



Ansible pour professionnels

Linux / Unix



Le support du cours «Ansible pour professionnels Linux/Unix » est non contractuel ; il ne doit pas être redistribué et/ou reproduit en partie ou en totalité sans permission explicite et écrite de la société Adlere.

Red Hat, le logo Red Hat, OpenShift et Ansible sont des marques déposées ou commerciales de Red Hat, Inc ou ses filiales aux États-Unis et dans d'autre pays. Linux® est une marque déposée de Linus Torvalds aux États-Unis et dans d'autre pays.

UNIX ® est une marque déposée par « The Open Group » aux Etats-Unis et dans d'autres pays.
Wiindows® est une marque déposée de Microsoft Corporation aux États-Unis et dans d'autre pays.

Les autres marques citées sont déposées par leurs propriétaires respectifs.



+adlere
DIGITAL EXPERTISE

modules usuels

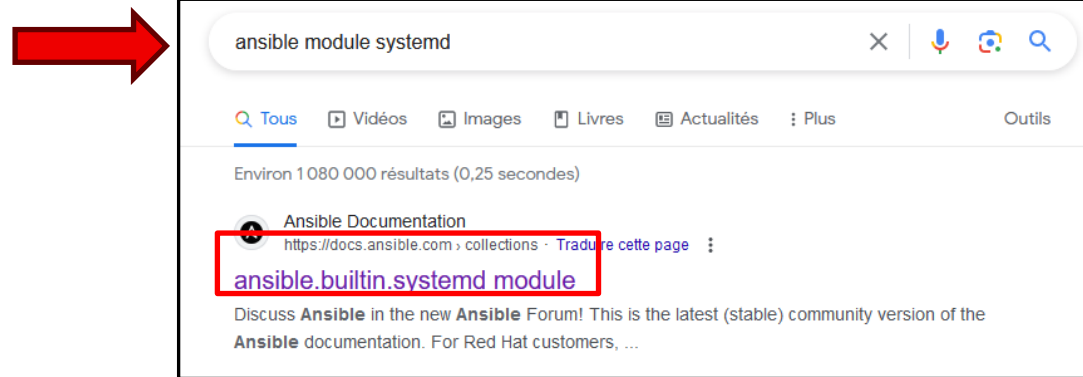


Playbook :

- des directives de fonctionnement (**hosts:**, **become:**, ...)
- succession d'appels à différents modules
 - avec une logique et une gestion des variables plus ou moins sophistiquée
- Un module est un programme (module) Python, écrit selon des normes précises
- invoqué avec des paramètres propres à chaque module, même s'il existe des conventions
 - state, path, src, dest, ...
- quand un playbook est exécuté, chaque tâche est transformée en programme Python qui est recopié sur la cible
 - il est important de connaître et pratiquer les modules Ansible
 - il en existe énormément, souvent insoupçonnés
 - il est important de savoir les rechercher et les utiliser
- Les modules listés plus loin ne sont qu'un petit échantillon de ce qui existe réellement
- Seules quelques options sont présentées, se référer à la **documentation** pour une liste exhaustive



- Accès facile à la documentation par moteur de recherche + mots-clefs "**ansible module**"



- Toujours vérifier que l'on est bien sur la dernière version de la documentation



- Accès à la documentation en ligne de commande

```
ansible-doc -l [-t type]
```

```
ansible-doc <MODULE>
```

```
ansible-doc -s <MODULE>
```



| Commande | Fonction |
|--|---|
| <code>ansible-doc -l</code> | Liste les documentations disponibles. Pour les composants qui n'apparaissent pas dans la sortie, regarder dans leur répertoire l'existence d'un README.md par exemple. |
| <code>ansible-doc -l -t XXXX</code> | Affiche les documentations disponibles dans une catégorie donnée (par défaut, "modules") ex : <code>ansible-doc -l -t inventory</code> |
| <code>ansible-doc -t XXXX -F</code> | Affiche le chemin d'accès au fichier python des composants listés |
| <code>ansible-doc ansible.builtin.lineinfile</code> <code>ansible-doc lineinfile</code> | Affiche la documentation du composant demandé Astuce: rechercher "EXA" (pour EXAMPLE, taper "/EXA") dans la sortie → l'affichage se positionne sur les exemples |
| <code>ansible-doc -s lineinfile</code> | Affiche la version courte de la documentation du module indiqué |



- La plupart des modules sont fournis en standard avec Ansible (collection ansible.builtin)
 - ansible.builtin : <https://docs.ansible.com/ansible/latest/collections/ansible/builtin/index.html>

- D'autres nécessitent d'installer la collection qui les apporte

community.general : <https://docs.ansible.com/ansible/latest/collections/community/general/index.html>

ansible.posix : <https://docs.ansible.com/ansible/latest/collections/ansible/posix/index.html>

[...]



ansible.builtin

ansible.posix

ansible.utils

ansible.windows

community.general

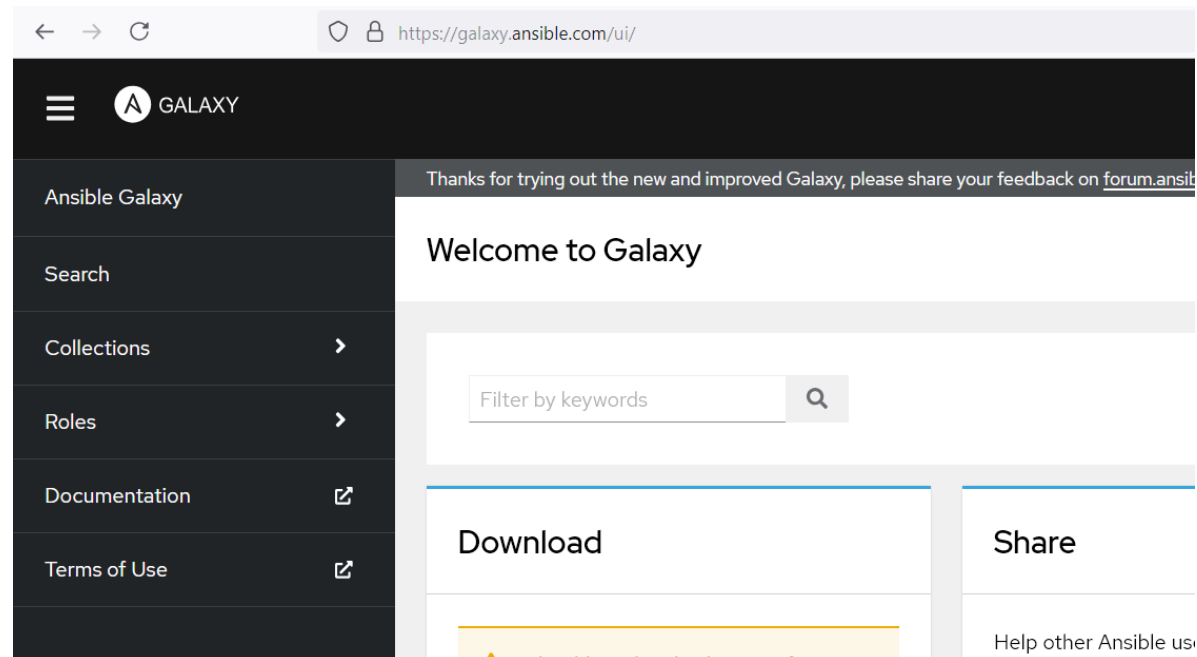
community.windows

community.docker

community.mysql

community.crypto

community.postgresql



- Si connexion internet : `ansible-galaxy collection install NAMESPACE.COLLECTION` (eg: `ansible.utils`)
 - Télécharge automatiquement depuis `galaxy.ansible.com`
 - version spécifique: `ansible-galaxy collection install community.general:=8.5.0`
- Sans connexion : on télécharge depuis <https://galaxy.ansible.com>, on dépose sur le système cible, puis :
 - `ansible-galaxy collection install archive.tar.gz`



Appel à un module - style d'écriture

Généralités

Admin Sys

Fichiers

Rôles RHEL

Jinja2

Nom de la tâche

```
- name: 'Creation d'instances EC2'
amazon.aws.ec2:
  assign_public_ip: true
  image: 'ami-c7d092f7'
  instance_tags:
    name: '{{ item }}'
    key_name: 'my_key'
  loop: '{{ instance_names }}'
  ignore_errors: true
  register: ec2_output
  when: ansible_os_family == 'Linux'
  tags:
    - tag1
    - tag2
```

declaration du module (FQCN)

paramètres de la tâche en ordre
alphabétique dans un groupement
logique, syntaxe multilignes,(d'autre source
préconisent ordre
alphabétique tout court)

opérateurs de boucle (loop, with_*)

options de la tâche (par ordre alphabétique)(e.g.
become, ignore_errors, register)

tags



De plus bas au plus haut niveau :

- **parted** pour la configuration des périphériques blocs
- **lvg** et **lvol** pour les groupes de volumes et volumes logiques
- **filesystem** pour créer / redimensionner les systèmes de fichiers
- **mount** pour configurer /etc/fstab (nfs compris)
- espaces de pagination pas (encore) supporté
- collection **community.general**
mais 'mount' dans **ansible.posix.mount**



- **name:** Creation d'un VG de swap
community.general.lvg:
 vg: vgswap
 pvs: /dev/vda1
 state: present
- **name:** Creation d'un LV de swap
community.general.lvol:
 vg: vgswap
 lv: lvswap
 size: 10g
- **name:** Formattage du LV de swap
ansible.builtin.command: mkswap /dev/vgswap/lvswap
when: ansible_swaptotal_mb < 128
- **name:** Activation du swap
ansible.builtin.command: swapon /dev/vgswap/lvswap
when: ansible_swaptotal_mb < 128



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

```
- name: Positionne un nom d'hôte
  ansible.builtin.hostname:
    name: web01
```

https://docs.ansible.com/ansible/latest/collections/ansible/posix/firewalld_module.html

```
- name: eth0 en zone externe
  ansible.posix.firewalld:
    zone: external
    interface: eth0
    permanent: yes
    state: enabled
```

```
- name: Activation d'une règle http
  ansible.posix.firewalld:
    service: http
    permanent: yes
    immediate: yes
    state: enabled
```



Avec `community.general.nmcli`:

```
- name: NIC configuration
  community.general.nmcli:
    conn_name: ens4-conn
    ifname: ens4
    type: ethernet
    ip4: 172.25.250.30/24
    gw4: 172.25.250.1
    state: present
```

https://docs.ansible.com/ansible/latest/collections/community/general/nmcli_module.html




Avec les rôles RHEL :

```
- name: NIC Configuration
  hosts: webservers
  vars:
    network_provider: nm
    network_connections:
      - name: ens4
        type: ethernet
        ip:
          address:
            - 172.25.250.30/24
  roles:
    - rhel-system-roles.network
```

- paquetage des rôles systèmes RHEL doit être installé
- `network_provider` peut être soit `nm` (NetworkManager) ou `initscripts` (rhel6)



```
- name: Installation conditionnelle de packages
  ansible.builtin.dnf:
    name:
      - make
      - git
      - curl
      - net-tools
      - tmux
      - tree
      - tar
    state: present
  when: "ansible_facts['distribution'] == 'RedHat'"
```



- name = paquetage à installer (liste acceptée)
- state : present, absent, latest
- autres modules identiques : package, apt

```
- name: Desinstaller Apache
  ansible.builtin.dnf:
    name: httpd
    state: absent
```

```
- name: Tout mettre a jour
  ansible.builtin.dnf:
    name: '*'
    state: latest
```

```
- name: Définir un module
  ansible.builtin.dnf:
    name: '@perl:5.26/minimal'
    state: present
```

```
- name: Installer le groupe Development Tools
  ansible.builtin.dnf:
    name: '@Development Tools'
    state: present
```

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



Généralités

Admin Sys

Fichiers

Rôles RHEL

Jinja2

SOUSCRIPTIONS

- **name:** Enregistre et s'attache à une souscription

```
community.general.redhat_subscription:
```

```
  username: yourusername
```

```
  password: yourpassword
```

```
  pool_ids: poolID
```

```
  state: present
```

- **name:** Active des dépôts Red Hat

```
community.general.rhsm_repository:
```

```
  name:
```

```
    - rhel-8-for-x86_64-baseos-rpms
```

```
    - rhel-8-for-x86_64-baseos-debug-rpms
```

```
  state: present
```

DÉPÔTS

- **name:** S'assure qu'un depot existe

```
ansible.builtin.yum_repository:
```

```
  file: example
```

```
  name: example-internal
```

```
  description: Depot interne ACME corp.
```

```
  baseurl: http://materials.example.com/yum/repository/
```

```
  enabled: yes
```

```
  gpgcheck: yes
```

```
  state: present
```




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

```
- name: Création d'un groupe auditeurs
  ansible.builtin.group:
    name: auditeurs
    state: present
    gid: 550
```

| Paramètre | Description |
|-----------|---|
| gid | GID du groupe |
| local | force l'utilisation de commandes à portée locale si elles sont installées (ie manipulation des groupes locaux versus ceux issus d'une AD) |
| name | nom du groupe |
| state | le groupe doit-il être present ou non sur le système distant |
| system | si yes, indique que le groupe est un groupe système |



Généralités

Admin Sys

Fichiers

Rôles RHEL

Jinja2

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

```
- name: Ajoute un utilisateur et ses groupes
  ansible.builtin.user:
    name: devops_user
    shell: /bin/bash
    groups: sys_admins, developers
    append: yes
    generate_ssh_key: yes
    ssh_key_bits: 2048
    ssh_key_file: .ssh/id_my_rsa
```

```
$ date +%s
1705161826
$ date --date='@1705161823'
Sat Jan 13 17:03:43 CET 2024
$
```

| Paramètre | Description |
|-------------|---|
| comment | description du compte |
| group | groupe principal |
| groups | liste des groupes additionnels. Si nul, tous les groups sont enlevés sauf le primaire |
| home | répertoire \$HOME de l'utilisateur |
| create_home | force ou non la création du répertoire home |
| uid | UID de l'utilisateur |
| password | hash du mot de passe |
| expires | date d'expiration du compte (Valeur epoch) |
| append | ajoute les groupes indiqués par 'groups' à ceux existant |

[Généralités](#)[Admin Sys](#)[Fichiers](#)[Rôles RHEL](#)[Jinja2](#)

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

```
---
- name: Configuration de mot de passe
  hosts: all
  gather_facts: no
  vars:
    - value: "motdepasse"
    - ht: "sha512"

  tasks:
    - name: Positionne un mot de passe pour user4 - cree user4 au besoin
      ansible.builtin.user:
        name: user4
        password: "{{ value | password_hash(hashtype=ht, ) }}"
```

- La documentation du module fournit plusieurs méthodes pour générer un hash

```
- name: copie une clef hôte sur un serveur
  ansible.builtin.known_hosts:
    path: /etc/ssh/ssh_known_hosts
    name: host1
    key: "{{ lookup('file', 'pubkeys/host1') }}"
```

Insère une clef d'hôte dans le 'known_hosts' distant

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

```
- name: Positionne un clef publique (exemple 1)
  ansible.posix.authorized_key:
    user: user1
    state: present
    key: "{{ lookup('file', '/home/user1/.ssh/id_rsa.pub') }}"
```

Insère une clef publique dans le
'authorized_hosts' distant

https://docs.ansible.com/ansible/latest/collections/ansible/posix/authorized_key_module.html

Avec lookup

En spécifiant
directement un fichier

```
- name: Positionne un clef publique (exemple 2)
  hosts: all

  tasks:
    - name: Positionne une clef publique
      ansible.posix.authorized_key:
        user: root
        state: present
        key: '{{ item }}'
      with_file:
        - ~/.ssh/id_rsa.pub
```



```
- ansible.builtin.cron:  
  name: "rotation des logs"  
  user: "root"  
  minute: 45  
  hour: 11  
  job:  
  "my_logrotate_script.sh"
```

| Paramètre | Description | |
|--------------|--|--|
| special_time | reboot, yearly, annually, monthly, weekly, daily, hourly | Notation de temps recurrent |
| state | absent, present | Indique si la commande doit exister ou être absente |
| cron_file | Null | on peut fournir un fichier crontab pré-écrit |
| backup | yes, no | Sauvegarde de la crontab en cours avant modification |

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



'ansible.builtin.service' = module générique
Actions communes (start, stop, restart, enable)

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

```
- name: start nginx
  ansible.builtin.service:
    name: nginx
    state: started
    enabled: true
```

| Paramètre | Description |
|-----------|--|
| name | Nom du service (firewalld, ...) |
| state | started / stopped / restarted / reloaded |
| enabled | true / false |

Module plus spécifique à systemd
Certaines distributions de linux n'utilisent pas systemd

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

```
- name: reload web server
  ansible.builtin.systemd:
    name: apache2
    state: reload
    daemon-reload: yes
    enabled: yes
```

| Paramètre | Description |
|---------------|---|
| daemon-reload | force la commande systemctl daemon-reload avant toute operation |
| name | Nom du service (firewalld, ...) |
| state | started / stopped / restarted / reloaded |
| enabled | yes / no /true / false |



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

- **name:** "Reboot après patch"
ansible.builtin.reboot:
 reboot_timeout: 180
- **name:** Reboot rapide
ansible.builtin.reboot:

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

- ```
Pause de 5 minutes
- ansible.builtin.pause:
 minutes: 5
```

[https://docs.ansible.com/ansible/latest/collections/ansible/builtin/wait\\_for\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/wait_for_module.html)

- **name:** Wait for web server to start  
**local\_action:**  
    **module:** wait\_for  
    **host:** "{{ webserver }}"  
    **port:** "{{ webserver\_port }}"  
    **delay:** 10  
    **timeout:** 300  
    **state:** started



Généralités

Admin Sys

Fichiers

Rôles RHEL

Jinja2

- à éviter autant que possible, mais ce n'est parfois pas possible
- nécessitent (sauf `ansible.builtin.raw`) Python sur la cible

```
- name: Lance une commande
 ansible.builtin.command:
 cmd: "uptime"
```

```
- name: cd somedir/ puis lance la commande en tant que
 db_owner, si /path/to/database n'existe pas
 ansible.builtin.command: /usr/bin/make_database.sh
 db_user db_name
 become: yes
 become_user: db_owner
 args:
 chdir: somedir/
 creates: /path/to/database
```

- Pas idempotent, remonte toujours un 'changed', on peut modifier ce comportement avec l'option 'creates' :

```
- name: Lance une commande si /tmp/uptime inexistant
 ansible.builtin.command:
 cmd: "uptime"
 creates: /tmp/uptime
```

- Module shell avec un chdir :

```
- name: cd somedir/ puis lance une commande
 ansible.builtin.shell:
 cmd: ls -l | grep log
 chdir: somedir/
```

- Approche non idempotente :

```
- name: Approche non idempotente avec le module shell
 ansible.builtin.shell:
 cmd: echo "nameserver 192.0.2.1" > /etc/resolv.conf
```

- Approche idempotente :

```
- name: Approche idempotente, avec le module copy
 ansible.builtin.copy:
 dest: /etc/resolv.conf
 content: "nameserver 192.0.2.1\n"
```



Généralités

Admin Sys

Fichiers

Rôles RHEL

Jinja2

- Se connecte à un service et vérifie le code retour ou le contenu renvoyé
- Par défaut les URLs sont suivies
- <https://curlconverter.com/ansible/>
- Forme de base :

```
- name: Test de site web
 ansible.builtin.uri:
 url: http://site.exemple.fr
 register: result
```

| Paramètre        | Description                            |
|------------------|----------------------------------------|
| follow_redirects | Suivi des redirections (all/safe/none) |
| status_code      | code retour attendu                    |
| return_content   | yes/no (à utiliser avec register)      |

```
- name: Test intranet web server
 hosts: localhost
 become: false
 tasks:
 - name: Connect to intranet web server
 ansible.builtin.uri:
 validate_certs: no
 force_basic_auth: yes
 user: username
 password: password
 url: https://servera.lab.example.com
 return_content: yes
 status_code: 200
 register: output
 - name: Display output
 ansible.builtin.debug:
 var: output.content
```

le contenu est stocké dans "output"

[https://docs.ansible.com/ansible/latest/collections/ansible/builtin/uri\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/uri_module.html)



[https://docs.ansible.com/ansible/latest/collections/ansible/builtin/lineinfile\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/lineinfile_module.html)

- **name:** Valide le fichier sudoers avant sauvegarde

```
ansible.builtin.lineinfile:
 path: /etc/sudoers
 state: present
 regexp: '^%ADMIN ALL='
 line: '%ADMIN ALL=(ALL) NOPASSWD: ALL'
 validate: /usr/sbin/visudo -cf %s
```

- **ansible.builtin.lineinfile:**  
 path: 'ifcfg-ens3'  
 backrefs: true  
 regexp: '^(ONBOOT=).\*\$'  
 line: '\1{{ myvar }}'  
 state: present

| Paramètre | Description                                                                      |
|-----------|----------------------------------------------------------------------------------|
| path      | Fichier à inspecter / modifier                                                   |
| regexp    | recherche l'expression mentionnée                                                |
| line      | la ligne à ajouter / enlever                                                     |
| state     | action à faire sur la ligne                                                      |
| validate  | action de verification à effectuer (cf visudo, mais aussi haproxy, rsyslog, ...) |
| owner     | propriétaire du fichier                                                          |
| groupe    | groupe du fichier                                                                |
| mode      | permissions (eg: mode: '0755')                                                   |



[https://docs.ansible.com/ansible/latest/collections/ansible/builtin/blockinfile\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/blockinfile_module.html)

```

- name: Demo blockinfile
 hosts: all
 gather_facts: no

 tasks:
 - name: Ajout d'un bloc de texte
 ansible.builtin.blockinfile:
 path: /tmp/myfile
 block: |
 Ligne 1 d'un bloc de texte
 Et maintenant la ligne deux.
 state: present
```

```
$ cat /tmp/myfile
Lorem ipsum dolor sit amet, consectetur
adipiscing elit.
BEGIN ANSIBLE MANAGED BLOCK
Ligne 1 d'un bloc de texte
Et maintenant la ligne deux.
END ANSIBLE MANAGED BLOCK
```

| Paramètre    | Description                                                                      |
|--------------|----------------------------------------------------------------------------------|
| path         | chemin du fichier à modifier                                                     |
| block        | Bloc de texte à ajouter / enlever                                                |
| state        | absent : enlève le bloc<br>present: ajoute le bloc                               |
| backup       | false   true                                                                     |
| create       | false   true                                                                     |
| validate     | action de verification à effectuer (cf visudo, mais aussi haproxy, rsyslog, ...) |
| insertafter  | EOF pour insérer à la fin du fichier, sinon on peut indiquer une regex de repère |
| insertbefore | BOF pour insérer en début de fichier, sinon on peut indiquer une regex de repère |



Généralités

Admin Sys

Fichiers

Rôles RHEL

Jinja2

- gère le contenu de fichiers .ini  
(ajoute, modifie, enlève des paramètres)
- ajout de sections manquantes
- se charge d'ajouter une ligne vide en fin de fichier (POSIX)

```
[drinks]
fav=lemonade
ice=no

[food]
starter=salad
main_course=chicken
```

```
- name: Ensure "fav=lemonade is in section "[drinks]" in specified file
 community.general.ini_file:
 path: /etc/conf
 section: drinks
 option: fav
 value: lemonade
 mode: '0600'
 backup: true
```

[https://docs.ansible.com/ansible/latest/collections/community/general/ini\\_file\\_module.html](https://docs.ansible.com/ansible/latest/collections/community/general/ini_file_module.html)





[https://docs.ansible.com/ansible/latest/collections/ansible/builtin/stat\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/stat_module.html)

```

- name: Demo stat
 hosts: all
 gather_facts: no

 tasks:
 - name: Utilisation de stat
 ansible.builtin.stat:
 path: /tmp/myfile
 checksum_algorithm: md5
 register: result

 - name: Affiche 'result'
 ansible.builtin.debug:
 var: result
```

Un dictionnaire avec environ 45 paramètres est renvoyé.

| Paramètre          | Description                                                 |
|--------------------|-------------------------------------------------------------|
| path               | Chemin d'accès au fichier                                   |
| follow             | false   true<br>Indique s'il faut suivre le lien symbolique |
| checksum_algorithm | md5   sha1 (défaut)   sha2254   sha256 [ sha384   sha512    |



- Depuis le système local vers une machine distante, sauf si contre-indication
- [https://docs.ansible.com/ansible/latest/collections/ansible/builtin/copy\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/copy_module.html)

```
- name: Copie de fichier et droits
 ansible.builtin.copy:
 src: foo.conf // implicite: ./files
 dest: /etc/foo.conf
 owner: foo
 group: foo
 mode: '0644'
 force: true
 backup: yes
```

Permet de créer le contenu d'un fichier aussi :

```
- ansible.builtin.copy:
 dest: /tmp/file.log
 content: |
 Lorem ipsum dolor sit amet,
 consectetur adipiscing elit,
 sed do eiusmod tempor incididunt
 ut labore et dolore magna aliqua.
```

| Paramètre  | Description                                                                                         |
|------------|-----------------------------------------------------------------------------------------------------|
| src        | chemin absolu ou relative de l'élément à transférer                                                 |
| dest       | où copier le fichier sur la machine distante                                                        |
| owner      | utilisateur d'appurtenance                                                                          |
| group      | groupe d'appartenance                                                                               |
| mode       | permissions du fichier                                                                              |
| backup     | yes   no                                                                                            |
| content    | quand un fichier est spécifié par 'dest', crée le fichier avec le contenu spécifié par cet attribut |
| remote_src | yes / no<br>le fichier à copier n'est pas local mais distant                                        |

| force le respect de la mise en page  
> pour tout aplatir sur une seule ligne



# Récupérer un fichier - ansible.builtin.fetch

29

Généralités

Admin Sys

Fichiers

Rôles RHEL

Jinja2

- [https://docs.ansible.com/ansible/latest/collections/ansible/builtin/fetch\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/fetch_module.html)
- Depuis le système distant vers le système de fichier local

```
- name: Récupère un fichier
 ansible.builtin.fetch:
 src: /home/user/.ssh/authorized_keys
 dest: ./directory/
 flat: yes
```

| Paramètre | Description                                                                                                                              |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------|
| src       | chemin absolu ou relatif du fichier                                                                                                      |
| dest      | emplacement en local                                                                                                                     |
| flat      | oui : le fichier est recopié directement en suivant le chemin<br>non : fichier recopié dans une arborescence<br><HOSTNAME>/chemin/absolu |



Positionne les attributs des fichiers, répertoires, liens symboliques  
Permet aussi d'effacer ces objets

```
- name: Modifie propriétés et permissions du fichier
 ansible.builtin.file:
 path: /etc/fichier.conf
 owner: foo
 group: foo
 mode: '0644'
```

```
- name: Efface un repertoire récursivement
 ansible.builtin.file:
 path: /etc/repertoire
 state: absent
```

| Paramètres | Description                                                                                 |
|------------|---------------------------------------------------------------------------------------------|
| src        | origine du lien (ce vers quoi le lien va pointer)                                           |
| dest       | nom du lien (ce qui pointe)                                                                 |
| owner      | propriétaire                                                                                |
| group      | groupe                                                                                      |
| mode       | permissions                                                                                 |
| state      | "absent" ← efface l'objet<br>"directory"<br>"file"<br>"hard"<br>"link"<br>"touch"           |
| recurse    | yes<br>applique les attributs récursivement<br>(uniquement quand 'state' est un repertoire) |

[https://docs.ansible.com/ansible/latest/collections/ansible/builtin/file\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/file_module.html)



```

- hosts: all
 gather_facts: no
 vars:
 file: sslscan-2.0.16.tgz

 tasks:
 - community.general.archive:
 path:
 - /opt/repertoire_1
 - /opt/repertoire_2
 dest: /tmp/{{ file }}
 format: bz2
```

- Crée une archive
- sources et archive sont sur l'hôte distant, rien n'est recopié sur le contrôleur
- on peut effacer après coup les fichiers archivés (remove: true)

| Paramètre    | Description                                                                  |
|--------------|------------------------------------------------------------------------------|
| path         | emplacement (distant) des chemins à placer dans l'archive; accepte une liste |
| dest         | emplacement où placer l'archive                                              |
| format       | type de compression à utiliser (bz2, gz, xz, tar, zip)                       |
| remove       | Efface les objets archives (true/false, false par défaut)                    |
| exclude_path | liste de chemins à exclure                                                   |

[https://docs.ansible.com/ansible/latest/collections/community/general/archive\\_module.html](https://docs.ansible.com/ansible/latest/collections/community/general/archive_module.html)



```

```

```
- hosts: all
 gather_facts: no

 tasks:
 - ansible.builtin.file:
 path: /tmp/tmp3
 state: directory

 - ansible.builtin.unarchive:
 src: sslscan-2.0.16.tar.gz
 dest: /tmp/tmp3
```

- Décompression d'une archive sur la machine distante
- Par défaut, l'archive à décompresser est copiée sur la cible depuis le contrôleur
- possibilité de lister après coup les fichiers qui ont été créés

[https://docs.ansible.com/ansible/latest/collections/ansible/builtin/unarchive\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/builtin/unarchive_module.html)

```
- name: Creation du repertoire de destination
 ansible.builtin.file:
 path: /opt/tomcat
 state: directory

- ansible.builtin.unarchive:
 src: "http://apache.org/apache-tomcat-8.5.15.tar.gz"
 dest: /opt/tomcat/ # already existing path
 creates: /opt/tomcat/
 remote_src: yes
```

| Paramètre  | Description                                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------|
| src        | emplacement (local ou distant) de l'archive                                                                     |
| remote_src | true si la source est à chercher sur la machine distante ou à télécharger                                       |
| dest       | emplacement où décompresser l'archive                                                                           |
| creates    | répertoire témoin, signe que l'archive a déjà été décompressée ou non, pour savoir s'il faut passer l'opération |





Collection `ansible.posix`

Nécessite `rsync` sur les deux systèmes

Utiliser `rsync` avec `ansible.builtin.command` pour les cas nécessitant une utilisation avancée.

```

- name: Demo synchronize
 hosts: all
 gather_facts: no

 tasks:
 # recopie le repertoire artefact dans /tmp
 distant
 - name: Utilisation de synchronize
 ansible.posix.synchronize:
 src: artefact
 dest: /tmp
 recursive: true
```

| Paramètre                          | Description                                                                                                     |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| compress                           | false   true                                                                                                    |
| delete                             | false   true<br>efface les fichiers sur la destination qui n'existent pas dans src (nécessite recursive = true) |
| src                                |                                                                                                                 |
| dest                               |                                                                                                                 |
| recursive                          | false   true                                                                                                    |
| + options sur les permissions, ... |                                                                                                                 |

[https://docs.ansible.com/ansible/latest/collections/ansible/posix/synchronize\\_module.html](https://docs.ansible.com/ansible/latest/collections/ansible/posix/synchronize_module.html)

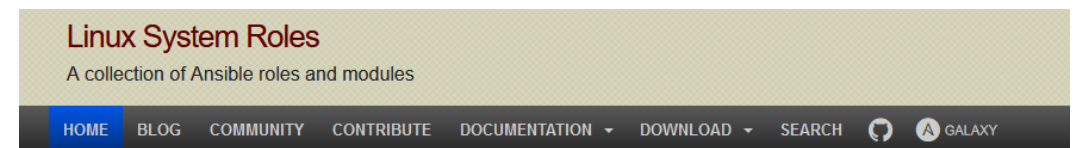
- Depuis RHEL 7.4, paquetage `rhel-system-roles` disponible pour gérer différents aspects toutes versions RH confondues (RHEL >6.1)  
par exemple, `ntpd` a été remplacé par `chronyd` → cf rôle "timesync"
- `dnf install rhel-system-roles` → `/usr/share/ansible/roles`
- Documentation : `/usr/share/doc/ansible/roles`
- environ 30 rôles
- pour gérer un parc mixant différentes versions de RedHat

Projet upstream :

<https://linux-system-roles.github.io/>

| Configuration related roles |                                |                 |              |              |
|-----------------------------|--------------------------------|-----------------|--------------|--------------|
| timesync                    | Time synchronization           | RHEL 6, 7, 8, 9 | RHEL 7, 8, 9 | RHEL 7.6/8.0 |
| network                     | Networking                     | RHEL 6, 7, 8, 9 | RHEL 7, 8, 9 | RHEL 7.6/8.0 |
| kdump                       | Kernel dumps                   | RHEL 6, 7, 8, 9 | RHEL 7, 8, 9 | RHEL 7.6/8.0 |
| storage                     | Storage                        | RHEL 7, 8, 9    | RHEL 7, 8, 9 | RHEL 7.6/8.1 |
| postfix                     | Postfix (mail transfer agent)  | RHEL 6, 7, 8, 9 | RHEL 7, 8, 9 | RHEL 7.6/8.0 |
| kernel_settings             | Kernel settings                | RHEL 7, 8, 9    | RHEL 7, 8, 9 | RHEL 7.9/8.3 |
| logging                     | Logging (rsyslog)              | RHEL 7, 8, 9    | RHEL 7, 8, 9 | RHEL 7.9/8.3 |
| metrics                     | Metrics (Performance Co-Pilot) | RHEL 6, 7, 8, 9 | RHEL 7, 8, 9 | RHEL 7.9/8.3 |
| ha_cluster                  | High availability clustering   | RHEL 8, 9       | RHEL 7, 8, 9 | RHEL 7.9/8.4 |
| cockpit                     | Web console                    | RHEL 7, 8, 9    | RHEL 8, 9    | RHEL 8.6/9.0 |

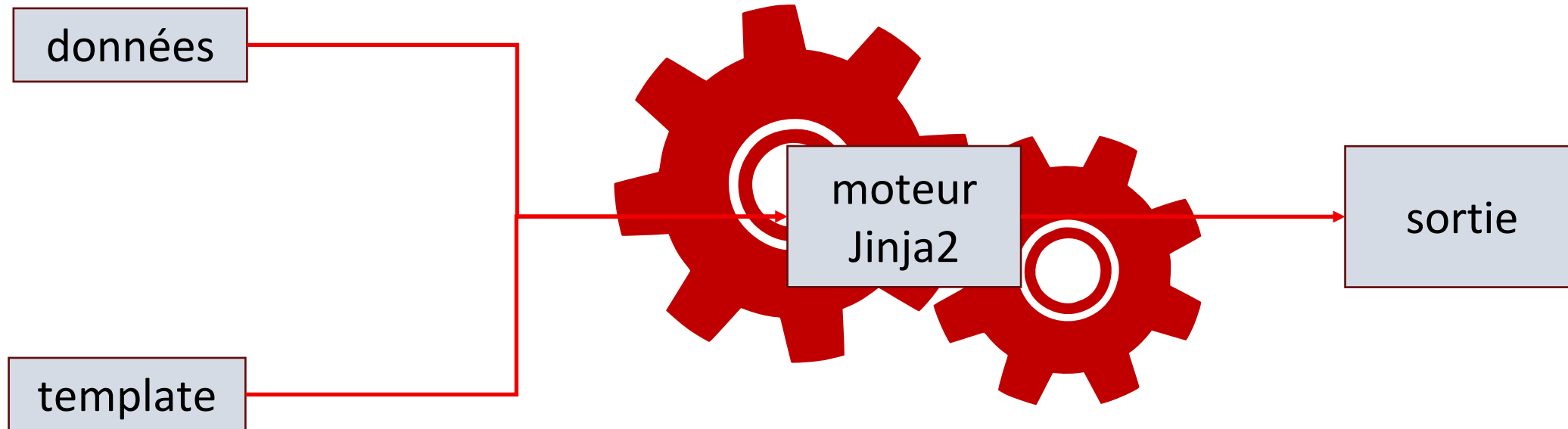
<https://access.redhat.com/articles/3050101>



The **Linux System Roles** are a set of Ansible Roles, also available as an Ansible Collection, used to manage and configure common GNU/Linux operating system components. Conceptually, the intent is to provide for the operating system components an automation "API" that is consistent across multiple major and minor releases. The roles are available in Ansible Galaxy at [linux-system-roles](https://galaxy.ansible.com/fedora/linux_system_roles). If you would prefer to use a collection instead of individual roles, see [https://galaxy.ansible.com/fedora/linux\\_system\\_roles](https://galaxy.ansible.com/fedora/linux_system_roles)

[https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/9/html/automating\\_system\\_administration\\_by\\_using\\_rhel\\_system\\_roles/index](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/automating_system_administration_by_using_rhel_system_roles/index)

<https://ttl255.com/jinja2-tutorial-part-1-introduction-and-variable-substitution/>  
<https://ttl255.com/jinja2-tutorial-part-2-loops-and-conditionals/>



<https://jinja.palletsprojects.com/en/3.1.x/>

Généralités

Admin Sys

Fichiers

Rôles RHEL

Jinja2

ansible.cfg

```
[defaults]
ansible_managed = Gere par ANSIBLE
```

datas.yml

```

packages:
 - git
 - tmux
 - tree

os_name: Red Hat
```

modele.j2

```
{{ ansible_managed }}
Voici la liste des packages :

{% for my_item in packages %}
 {{ loop.index }} {{ my_item }}
{% endfor %}

OS destination : {{ os_name }}

Ansible fact: {{ ansible_facts['distribution'] }}
```

```

- name: Test jinja2
 hosts: localhost
 connection: local

 tasks:
 - name: Genere le fichier
 ansible.builtin.template:
 src: modele.j2
 dest: /tmp/output.txt
```

jinja2-demo.yml

```
ansible-playbook -e@datas.yml -i inventory jinja2.yml
```



## playbook.yml

```

- name: Test jinja2
 hosts: all

 tasks:
 - name: Genere le fichier
 ansible.builtin.template:
 src: etc-hosts.j2
 dest: /tmp/output.txt
```

## /tmp/output

```
192.168.1.1 server01.example.com server01
192.168.1.2 server02.example.com server02
192.168.1.3 server03.example.com server03
```

## etc-hosts.j2

```
{% for host in groups['all'] %}
{{ hostvars[host]['ansible_facts']['default_ipv4']['address'] }} {{ hostvars[host]['ansible_facts']['fqdn'] }} {{
hostvars[host]['ansible_facts']['hostname'] }}
{% endfor %}
```

### Structure de contrôle

```
{% if kenny.sick %}
 Kenny is sick.
{% elif kenny.dead %}
 You killed Kenny!
{% else %}
 Kenny looks okay --- so far
{% endif %}
```

### Structure de contrôle avec filtre

```
{% if myvar | int is odd %}
Variable impaire
{% elif myvar | int is even %}
Variable paire
{% endif %}
```

### Générer du texte de remplissage

```
{{ lipsum(n=5, html=false, min=20, max=100) }}
```





**Merci**

