DevOps Sesión 14 (2022-03-28) Ansible + ELK

Documentación relacionada

> - ./5-Topic 705 Service Operations
> - ./5-Topic 705 Service Operations/MV-ELK formacion vmwareplayer.txt
> - ./5-Topic 705 Service Operations/Clase Monitorizacion.txt

inventario dinámico Ansible

> - ./4-Topic 704 Configuration Management/ec2_ansible-aws/Configurar inventario dinámico Ansible AWS.pdf
> - ./4-Topic 704 Configuration Management/ec2_ansible-aws/README.md
> - https://blog.mauriciovillagran.uy/2019/AnsibleDynamicInventory/

- ec2.py, ec2.ini (posiblemente deprecado, mejor usar el método del PDF)

Ansible + ESXi

> - Material Curso Ansible/Ansible-Vmware-vSphere

instalación VMWare Player + ELK

> - ./5-Topic 705 Service Operations/MV-ELK formacion vmwareplayer.txt
> - ./5-Topic 705 Service Operations/Material Curso ELK/1-Laboratorios ELK.pdf
> - ./5-Topic 705 Service Operations/Presentacion Herramientas para el manejo de logs.pdf
> - https://drive.google.com/drive/folders/1RdPXZfIRfjoOghbFYpw9ESlsNBpYacjQ

- root:000000
- `ip a` → (ens37) 172.16.132.128

Herramientas manejo logs

- kubernetes: prometheus + grafana
    - 1-Laboratorios ELK.pdf, pag. 90
    - 2-Despliegue de Aplicaciones Kubernetes/kubernetes-Helm3-API-Metrics-Server
        - servidor de métricas
        - helm: instalación software en k8s tipo apt

ELK

- ./5-Topic 705 Service Operations/Presentacion Herramientas para el manejo de logs.pdf, pág 11
- ElasticSearch: motor BDD clave=valor
    - puertos 9200,9300
- Logstash: pre-procesador de logs
    - puerto: 5044
- Beats: clientes ligeros que capturan los datos para ElasticSearch o Logstash
    - winlogbeats (pago?)
- Kibana: intérprete gráfico de los datos de ElasticSearch
    - puerto: 5601

instalación

```
yum install git -y
cd /
git clone https://github.com/agarciafer/elk.git
cd /root
rpm -ivh metricbeat-6.7.1-x86_64.rpm
rpm -ivh logstash-6.7.1.rpm
cp /elk/example.conf /etc/logstash
/usr/share/logstash/bin/logstash -f /etc/logstash/example.conf
rpm -ivh elasticsearch-6.7.1.rpm
rpm -ivh kibana-6.7.1-x86_64.rpm
```

; /etc/elasticsearch/elasticsearch.yml

```
   57 network.host: [ "localhost", "192.168.1.150" ]
```

```
systemctl start elasticsearch.service
systemctl status elasticsearch.service
systemctl enable elasticsearch.service

netstat -putan | grep -w 9200
netstat -putan | grep -w 9300
```

; /etc/kibana/kibana.yml

```
 7 server.host: "192.168.93.128" # dirección MV
28 elasticsearch.hosts: ["http://localhost:9200"]
```

```
systemctl start kibana.service
systemctl status kibana.service
systemctl enable kibana.service

netstat -putan | grep -w 5601
```

- http://192.168.93.128:5601/

beats

- 1-Laboratorios ELK.pdf, pag. 20

- ; /etc/metricbeat/metricbeat.yml

```
49 setup.dashboards.enabled: true
67   host: "192.168.93.128:5601"
144 xpack.monitoring.enabled: true
151 xpack.monitoring.elasticsearch:
```

- **/etc/metricbeat/modules.d**

- ```
  metricbeat modules list
  systemctl start metricbeat.service
  systemctl status metricbeat.service
  systemctl enable metricbeat.service
  tail -f /var/log/elasticsearch/elasticsearch.log # comprobar que metricbeat está enviando datos
  metricbeat test config -c /etc/metricbeat/metricbeat.yml
  ```

- En Kibana, activamos **Monitoring**
- vamos **Dashboard** y buscamos **[Metricbeat System] Overview**

habilitar módulo (docker)

- https://www.elastic.co/guide/en/beats/metricbeat/6.7/metricbeat-module-docker.html

- ```
  docker run -dtiP --name web-1 httpd
  docker run -dtiP --name web-2 nginx
  ```

- ```
  metricbeat modules enable docker
  ```

- ; /etc/metricbeat/modules.d/docker.yml

```
# Module: docker
# Docs:
https://www.elastic.co/guide/en/beats/metricbeat/6.7/metricbeat-module-docker.html

- module: docker
  metricsets:
    - container
```
```

```
    - cpu
    - diskio
    - event
    - healthcheck
    - info
    - memory
    - network
  period: 10s
  hosts: ["unix:///var/run/docker.sock"]

  # If set to true, replace dots in labels with `_`.
  labels.dedot: false

  # To connect to Docker over TLS you must specify a client and CA
certificate.
  #ssl:
    #certificate_authority: "/etc/pki/root/ca.pem"
    #certificate:           "/etc/pki/client/cert.pem"
    #key:                   "/etc/pki/client/cert.key"
```

- En Kibana, vamos a **Dashboard** y buscamos **[Metricbeat Docker] Overview**

TODO