

Ansible

Travaux pratiques

Marc Baudoin

Hybrix

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

Le cinquième exercice est à réaliser sous forme de rôles.

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`.

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`:

<code>local4.*</code>	<code>/var/log/test</code>
-----------------------	----------------------------

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`.

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 :

<code>/srv/nfs</code>	<code>198.51.100.0/24(rw)</code>
-----------------------	----------------------------------

(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 :

```
1 ---
2 - name: Exercice 1
3   hosts: test
4   become: true
5   tasks:
6     - name: Répertoires /home1 ... /home9
7       ansible.builtin.file:
8         path: /home{{ item }}
9         state: directory
10        owner: root
11        group: root
12        mode: '755'
13        loop: "{{ range ( 1 , 9 + 1 ) | list }}" # noqa: jinja[spacing]
14    - name: Répertoire /auto
15      ansible.builtin.file:
16        path: /auto
17        state: directory
18        owner: root
19        group: root
20        mode: '755'
21    - name: Liens symboliques /auto/home1 ... /auto/home9
22      ansible.builtin.file:
23        path: /auto/home{{ item }}
24        src: /home{{ item }}
25        state: link
26        owner: root
27        group: root
28        loop: "{{ range ( 1 , 9 + 1 ) | list }}" # noqa: jinja[spacing]
```

Avec l'ancienne syntaxe pour les boucles :

```
1 ---
2 - name: Exercice 1
3   hosts: test
4   become: true
5   tasks:
6     - name: Répertoires /home1 ... /home9
7       ansible.builtin.file:
8         path: /home{{ item }}
9         state: directory
10        owner: root
11        group: root
12        mode: '755'
13    with_sequence: start=1 end=9
14    - name: Répertoire /auto
15      ansible.builtin.file:
16        path: /auto
17        state: directory
18        owner: root
19        group: root
20        mode: '755'
21    - name: Liens symboliques /auto/home1 ... /auto/home9
22      ansible.builtin.file:
23        path: /auto/home{{ item }}
24        src: /home{{ item }}
25        state: link
26        owner: root
27        group: root
28    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) :

```
1 ---
2 - name: Exercice 2
3   hosts: test
4   become: true
5   tasks:
6     - name: Archive du répertoire /etc
7       community.general.archive:
8         path: /etc
9         dest: /tmp/etc.tar.gz
10        owner: root
11        group: root
12        mode: '444'
```

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

```
1 ---
2 - name: Exercice 2 (version ansible.builtin.command)
3   hosts: test
4   become: true
5   tasks:
6     - name: Archive du répertoire /etc
7       ansible.builtin.command:
8         cmd: tar cvfz /tmp/etc.tar.gz /etc
9         creates: /tmp/etc.tar.gz
```

Solution 3

```
1 ---
2 - name: Exercice 3
3   hosts: test
4   become: true
5   tasks:
6     - name: Utilisateur jlapiin
7       ansible.builtin.user:
8         name: jlapiin
9         group: users
10        comment: 'Jojo Lapin'
11    - name: Tâche planifiée
12      ansible.builtin.cron:
13        name: cron
14        cron_file: date
15        minute: "{{ ( ansible_date_time.minute | int + 1 ) % 60 }}" # noqa: jinja[spacing]
16        user: jlapiin
17        job: date >> /tmp/date
```

Solution 4

Avec le module `ansible.builtin.lineinfile`:

```
1 ---
2 - name: Exercice 4
3   hosts: test
4   become: true
5   tasks:
6     - name: Configuration rsyslog
7       ansible.builtin.lineinfile:
8         path: /etc/rsyslog.conf
9         line: 'local4.*          /var/log/test'
10        regexp: '^local4'
11      notify:
12        - rsyslog_restart
13    handlers:
14      - name: Redémarrage de rsyslog
15        ansible.builtin.service:
16          name: rsyslog
17          state: restarted
18        listen: rsyslog_restart
```

Avec le module `ansible.builtin.copy`:

```
1 ---
2 - name: Exercice 4
3   hosts: test
4   become: true
5   tasks:
6     - name: Configuration rsyslog
7       ansible.builtin.copy:
8         src: local4.conf
9         dest: /etc/rsyslog.d/local4.conf
10        owner: root
11        group: root
12        mode: '444'
13      notify:
14        - rsyslog_restart
15    handlers:
16      - name: Redémarrage de rsyslog
17        ansible.builtin.service:
18          name: rsyslog
19          state: restarted
```

```
20 listen: rsyslog_restart
```

Test isolé :

```
1 ---
2 - name: Exercice 4
3   hosts: test
4   tasks:
5     - name: Test rsyslog
6       community.general.syslogger:
7         msg: 'test rsyslog'
8         facility: local4
9         priority: info
```

Test intégré :

```
1 ---
2 - name: Exercice 4
3   hosts: test
4   become: true
5   tasks:
6     - name: Configuration rsyslog
7       ansible.builtin.lineinfile:
8         path: /etc/rsyslog.conf
9         line: 'local4.* /var/log/test'
10        regexp: '^local4'
11      notify:
12        - rsyslog_restart
13        - rsyslog_test
14    handlers:
15      - name: Redémarrage de rsyslog
16        ansible.builtin.service:
17          name: rsyslog
18          state: restarted
19        listen: rsyslog_restart
20      - name: Test rsyslog
21        community.general.syslogger:
22          msg: 'test rsyslog'
23          facility: local4
24          priority: info
25        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

```
1 [nfs_serveur]
2 test1.example.com nfs_serveur_reseau=198.51.100.0/24
3
4 [nfs_client]
5 test2.example.com nfs_client_serveur=test1.example.com nfs_client_chemin=/srv/nfs
```

nfs.yml

```
1 ---
2
3 - name: Exercice 5 (serveur)
4   hosts: nfs_serveur
5   become: true
6   roles:
7     - nfs_serveur
8
9 - name: Exercice 5 (client)
10  hosts: nfs_client
11  become: true
12  roles:
13    - nfs_client
```

roles/nfs_serveur/vars/RedHat.yml

```
1 ---
2
3 nfs_serveur_paquet: nfs-utils
```

roles/nfs_serveur/vars/Debian.yml

```
1 ---
2
3 nfs_serveur_paquet: nfs-kernel-server
```

roles/nfs_serveur/tasks/main.yml

```
1 ---
2
3 - name: Inclusion des variables
4   ansible.builtin.include_vars: "{{ ansible_os_family }}.yml"
5
6 - name: Installation serveur NFS
7   ansible.builtin.package:
8     name: "{{ nfs_serveur_paquet }}"
9     state: present
10  notify:
11    - nfs_serveur_start_enable
12
13 - name: Répertoire /srv/nfs
14   ansible.builtin.file:
15     path: /srv/nfs
16     state: directory
17     owner: root
18     group: root
19     mode: '755'
20
21 - name: Fichier /etc/exports
22   ansible.builtin.lineinfile:
23     path: /etc/exports
24     line: '/srv/nfs      {{ nfs_serveur_reseau }}(rw)'
25     regexp: '^/srv/nfs'
26   notify:
27     - nfs_serveur_restart
28   tags:
29     - nfs_serveur_exports
```

roles/nfs_serveur/handlers/main.yml

```
1 ---
2
3 - name: Démarrage et activation NFS
4   ansible.builtin.service:
5     name: nfs-server
6     state: started
7     enabled: true
8   listen: nfs_serveur_start_enable
9
10 - name: Redémarrage NFS
11   ansible.builtin.service:
12     name: nfs-server
13     state: restarted
14   listen: nfs_serveur_restart
```

roles/nfs_client/vars/RedHat.yml

```
1 ---
2
3 nfs_client_paquet: nfs-utils
```

roles/nfs_client/vars/Debian.yml

```
1 ---
2
3 nfs_client_paquet: nfs-common
```

roles/nfs_client/tasks/main.yml

```
1 ---
2
3 - name: Inclusion des variables
4   ansible.builtin.include_vars: "{{ ansible_os_family }}.yml"
5
6 - name: Installation client NFS
7   ansible.builtin.package:
8     name: "{{ nfs_client_paquet }}"
9     state: present
10
11 - name: Configuration de /etc/fstab et montage du serveur NFS
12   ansible.posix.mount:
13     src: "{{ nfs_client_serveur }}:{{ nfs_client_chemin }}"
14     path: /mnt
15     fstype: nfs
16     state: mounted
```

Coulisses

hosts

```
1 [ovhcloud_controle]
2 d2-2-rbx-a-1      ansible_host=91.134.100.192      ovhcloud_stagiaire=1
3 d2-2-rbx-a-2      ansible_host=91.134.101.238      ovhcloud_stagiaire=2
4 d2-2-rbx-a-3      ansible_host=91.134.102.107      ovhcloud_stagiaire=3
5 d2-2-rbx-a-4      ansible_host=91.134.99.10        ovhcloud_stagiaire=4
6 d2-2-rbx-a-5      ansible_host=91.134.96.124       ovhcloud_stagiaire=5
7 d2-2-rbx-a-6      ansible_host=91.134.102.163      ovhcloud_stagiaire=6
8 d2-2-rbx-a-7      ansible_host=91.134.102.82       ovhcloud_stagiaire=7
9 d2-2-rbx-a-8      ansible_host=91.134.96.186       ovhcloud_stagiaire=8
10 d2-2-rbx-a-9      ansible_host=91.134.100.236      ovhcloud_stagiaire=9
11 d2-2-rbx-a-10     ansible_host=91.134.96.253       ovhcloud_stagiaire=10
12 d2-2-rbx-a-11     ansible_host=91.134.99.211       ovhcloud_stagiaire=11
13
14 [ovhcloud_victimtimes]
15 d2-2-rbx-a-12     ansible_host=91.134.99.25        ovhcloud_stagiaire=1
16 d2-2-rbx-a-13     ansible_host=91.134.97.140       ovhcloud_stagiaire=1
17 d2-2-rbx-a-14     ansible_host=91.134.97.203       ovhcloud_stagiaire=2
18 d2-2-rbx-a-15     ansible_host=91.134.101.211      ovhcloud_stagiaire=2
19 d2-2-rbx-a-16     ansible_host=91.134.96.206       ovhcloud_stagiaire=3
20 d2-2-rbx-a-17     ansible_host=91.134.98.248       ovhcloud_stagiaire=3
21 d2-2-rbx-a-18     ansible_host=91.134.103.159      ovhcloud_stagiaire=4
22 d2-2-rbx-a-19     ansible_host=91.134.102.123      ovhcloud_stagiaire=4
23 d2-2-rbx-a-20     ansible_host=91.134.97.211       ovhcloud_stagiaire=5
24 d2-2-rbx-a-21     ansible_host=91.134.100.196      ovhcloud_stagiaire=5
25 d2-2-rbx-a-22     ansible_host=91.134.98.83        ovhcloud_stagiaire=6
26 d2-2-rbx-a-23     ansible_host=91.134.100.182      ovhcloud_stagiaire=6
27 d2-2-rbx-a-24     ansible_host=91.134.98.72        ovhcloud_stagiaire=7
28 d2-2-rbx-a-25     ansible_host=91.134.101.163      ovhcloud_stagiaire=7
29 d2-2-rbx-a-26     ansible_host=91.134.98.73        ovhcloud_stagiaire=8
30 d2-2-rbx-a-27     ansible_host=91.134.99.117       ovhcloud_stagiaire=8
31 d2-2-rbx-a-28     ansible_host=91.134.96.107       ovhcloud_stagiaire=9
32 d2-2-rbx-a-29     ansible_host=91.134.101.109      ovhcloud_stagiaire=9
33 d2-2-rbx-a-30     ansible_host=91.134.98.125       ovhcloud_stagiaire=10
34 d2-2-rbx-a-31     ansible_host=91.134.97.240       ovhcloud_stagiaire=10
35 d2-2-rbx-a-32     ansible_host=91.134.72.168       ovhcloud_stagiaire=11
36 d2-2-rbx-a-33     ansible_host=91.134.96.17        ovhcloud_stagiaire=11
37
38 [ovhcloud:children]
39 ovhcloud_controle
40 ovhcloud_victimtimes
41
42 [ovhcloud:vars]
43 ansible_ssh_extra_args='-o StrictHostKeyChecking=accept-new'
44 ansible_ssh_private_key_file=/home/babafou/.ssh/id_ecdsa-ovh
45 ansible_user=rocky
```

ovhcloud.yml

```
1 ---
2
3 - name: Toutes les machines
4   hosts: ovhcloud
5   become: true
6   tasks:
7     - name: Authentification par mot de passe (EL8)
8       ansible.builtin.lineinfile:
9         path: /etc/ssh/sshd_config
10        line: PasswordAuthentication yes
11        regexp: ^PasswordAuthentication
12        when: ansible_os_family == 'RedHat' and
13              ansible_distribution_major_version == '8'
14        notify:
15          - ovhcloud_sshd_restart
16     - name: Authentification par mot de passe (EL9)
17       ansible.builtin.file:
18         path: /etc/ssh/sshd_config.d/50-cloud-init.conf
19         state: absent
20        when: ansible_os_family == 'RedHat' and
21              ansible_distribution_major_version == '9'
22        notify:
23          - ovhcloud_sshd_restart
24     - name: Fuseau horaire
25       community.general.timezone:
26         name: Europe/Paris
27        notify:
28          - ovhcloud_cron_{{ ansible_os_family }}
29     - name: Utilisateur formation
30       ansible.builtin.user:
31         name: formation
32         password: $6$1ZqdoMck$f9IVc0e4oKobabuEk8N4E0.2
33           moq0RZ8GEbLw0JNnD6ifRXxfx00QyWJmdWjbRIiirqNBrJNwwhBrz1KiTThcK1
34         # toto
35         uid: 1664
36         group: users
37         comment: 'stagiaire formation'
38         shell: /bin/bash
39     - name: ~formation/.ssh
40       ansible.builtin.file:
41         path: /home/formation/.ssh
42         state: directory
43         owner: formation
44         group: users
45         mode: '700'
46     - name: /etc/sudoers.d/formation
47       ansible.builtin.copy:
48         content: "formation    ALL = (root) NOPASSWD: ALL\n" # noqa: no-tabs
49         dest: /etc/sudoers.d/formation
50         owner: root
51         group: root
52         mode: '444'
```

```

52 # pas besoin de désactiver firewalld
53 handlers:
54   - name: Redémarrage de sshd
55     ansible.builtin.service:
56       name: sshd
57       state: restarted
58     listen: ovhcloud_sshd_restart
59   - name: Redémarrage de cron
60     ansible.builtin.service:
61       name: cron
62       state: restarted
63     listen: ovhcloud_cron_Debian
64   - name: Redémarrage de crond
65     ansible.builtin.service:
66       name: crond
67       state: restarted
68     listen: ovhcloud_cron_RedHat
69
70 - name: Machines de contrôle
71   hosts: ovhcloud_controle
72   become: true
73   tasks:
74     - name: EPEL
75       ansible.builtin.package:
76         name: epel-release
77         state: present
78       when: ansible_os_family == 'RedHat'
79     - name: PPA Ansible
80       ansible.builtin.apt_repository:
81         repo: ppa:ansible/ansible
82       when: ansible_distribution == 'Ubuntu'
83     - name: Installations
84       ansible.builtin.package:
85         name: [ ansible , nano , tree , vim ] # noqa: yamll[brackets] yamll[
86           commas]
87         state: present
88     - name: ~formation/.vimrc
89       ansible.builtin.copy:
90         content: "autocmd BufNewFile,BufRead *.yaml      set cursorcolumn\n" #
91         noqa: no-tabs
92         dest: /home/formation/.vimrc
93         owner: formation
94         group: users
95         mode: '644'
96     - name: ~formation/ansible.cfg
97       community.general.ini_file:
98         path: /home/formation/ansible.cfg
99         section: defaults
100         option: inventory
101         value: hosts
102         owner: formation
103         group: users
104         mode: '444'
105     - name: ~formation/ansible.cfg (suppression d'une ligne blanche)

```

```

104     ansible.builtin.lineinfile:
105         path: /home/formation/ansible.cfg
106         regexp: ^$
107         state: absent
108     - name: ~formation/hosts
109       ansible.builtin.template:
110         src: hosts.j2
111         dest: /home/formation/hosts
112         owner: formation
113         group: users
114         mode: '644'
115     - name: ~formation/.ssh/id_ed25519*
116       community.crypto.openssh_keypair:
117         path: /home/formation/.ssh/id_ed25519
118         type: ed25519
119         # passphrase: toto
120         owner: formation
121         group: users
122     - name: ~formation/.ssh/id_ed25519.pub
123       ansible.builtin.fetch:
124         src: /home/formation/.ssh/id_ed25519.pub
125         dest: /tmp/id_ed25519.pub-{{ ovhcloud_stagiaire }}
126         flat: true
127
128     - name: Machines à gérer
129       hosts: ovhcloud_victimtes
130       become: true
131       tasks:
132         - name: ~formation/.ssh/authorized_keys
133           ansible.builtin.copy:
134             src: /tmp/id_ed25519.pub-{{ ovhcloud_stagiaire }}
135             dest: /home/formation/.ssh/authorized_keys
136             owner: formation
137             group: users
138             mode: '600'

```

hosts.j2

```

1 [test]
2 {% for item in groups.ovhcloud_victimtes %}
3 {% if hostvars[item]['ovhcloud_stagiaire'] == ovhcloud_stagiaire %}
4 {{ hostvars[item]['inventory_hostname'] }}      ansible_host={{
5     hostvars[item]['ansible_host'] }}
6 {% endif %}
7 {% endfor %}
8
9 [test:vars]
10 ansible_ssh_extra_args='-o StrictHostKeyChecking=accept-new'

```