons (activation, démarrage, redémarrage, etc.).
- Le module ansible.builtin.service est souvent utilisé dans des gestionnaires.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/service_module.html

Le module ansible.builtin.template

module-ansible.builtin.template.yml

```
---
- name: Module ansible.builtin.template
  hosts: test
  become: true
  tasks:
    - name: Configuration hôte virtuel
      ansible.builtin.template:
        src: nginx-vhost.conf.j2
        dest: /etc/nginx/conf.d/{{ inventory_hostname }}.conf
        owner: root
        group: root
        mode: '444'
```

- Le module ansible.builtin.template fonctionne sur le même principe que le module ansible.builtin.copy mais il effectue des traitements dans le fichier en utilisant le système Jinja2.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/template_module.html

Le module ansible.builtin.user

module-ansible.builtin.user.yml

```
---
- name: Module ansible.builtin.user
  hosts: test
  become: true
  tasks:
    - name: Création utilisateur
      ansible.builtin.user:
        name: jlapin
        #uid: 1664
        group: users
        comment: 'Jojo Lapin'
```

- Le module ansible.builtin.user permet la gestion des comptes utilisateurs.

https://docs.ansible.com/ansible/latest/collections/ansible/builtin/user_module.html
https://www.theurbanpenguin.com/managing-users-in-ansible/
https://www.youtube.com/watch?v=UEfYIYVe9yw

La commande ansible-doc

- La commande ansible-doc permet d'afficher la documentation du ou des modules en arguments :

```
$ ansible-doc ansible.builtin.lineinfile
```

ou avec l'ancien nom du module :

```
$ ansible-doc lineinfile
```

- L'option -l (ou --list) affiche la liste des modules disponibles :

```
$ ansible-doc -l
```

https://docs.ansible.com/ansible/latest/cli/ansible-doc.html

Sommaire

Bibliographie

[1] James Freeman, Fabio Alessandro Locati et Daniel Oh
Practical Ansible
Anglais
2e édition
Packt Publishing, septembre 2023
url : https://www.packtpub.com/product/practical-ansible-second-edition/9781805129974

[2] Yannig Perré
Ansible — Gérez la configuration de vos serveurs et le déploiement de vos applications
3e édition
Éditions ENI, mai 2023
url : https://www.editions-eni.fr/livre/ansible-gerez-la-configuration-de-vos-serveurs-et-le-deploiement-de-vos-applications-3e-edition-9782409039720

Bibliographie

[3] Gineesh Madapparambath
Ansible for Real-Life Automation
Anglais
Packt Publishing, septembre 2022
url : https://www.packtpub.com/product/ansible-for-real-life-automation/9781803235417

[4] Bas Meijer, Lorin Hochstein et René Moser
Ansible Up & Running — Automating Configuration Management and Deployment the Easy Way
Anglais
3e édition
O'Reilly Media, juillet 2022
url : http://www.ansiblebook.com/

Bibliographie

[5] James Freeman et Jesse Keating
Mastering Ansible
Anglais
4e édition
Packt Publishing, décembre 2021
url : https://www.packtpub.com/product/mastering-ansible-fourth-edition/9781801818780

[6] Philippe Pinchon
Red Hat Ansible Engine — Gérez l'automatisation de vos configurations Linux
Éditions ENI, octobre 2020
url : https://www.editions-eni.fr/livre/red-hat-ansible-engine-gerez-l-automatisation-de-vos-configurations-linux-9782409027291

Bibliographie

[7] Josh Duffney
become Ansible — Zero to Production-Ready
Anglais
1er septembre 2020
url : https://becomeansible.com/

[8] Jeff Geerling
Ansible for DevOps — Server and configuration management for humans
Anglais
2e édition
5 août 2020
url : https://www.ansiblefordevops.com/

Bibliographie

[9] Fabio Alessandro Locati
Learning Ansible 2.7
Anglais
3e édition
Packt Publishing, avril 2019
url : https://www.packtpub.com/networking-and-servers/learning-ansible-27-third-edition

[10] Mohamed Alibi
Ansible Quick Start Guide
Anglais
Packt Publishing, septembre 2018
url : https://www.packtpub.com/virtualization-and-cloud/ansible-quick-start-guide

Bibliographie

[11] Russ McKendrick
Learn Ansible
Anglais
Packt Publishing, juin 2018
url :
https://www.packtpub.com/virtualization-and-cloud/learn-ansible

[12] Aditya Patawari et Vikas Aggarwal
Ansible 2 Cloud Automation Cookbook
Anglais
Packt Publishing, février 2018
url : https://www.packtpub.com/virtualization-and-cloud/ansible-2-cloud-automation-cookbook

Bibliographie

[13] Akash Mahajan et Madhu Akula
Security Automation with Ansible 2
Anglais
Packt Publishing, décembre 2017
url : https://www.packtpub.com/virtualization-and-cloud/security-automation-ansible-2

[14] Jonathan McAllister
Implementing DevOps with Ansible 2
Anglais
Packt Publishing, juillet 2017
url : https://www.packtpub.com/networking-and-servers/implementing-devops-ansible-2

Bibliographie

[15] Rishabh Das
Extending Ansible
Anglais
Packt Publishing, mars 2016
url : https://www.packtpub.com/networking-and-servers/extending-ansible

[16] Gourav Shah
Ansible Playbook Essentials
Anglais
Packt Publishing, août 2015
url : https://www.packtpub.com/networking-and-servers/ansible-playbook-essentials

Bibliographie

[17] Daniel Hall
Ansible Configuration Management
Anglais
2e édition
Packt Publishing, avril 2015
url : https://www.packtpub.com/networking-and-servers/ansible-configuration-management-second-edition