Metricbeat YAML:

---

- 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

Filebeat Playbook:

---

- 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

SCRIPTS:

#!/bin/bash

mkdir ~/research 2> /dev/null

echo "A Quick System Audit Script" > ~/research/sys\_info.txt

date >> ~/research/sys\_info.txt

echo "" >> ~/research/sys\_info.txt

echo "Machine Type Info:" >> ~/research/sys\_info.txt

echo $MACHTYPE >> ~/research/sys\_info.txt

echo -e "Uname info: $(uname -a) \n" >> ~/research/sys\_info.txt

echo -e "Ip info: $(ip addr | grep inet |

tail -2 | head -1) \n" >> ~/research/sys\_info.txt

echo -e "Hostname: $(hostname -s) \n" >> ~/research/sys\_info.txt

echo "DNS Servers: " >> ~/research/sys\_info.txt

cat /etc/resolv.conf >> ~/research/sys\_info.txt

echo -e "\nMemory Info:" >> ~/research/sys\_info.txt

free >> ~/research/sys\_info.txt

echo -e "\nCPU Info:" >> ~/research/sys\_info.txt

lscpu | grep CPU >> ~/research/sys\_info.txt

echo -e "\nDisk Usage:" >> ~/research/sys\_info.txt

df -H | head -2 >> ~/research/sys\_info.txt

echo -e "\nWho is logged in: \n $(who -a) \n" >> ~/research/sys\_info.txt

find / -type f -perm /4000 >> ~/research/sys\_info.txt

echo -e "\nTop 10 Processes" >> ~/research/sys\_info.txt

ps aux -m | awk {'print $1, $2, $3, $4, $11'} | head >> ~/research/sys\_info.txt

25,1 Bot

#!/bin/bash

echo "A Quick System Audit Script"

1013

echo "Machine Type Info:"

echo $MACHTYPE

echo -e "uname info: $(uname -a) /n"

echo -e "IP Info: $(ip addr | head -9 | tail -1) /n"