

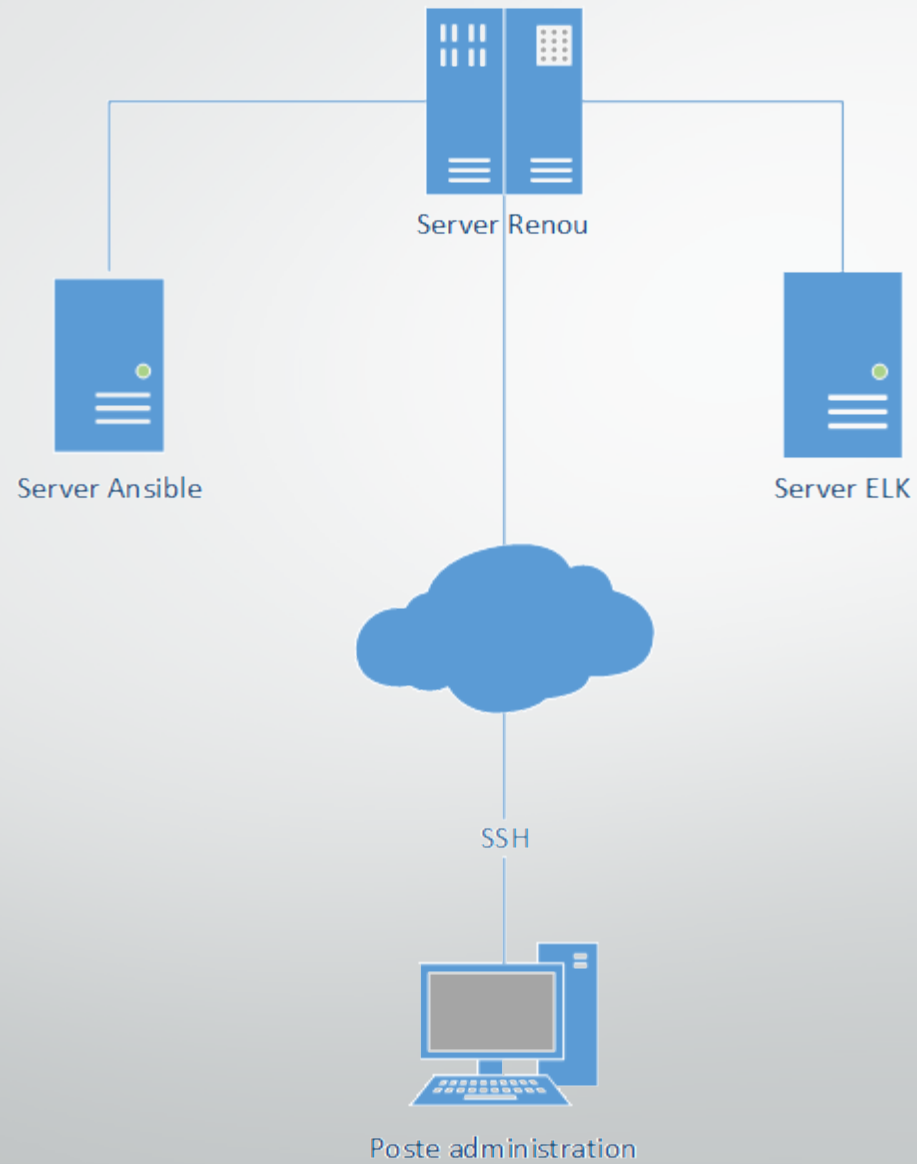


Ansible - ELK

Ansible - ELK

- Reminder
- Tree installation
- What is an ELK stack ?
- Demo
- Deliverable
- Blocking points
- GitHub

Topology



Reminder - Todo List

<i>Nom de tâche</i>	<i>ID</i>	<i>Début</i>	<i>Terminer</i>	<i>Durée</i>
Déploiement de la maquette	1	15/03/2016	18/03/2016	4j
Prise en main de Ansible	2	15/03/2016	02/05/2016	49j
Créations de playbook et déploiement sur les serveurs	3	02/05/2016	14/06/2016	44j
Déploiement manuel d'une stack ELK	4	15/05/2016	29/06/2016	46j
Etablissement de l'Ansible	5	15/05/2016	29/06/2016	46j

What is an ELK stack ?



Tree installation

```
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

15 directories, 18 files
```



DEMO

Deliverable

- Some documentations : Ansible & ELK
- Install playbooks
- Rsyslog conf files
- Logstash groks
- Templates exemples (nginx,syslog,apache,...)

Blocking point

- Standardisation of the received logs (grok)
- Sizing of the hardware
- Relevant kibana dashboard

GitHub

- Progression is available on our GitHub at this link
<https://github.com/Nodulaire/Ansible-ELK>