Installation de la stack ELK (Xenial/Ubuntu 16 LTS)

Structure des playbooks

Chaque playbook suit la structure suivante :

Squelette playbook Développer la source

```
XXX
├── defaults
|   └── XXX_options.yml
├── src
|   ├── file_conf_1
|   ├── file_conf_2
└── tasks
    └── XXX_logstash.yml
```

Le fichier *defaults/XXX_options.yml* contient toutes les variables (version, chemin, valeurs par défaut etc...) utilisées dans le ficher *tasks/install_XXX.yml.*

Le dossier *src* est optionnel : il contient d'éventuels fichiers de configuration.

Arborescence des playbooks pour ELK

Voici la structure complète pour l'installation de la stack ELK :

Arborescence des Playbooks d'installation d'une Stack ELK Développer la source

```
elk/
├── defaults
|   └── elk_options.yml
├── elasticsearch
|   ├── defaults
|   |   └── elasticsearch_options.yml
|   └── tasks
|       └── install_elasticsearch.yml
├── kibana
|   ├── defaults
|   |   └── kibana_options.yml
|   └── tasks
|       └── install_kibana.yml
├── logstash
|   ├── defaults
|   |   └── logstash_options.yml
|   ├── src
|   |   ├── 01-lumberjack-input.conf
|   |   ├── 10-syslog.conf
```

```
|   |   ├── 20-rsyslog.conf
|   |   ├── 30-output-stdout.conf
|   |   ├── ca.pem
|   |   ├── elk-cert.pem
|   |   └── elk-key.pem
|   └── tasks
|       └── install_logstash.yml
├── nginx
|   ├── defaults
|   |   └── nginx_options.yml
|   └── tasks
|       └── install_nginx.yml
└── tasks
    └── install_elk.yml
java/
└── install_java.yml
```

Dans notre cas le fichier elk/tasks/install_elk.yml est le playbook de déploiement "général". Il fait appel aux playbooks nécessaires à l'installation de la stack.

install_elk.yml Développer la source

```
---
- hosts: ELK
  remote_user: root
  tasks:
    - include_vars: '/home/administrateur/playbooks/elk/defaults/elk_options.yml'
    - include: '{{java_path}}/install_java.yml'
    - include: '{{elk_path}}/elasticsearch/tasks/install_elasticsearch.yml'
    - include: '{{elk_path}}/kibana/tasks/install_kibana.yml'
    - include: '{{elk_path}}/nginx/tasks/install_nginx.yml'
    - include: '{{elk_path}}/logstash/tasks/install_logstash.yml'

    - name: Install packages
      apt:
        name={{item.paquet}}
        update_cache=yes
        state=present
      with_items:
        - { paquet: "rsyslog-gnutls" }
        - { paquet: "gnutls-bin" }
        - { paquet: "aptitude" }
      tags: [ELK]

    - name: Upgrade packages
      apt: upgrade=yes
      tags: [ELK]
```

Attention c'est le seul fichier qui doit contenir les entêtes Ansible :

En-tête du playbook principal Développer la source

```
---
- hosts: ELK
  remote_user: root
  tasks:
    - include_vars: '/home/administrateur/playbooks/elk/defaults/elk_options.yml'
    - include: '{{java_path}}/install_java.yml'
    - include: '{{elk_path}}/elasticsearch/tasks/install_elasticsearch.yml'
    - include: '{{elk_path}}/kibana/tasks/install_kibana.yml'
    - include: '{{elk_path}}/nginx/tasks/install_nginx.yml'
    - include: '{{elk_path}}/logstash/tasks/install_logstash.yml'
```

Tous les fichiers *include* doivent commencer directement au niveau des *tasks*, comme suit :

Exemple playbook secondaire Développer la source

```
  - include_vars:
'/home/administrateur/playbooks/elk/nginx/defaults/nginx_options.yml'

  - name: Installation des paquets nginx
    apt:
      name=nginx
      state=present
      update_cache=true
    tags: [nginx]

  - name: Start Nginx on Boot
    service: name=nginx enabled=yes
    tags: [nginx]
  - name: Starting Nginx
    service: name=nginx state=started
    tags: [nginx]
```

Vous trouverez dans les pages annexes tous les *playbooks* nécessaires pour le déploiement d'une stack ELK.