---

- 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

---

- 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

---

- 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

1. Permissions on /etc/shadow should allow only root read and write access.  
   * Command to inspect permissions:ls -l /etc/shadow
   * Command to set permissions (if needed):
2. Permissions on /etc/gshadow should allow only root read and write access.  
   * Command to inspect permissions:ls -l gshadow
   * Command to set permissions (if needed):
3. Permissions on /etc/group should allow root read and write access, and allow everyone else read access only.  
   * Command to inspect permissions:ls -l group
   * Command to set permissions (if needed):
4. Permissions on /etc/passwd should allow root read and write access, and allow everyone else read access only.  
   * Command to inspect permissions:ls -l passwd
   * Command to set permissions (if needed):

### **Step 2: Create User Accounts**

1. Add user accounts for sam, joe, amy, sara, and admin.  
   * Command to add each user account (include all five users):sudo adduser sam sudo adduser joe sudo adduser amy sudo adduser sara sudo adduser admin
2. Ensure that only the admin has general sudo access.  
   * Command to add admin to the sudo group: sudo usermod -aG sudo admin

### **Step 3: Create User Group and Collaborative Folder**

1. Add an engineers group to the system.  
   * Command to add group:sudo groupadd engineers
2. Add users sam, joe, amy, and sara to the managed group.  
   * Command to add users to engineers group (include all four users):sudo usermod -a -G engineers sam. sudo usermod -a -G engineers joe. Sudo usermod -a -G engineers amy. Sudo usermod -a -G engineers sara
3. Create a shared folder for this group at /home/engineers.  
   * Command to create the shared folder:sudo mkdir -p /home/engineers
4. Change ownership on the new engineers' shared folder to the engineers group.  
   * Command to change ownership of engineer's shared folder to engineer group:sudo chgrp -R engineers /home/engineers

### **Step 4: Lynis Auditing**

1. Command to install Lynis:suod apt install lynis
2. Command to see documentation and instructions:sudo lynis show version
3. Command to run an audit:sudo lynis audit system