Top of Form

Bottom of Form

Top of Form

Bottom of Form

|  |  |
| --- | --- |
|  | --- |
|  | - name: Install Filebeat and metribeat |
|  | hosts: webservers |
|  | remote\_user: redteamadmin |
|  | become: yes |
|  | tasks: |
|  | - name: Download filebeat package |
|  | command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.4.0-amd64.deb |
|  | - name: Install filebeat package |
|  | command: dpkg -i filebeat-7.4.0-amd64.deb |
|  | - name: Copy over filebeat configuration |
|  | copy: |
|  | src: /etc/ansible/files/filebeat-config.yml |
|  | dest: /etc/filebeat/filebeat.yml |
|  | mode: '0644' |
|  | - name: Enable and configure system module |
|  | command: filebeat modules enable system |
|  | - name: Setup filebeat |
|  | command: filebeat setup |
|  | - name: Start Filebeat service |
|  | command: service filebeat start |
|  |  |
|  | \*save and quit |
|  |  |
|  | You'll also need to download a config file as well that you can curl from this : https://www.elastic.co/guide/en/beats/filebeat/index.html |
|  | and put it in a new directory inside the ansible directory called files or whatever you want it, you know the drill here. |
|  |  |
|  | \*IMPORTANT NOTICE! Youll have to go inside this config playbook and manually change two things. ctl W to word search 'host' and change the ip addresses for the two of them so they match your elk machines ip or else it wont work |