*daniel sonora*

*Ansibles*

FILE BEAT

---

- name: Installing and Launch Filebeat

hosts: webservers

become: yes

tasks:

# Use command module

- name: Download filebeat .deb file

command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb

# Use command module

- name: Install filebeat .deb

command: dpkg -i filebeat-7.4.0-amd64.deb

# Use copy module

- name: Drop in filebeat.yml

copy:

src: /etc/ansible/files/filebeat-config.yml

dest: /etc/filebeat/filebeat.yml

# Use command module

- name: Enable and Configure System Module

command: filebeat modules enable system

# Use command module

- name: Setup filebeat

command: filebeat setup

# Use command module

- name: Start filebeat service

command: service filebeat start

# Use systemd module

- name: Enable service filebeat on boot

systemd:

name: filebeat

enabled: yes

METRIC BEAT

---

- name: Install metric beat

hosts: webservers

become: true

tasks:

# Use command module

- name: Download metricbeat

command: curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.4.0-amd64.deb

# Use command module

- name: install metricbeat

command: dpkg -i metricbeat-7.4.0-amd64.deb

# Use copy module

- name: drop in metricbeat config

copy:

src: /etc/ansible/files/metricbeat-config.yml

dest: /etc/metricbeat/metricbeat.yml

# Use command module

- name: enable and configure docker module for metric beat

command: metricbeat modules enable docker

# Use command module

- name: setup metric beat

command: metricbeat setup

# Use command module

- name: start metric beat

command: service metricbeat start

# Use systemd module

- name: Enable service metricbeat on boot

systemd:

name: metricbeat

enabled: yes

ELK

---

- name: Configure Elk VM with Docker

hosts: elk

remote\_user: azadmin

become: true

tasks:

# Use apt module

- name: Install docker.io

apt:

update\_cache: yes

name: docker.io

state: present

# Use apt module

- name: Install pip3

apt:

force\_apt\_get: yes

name: python3-pip

state: present

# Use pip module

- name: Install Docker python module

pip:

name: docker

state: present

# Use sysctl module

- name: Use more memory

sysctl:

name: vm.max\_map\_count

value: "262144"

state: present

reload: yes

# Use docker\_container module

- name: download and launch a docker elk container

docker\_container:

name: elk

image: sebp/elk:761

state: started

restart\_policy: always

published\_ports:

- 5601:5601

- 9200:9200

- 5044:5044

# Use systemd module

- name: Enable service docker on boot

systemd:

name: docker

enabled: yes