Ansible

Travaux pratiques

Marc Baudoin

Hybrix

N'ALLEZ PAS PLUS LOIN QUE LA TROISIÈME PAGE

Ces exercices sont destinés :

- à vous familiariser avec la syntaxe et le fonctionnement d'Ansible ;
- à vous permettre d'approfondir certains aspects abordés dans la partie théorique ;
- à prendre conscience de problèmes usuels rencontrés dans l'utilisation d'Ansible et à voir comment les résoudre ;
- à déclencher des questions : n'hésitez pas à les poser.

Évidemment, ces exercices contiennent des pièges... Si vous tombez dedans, rien de grave, c'est fait pour. Si vous les détectez, c'est bien mais il n'y a malheureusement rien à gagner.

Environnement de travaux pratiques

Votre machine de contrôle dispose déjà d'un fichier `ansible.cfg` et d'un inventaire. N'hésitez pas à les consulter mais ne les modifiez pas pour l'instant.

Ansible est installé sur la machine de contrôle et les clés SSH sont en place (sans mot de passe).

La commande `sudo` est configurée (sans mot de passe) sur les machines à gérer.

Les éditeurs de texte `vim` et `nano` sont installés sur la machine de contrôle. Vous pouvez en installer d'autres au besoin ou travailler sur votre propre machine et transférer les fichiers sur la machine de contrôle.

Les quatre premiers exercices sont à réaliser sous la forme d'un livret autonome pour chacun.

Exercice 1

1. Créer un ensemble de répertoires `/home1` … `/home9`.
2. Créer un ensemble de liens symboliques `/auto/home1` → `/home1`, etc.

Exercice 2

Créer une archive `/tmp/etc.tar.gz` du répertoire `/etc`.

Qu'en est-il de l'idempotence ?

Exercice 3

1. Créer un utilisateur (ne pas spécifier de numéro d'utilisateur, le prochain numéro libre sera automatiquement utilisé).
2. Configurer l'exécution d'une tâche planifiée pour le daemon `cron` (par exemple la commande `date >> /tmp/date` afin de pouvoir facilement vérifier qu'elle a correctement fonctionné) à faire exécuter sous l'identité de l'utilisateur créé ci-dessus dans la minute qui suit l'exécution de la commande `ansible-playbook` (ne pas spécifier d'autres paramètres tels que l'heure, le jour ou le mois, ceci est sans intérêt pour cet exercice).

   Qu'en est-il de l'idempotence ?

Exercice 4

1. Configurer le service de journalisation rsyslog pour placer les messages de la catégorie `local4` dans le fichier `/var/log/test`. Pour cela, ajouter la ligne suivante dans le fichier `/etc/rsyslog.conf` ou créer un fichier la contenant et ayant l'extension `.conf` dans le répertoire `/etc/rsyslog.d` :

   ```
   local4.*        /var/log/test
   ```

   Si la configuration du service de journalisation rsyslog est effectivement modifiée, il est ensuite nécessaire de redémarrer ce service.
2. Tester le bon fonctionnement de la journalisation au moyen de la commande `logger`.

Le cinquième exercice est à réaliser sous forme de rôles.

Exercice 5

1. Faire d'une machine un serveur NFS :

   a) installer le paquet :

      - `nfs-utils` sur *Red Hat Enterprise Linux* et Fedora
      - `nfs-kernel-server` sur Debian et Ubuntu

   b) créer le répertoire `/srv/nfs`

   c) ajouter au fichier `/etc/exports` une ligne contenant :

   ```
   /srv/nfs        198.51.100.0/24(rw)
   ```

   (adapter la plage d'adresses à celle du réseau local)

   d) lancer ou relancer le service `nfs-server`

2. Faire de l'autre machine un client NFS :

   a) installer le paquet :

      - `nfs-utils` sur *Red Hat Enterprise Linux* et Fedora
      - `nfs-common` sur Debian et Ubuntu

   b) ajouter une entrée correcte dans le fichier `/etc/fstab`

   c) effectuer le montage

Solution 1

Avec la nouvelle syntaxe pour les boucles :

```
---
- name: Exercice 1
  hosts: test
  become: true
  tasks:
    - name: Répertoires /home1 ... /home9
      ansible.builtin.file:
        path: /home{{ item }}
        state: directory
        owner: root
        group: root
        mode: '755'
      loop: "{{ range ( 1 , 9 + 1 ) | list }}" # noqa: jinja[spacing]
    - name: Répertoire /auto
      ansible.builtin.file:
        path: /auto
        state: directory
        owner: root
        group: root
        mode: '755'
    - name: Liens symboliques /auto/home1 ... /auto/home9
      ansible.builtin.file:
        path: /auto/home{{ item }}
        src: /home{{ item }}
        state: link
        owner: root
        group: root
      loop: "{{ range ( 1 , 9 + 1 ) | list }}" # noqa: jinja[spacing]
```

Avec l'ancienne syntaxe pour les boucles :

```
---
- name: Exercice 1
  hosts: test
  become: true
  tasks:
    - name: Répertoires /home1 ... /home9
      ansible.builtin.file:
        path: /home{{ item }}
        state: directory
        owner: root
        group: root
        mode: '755'
      with_sequence: start=1 end=9
    - name: Répertoire /auto
      ansible.builtin.file:
        path: /auto
        state: directory
        owner: root
        group: root
        mode: '755'
    - name: Liens symboliques /auto/home1 ... /auto/home9
      ansible.builtin.file:
        path: /auto/home{{ item }}
        src: /home{{ item }}
        state: link
        owner: root
        group: root
      with_sequence: start=1 end=9
```

Solution 2

Avec le module `community.general.archive` (idempotence excellente mais au prix d'une utilisation des ressources potentiellement importante) :

```
---
- name: Exercice 2
  hosts: test
  become: true
  tasks:
    - name: Archive du répertoire /etc
      community.general.archive:
        path: /etc
        dest: /tmp/etc.tar.gz
        owner: root
        group: root
        mode: '444'
```

Avec le module `ansible.builtin.command` (idempotence imparfaite mais très faible utilisation des ressources) :

```
---
- name: Exercice 2 (version ansible.builtin.command)
  hosts: test
  become: true
  tasks:
    - name: Archive du répertoire /etc
      ansible.builtin.command:
        cmd: tar cvfz /tmp/etc.tar.gz /etc
        creates: /tmp/etc.tar.gz
```

Solution 3

```yaml
---
- name: Exercice 3
  hosts: test
  become: true
  tasks:
    - name: Utilisateur jlapin
      ansible.builtin.user:
        name: jlapin
        group: users
        comment: 'Jojo Lapin'
    - name: Tâche planifiée
      ansible.builtin.cron:
        name: cron
        cron_file: date
        minute: "{{ ( ansible_date_time.minute | int + 1 ) % 60 }}" # noqa: jinja[spacing]
        user: jlapin
        job: date >> /tmp/date
```

Solution 4

Avec le module `ansible.builtin.lineinfile` :

```
---
- name: Exercice 4
  hosts: test
  become: true
  tasks:
    - name: Configuration rsyslog
      ansible.builtin.lineinfile:
        path: /etc/rsyslog.conf
        line: 'local4.*         /var/log/test'
        regexp: '^local4'
      notify:
        - rsyslog_restart
  handlers:
    - name: Redémarrage de rsyslog
      ansible.builtin.service:
        name: rsyslog
        state: restarted
      listen: rsyslog_restart
```

Avec le module `ansible.builtin.copy` :

```
---
- name: Exercice 4
  hosts: test
  become: true
  tasks:
    - name: Configuration rsyslog
      ansible.builtin.copy:
        src: local4.conf
        dest: /etc/rsyslog.d/local4.conf
        owner: root
        group: root
        mode: '444'
      notify:
        - rsyslog_restart
  handlers:
    - name: Redémarrage de rsyslog
      ansible.builtin.service:
        name: rsyslog
        state: restarted
```

```
      listen: rsyslog_restart
```

Test isolé :

```
---
- name: Exercice 4
  hosts: test
  tasks:
    - name: Test rsyslog
      community.general.syslogger:
        msg: 'test rsyslog'
        facility: local4
        priority: info
```

Test intégré :

```
---
- name: Exercice 4
  hosts: test
  become: true
  tasks:
    - name: Configuration rsyslog
      ansible.builtin.lineinfile:
        path: /etc/rsyslog.conf
        line: 'local4.*         /var/log/test'
        regexp: '^local4'
      notify:
        - rsyslog_restart
        - rsyslog_test
  handlers:
    - name: Redémarrage de rsyslog
      ansible.builtin.service:
        name: rsyslog
        state: restarted
      listen: rsyslog_restart
    - name: Test rsyslog
      community.general.syslogger:
        msg: 'test rsyslog'
        facility: local4
        priority: info
      listen: rsyslog_test
```

Solution 5

organisation des fichiers

```
├── ansible.cfg
├── hosts
├── nfs.yml
└── roles/
    ├── nfs_client/
    │   ├── tasks/
    │   │   └── main.yml
    │   └── vars/
    │       ├── Debian.yml
    │       └── RedHat.yml
    └── nfs_serveur/
        ├── handlers/
        │   └── main.yml
        ├── tasks/
        │   └── main.yml
        └── vars/
            ├── Debian.yml
            └── RedHat.yml
```

hosts

```
[nfs_serveur]
test1.example.com nfs_serveur_reseau=198.51.100.0/24

[nfs_client]
test2.example.com nfs_client_serveur=test1.example.com nfs_client_chemin=/srv/nfs
```

nfs.yml

```
---

- name: Exercice 5 (serveur)
  hosts: nfs_serveur
  become: true
  roles:
    - nfs_serveur

- name: Exercice 5 (client)
  hosts: nfs_client
  become: true
  roles:
    - nfs_client
```

roles/nfs_serveur/vars/RedHat.yml

```
---

nfs_serveur_paquet: nfs-utils
```

roles/nfs_serveur/vars/Debian.yml

```
---

nfs_serveur_paquet: nfs-kernel-server
```

roles/nfs_serveur/tasks/main.yml

```yaml
---

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

- name: Installation serveur NFS
  ansible.builtin.package:
    name: "{{ nfs_serveur_paquet }}"
    state: present
  notify:
    - nfs_serveur_start_enable

- name: Répertoire /srv/nfs
  ansible.builtin.file:
    path: /srv/nfs
    state: directory
    owner: root
    group: root
    mode: '755'

- name: Fichier /etc/exports
  ansible.builtin.lineinfile:
    path: /etc/exports
    line: '/srv/nfs     {{ nfs_serveur_reseau }}(rw)'
    regexp: '^/srv/nfs'
  notify:
    - nfs_serveur_restart
  tags:
    - nfs_serveur_exports
```

roles/nfs_serveur/handlers/main.yml

```yaml
---

- name: Démarrage et activation NFS
  ansible.builtin.service:
    name: nfs-server
    state: started
    enabled: true
  listen: nfs_serveur_start_enable

- name: Redémarrage NFS
  ansible.builtin.service:
    name: nfs-server
    state: restarted
  listen: nfs_serveur_restart
```

roles/nfs_client/vars/RedHat.yml

```
---

nfs_client_paquet: nfs-utils
```

roles/nfs_client/vars/Debian.yml

```
---

nfs_client_paquet: nfs-common
```

roles/nfs_client/tasks/main.yml

```
---

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

- name: Installation client NFS
  ansible.builtin.package:
    name: "{{ nfs_client_paquet }}"
    state: present

- name: Configuration de /etc/fstab et montage du serveur NFS
  ansible.posix.mount:
    src: "{{ nfs_client_serveur }}:{{ nfs_client_chemin }}"
    path: /mnt
    fstype: nfs
    state: mounted
```

Coulisses

hosts

```
[ovhcloud_controle]
d2-2-sbg5-1     ansible_host=51.68.82.220       ovhcloud_stagiaire=1
d2-2-sbg5-10    ansible_host=51.68.82.221       ovhcloud_stagiaire=2

[ovhcloud_victimes]
d2-2-sbg5-2     ansible_host=217.182.93.167     ovhcloud_stagiaire=1
d2-2-sbg5-3     ansible_host=51.91.147.253      ovhcloud_stagiaire=1
d2-2-sbg5-4     ansible_host=217.182.93.168     ovhcloud_stagiaire=2
d2-2-sbg5-5     ansible_host=51.91.147.254      ovhcloud_stagiaire=2

[ovhcloud:children]
ovhcloud_controle
ovhcloud_victimes

[ovhcloud:vars]
ansible_ssh_private_key_file=/home/babafou/.ssh/id_ecdsa-ovh
ansible_user=rocky
```

ovhcloud.yml

```yaml
---

- name: Toutes les machines
  hosts: ovhcloud
  become: true
  tasks:
    - name: Authentification par mot de passe (EL8)
      ansible.builtin.lineinfile:
        path: /etc/ssh/sshd_config
        line: PasswordAuthentication yes
        regexp: ^PasswordAuthentication
      when:
        - ansible_os_family == 'RedHat'
        - ansible_distribution_major_version == '8'
      notify:
        - ovhcloud_sshd_restart
    - name: Authentification par mot de passe (EL9, EL10)
      ansible.builtin.file:
        path: /etc/ssh/sshd_config.d/50-cloud-init.conf
        state: absent
      when:
        - ansible_os_family == 'RedHat'
        - ansible_distribution_major_version in [ '9' ,'10' ]
      notify:
        - ovhcloud_sshd_restart
    - name: Fuseau horaire
      community.general.timezone:
        name: Europe/Paris
      notify:
        - ovhcloud_cron_{{ ansible_os_family }}
    - name: Utilisateur formation
      ansible.builtin.user:
        name: formation
        password: $6$1ZqdoMck$f9IVc0e4oKobabuEk8N4EO.2
            moqORZ8GEbLw0JNnD6ifRXxfx0OQyWJmdWjbRIiirqNBrJNwwhBrz1KiTThcK1
        # toto
        uid: 1664
        group: users
        comment: 'stagiaire formation'
        shell: /bin/bash
    - name: Répertoire ~formation/.ssh
      ansible.builtin.file:
        path: /home/formation/.ssh
        state: directory
        owner: formation
        group: users
        mode: '700'
    - name: Fichier /etc/sudoers.d/formation
      ansible.builtin.copy:
        content: "formation     ALL = (root) NOPASSWD: ALL\n" # noqa: no-tabs
        dest: /etc/sudoers.d/formation
        owner: root
```

```
        group: root
        mode: '444'
# pas besoin de désactiver firewalld
  handlers:
    - name: Redémarrage de sshd
      ansible.builtin.service:
        name: sshd
        state: restarted
      listen: ovhcloud_sshd_restart
    - name: Redémarrage de cron
      ansible.builtin.service:
        name: cron
        state: restarted
      listen: ovhcloud_cron_Debian
    - name: Redémarrage de crond
      ansible.builtin.service:
        name: crond
        state: restarted
      listen: ovhcloud_cron_RedHat

- name: Machines de contrôle
  hosts: ovhcloud_controle
  become: true
  tasks:
    - name: EPEL
      ansible.builtin.package:
        name: epel-release
        state: present
      when:
        - ansible_os_family == 'RedHat'
        - ansible_distribution_major_version != '10'
    - name: PPA Ansible
      ansible.builtin.apt_repository:
        repo: ppa:ansible/ansible
      when: ansible_distribution == 'Ubuntu'
    - name: Installation d'Ansible
      ansible.builtin.package:
        name: ansible
        state: present
      when: ansible_os_family != 'RedHat' or
          ansible_distribution_major_version != '10'
    - name: Installation d'Ansible
      ansible.builtin.package:
        name: ansible-core
        state: present
      when:
        - ansible_os_family == 'RedHat'
        - ansible_distribution_major_version == '10'
    - name: Installations (autres paquets)
      ansible.builtin.package:
        name: [ nano , tree , unzip , vim ] # noqa: yaml[brackets] yaml[
            commas]
        state: present
    - name: Répertoire ~formation/.vim
```

```
    ansible.builtin.file:
      path: /home/formation/.vim
      state: directory
      owner: formation
      group: users
      mode: '755'
  - name: Couleurs pour Vim
    ansible.builtin.unarchive:
      src: https://www.vim.org/scripts/download_script.php?src_id=18915
      dest: /home/formation/.vim
      remote_src: true
      creates: /home/formation/.vim/colors
      owner: formation
      group: users
  - name: Fichier ~formation/.vimrc
    ansible.builtin.copy:
      content: |
        set t_Co=256
        colorscheme calmar256-light
        autocmd FileType yaml set cursorcolumn cursorline
      dest: /home/formation/.vimrc
      owner: formation
      group: users
      mode: '644'
  - name: Fichier ~formation/ansible.cfg
    community.general.ini_file:
      path: /home/formation/ansible.cfg
      section: defaults
      option: inventory
      value: hosts
      owner: formation
      group: users
      mode: '444'
  - name: Fichier ~formation/ansible.cfg (suppression d'une ligne blanche)
    ansible.builtin.lineinfile:
      path: /home/formation/ansible.cfg
      regexp: ^$
      state: absent
  - name: Fichier ~formation/hosts
    ansible.builtin.template:
      src: hosts.j2
      dest: /home/formation/hosts
      owner: formation
      group: users
      mode: '644'
  - name: Fichiers ~formation/.ssh/id_ed25519*
    community.crypto.openssh_keypair:
      path: /home/formation/.ssh/id_ed25519
      type: ed25519
      # passphrase: toto
      owner: formation
      group: users
  - name: Récupération du fichier ~formation/.ssh/id_ed25519.pub
    ansible.builtin.fetch:
```

```
        src: /home/formation/.ssh/id_ed25519.pub
        dest: /tmp/id_ed25519.pub-{{ ovhcloud_stagiaire }}
        flat: true

- name: Machines à gérer
  hosts: ovhcloud_victimes
  become: true
  tasks:
    - name: Transfert du fichier ~formation/.ssh/authorized_keys
      ansible.builtin.copy:
        src: /tmp/id_ed25519.pub-{{ ovhcloud_stagiaire }}
        dest: /home/formation/.ssh/authorized_keys
        owner: formation
        group: users
        mode: '600'
```

hosts.j2

```
[test]
{% for item in groups.ovhcloud_victimes %}
{% if hostvars[item]['ovhcloud_stagiaire'] == ovhcloud_stagiaire %}
{{ hostvars[item]['inventory_hostname'] }}      ansible_host={{
   hostvars[item]['ansible_host'] }}
{% endif %}
{% endfor %}

[test:vars]
ansible_ssh_extra_args='-o StrictHostKeyChecking=accept-new'
```