Day 2 Activity File: Filebeat Installation

Now that we have our ELK monitoring server up installed and configured, we're going to add another tool called **Filebeat**.

Taking raw log files and trying to make sense of all the data is often difficult and time consuming. We can use Filebeat to collect, parse, and visualize ELK logs in a single command. This will help us better track our organizational goals.

By the end of class today, you should complete the following steps:

1. **Install Filebeat**. Verify your ELK server container is up and running, and install Filebeat on your Web-VM's so they send log files to the ELK server.
2. **Create the Filebeat configuration file**. Create and edit the Filebeat configuration file that you will copy into place using Ansible.
3. **Create the Filebeat installation play**. Create another Ansible playbook that accomplishes all the steps needed to install Filebeat.
4. **Verify the installation and playbook**. Confirm that your installation and playbook worked by verifying that the ELK stack is receiving logs.

Resources

Below are links to the Filebeat and Docker documentation. It is strongly suggested that you read through these before starting the activity:

- Filebeat Container Documentation
- Docker Commands Cheat Sheet

You can also use the following resources if you get stuck:

- Docker and Ansible Cloud Week Cheat Sheet
- Ansible Roles

Getting Started

Today, you will continue building up your ELK server. Specifically, if you have completed the installation step, you will proceed to install **Filebeat**.

- Recall that Filebeat helps generate and organize log files to send to Logstash and Elasticserver. Specifically, it logs information about the file system, including when and which files have changed.
- Filebeat is often used to collect log files from very specific files, such as logs generated by Apache, Microsoft Azure tools, the Nginx web server, or MySQl databases. Today you will be using it to monitor the Apache server and MySQL database logs generated by DVWA.

- Since Filebeat is built to collect data about specific files on remote machines, it must be installed on the VMs you want to monitor. You will install Filebeat on the DVWA container you created during the cloud security week. This will provide you with a rich source of logs after you complete your deployment.

Instructions

1. Installing Filebeat on the DVWA Container

First, make sure that the ELK server container is up and running:

- Navigate to http://[your.VM.IP]:5601/app/kibana. Use the public IP address of the ELK server that you created.
- Click 'Explore on my Own'
- If you do not see the Kibana server landing page, open a terminal on your computer and SSH into the ELK server.
    - Run `docker container list -a` to verify that the container is on.
    - If it isn't, run `docker start elk`.

Next, use the ELK server's GUI to begin installing Filebeat on your DVWA VM.

Navigate to your ELK server's IP address:

- Click **Add Log Data**.
- Choose **System Logs**.
- Click on the **DEB** tab under **Getting Started**.

Here you will find the most up-to-date Filebeat installation instructions for Linux.

- Note that you do not need to do anything on this page. Since Filebeat is open source, it is updated frequently. Therefore, specific details around installation can change. This site will always have the most up-to-date instructions.

2. Creating the Filebeat Configuration File

Next, we will create a Filebeat configuration file, after which we will create the Ansible playbook file.

At that point, we will translate the instructions in the DEB tab into a new Ansible play, which you will use to automatically install Filebeat on your DVWA machines.

- Translating installation instructions to reusable playbooks is a common task for modern infrastructure teams. Being able to explain the value of this task and the plays you've created will be valuable in job interviews.
- Creating this play will allow you to easily install Filebeat on any machine you want to monitor later, whether for class, work, or a personal project.

Open a terminal and SSH into your jump box:

- Start the Ansible container.
- Use the correct Docker command to attach to your Ansible container.

As mentioned earlier, the Filebeat installation instructions require you to create a Filebeat configuration file.

- You will need to edit this file so that it has the correct settings to work with your ELK server.

You can use the provided template for the Filebeat configuration file: Filebeat Configuration File Template.

- Note that when text is copy and pasted from the web into your terminal, formatting differences are likely to occur that will corrupt this configuration file.
- Using `curl` is a better way to avoid errors and we have the file hosted for public download HERE
- Run: `curl https://gist.githubusercontent.com/slape/5cc350109583af6cbe577bbcc0710c93/raw/eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat > /etc/ansible/files/filebeat-config.yml`

```
root@6160a9be360e:/etc/ansible# curl https://gist.githubusercontent.com/
slape/5cc350109583af6cbe577bbcc0710c93/raw/
eca603b72586fbe148c11f9c87bf96a63cb25760/Filebeat > filebeat-config.yml
 % Total    % Received % Xferd  Average Speed   Time    Time     Time
Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 73112  100 73112    0     0   964k      0 --:--:-- --:--:-- --:--:--
964k
```

Once you have this file on your Ansible container, edit this file as specified in the Filebeat instructions (the specific steps are also detailed below).

- The username is `elastic` and the password is `changeme`.
- Scroll to line #1106 and replace the IP address with the IP address of your ELK machine.
- `output.elasticsearch:`
- `hosts: ["10.1.0.4:9200"]`
- `username: "elastic"`
  `password: "changeme"`
- Scroll to line #1806 and replace the IP address with the IP address of your ELK machine.
- `setup.kibana:`
- `host: "10.1.0.4:5601"`
- Note that the default credentials are `elastic:changeme` and should not be changed at this step.
- Save this file in `/etc/ansible/files/filebeat-config.yml`.

3. Creating the Filebeat Installation Play

Next, create a new playbook that installs Filebeat and then copies the Filebeat configuration file you just made to the correct location.

- On the Ansible VM, create a playbook file, `filebeat-playbook.yml`.
    - Locate this file in your `/etc/ansible/roles/` directory.
- Open your playbook and implement the following tasks:
    - Download the `.deb` file from artifacts.elastic.co.
    - Install the `.deb` file using the `dpkg` command shown below:
        - `dpkg -i filebeat-7.4.0-amd64.deb`
    - Copy the Filebeat configuration file from your Ansible container to your WebVM's where you just installed Filebeat. Make sure it is copied to: `/etc/filebeat/filebeat.yml`
        - Use Ansible's `copy` module to copy the entire configuration file to the correct place.
    - Run the following commands:
        - `filebeat modules enable system`
        - `filebeat setup`
        - `filebeat -e`

You may find the following hints and links helpful:

- This play should only run on the web machines that are running the DVWA containers.
- Refer to the Ansible playbook documentation if needed.
- Use the Ansible `copy` module to move `filebeat-config.yml` onto the Web VMs.
- You can use the `command` module to run `curl`, `dpkg`, and Filebeat commands.
    - Use `curl -O` or `curl -o` to download the `dpkg` file.

Note: You can use the following template for configuring the Filebeat playbook: Filebeat Playbook Template. You can also build your own if you'd like an additional challenge.

After you create and save this file, run it to install Filebeat on the DVWA machines.

4. Verifying Installation and Playbook

After the playbook completes, follow the steps below to confirm that the ELK stack is receiving logs from your DVWA machines:

- Navigate back to the Filebeat installation page on the ELK server GUI.
- On the same page, scroll to **Step 5: Module Status** and click **Check Data**.
- Scroll to the bottom of the page and click **Verify Incoming Data**.

If your installation was successful, take a screenshot of what you see before proceeding.

Day 2 Milestone

If your ELK server is receiving logs, congratulations! You've successfully deployed a live, functional ELK stack and now have plays that can:

- Install and launch Docker containers on a host machine.
- Configure and deploy an ELK server.
- Install Filebeat on any Debian-flavored Linux server.

Even more significant is that you've done all of this through automation with Ansible. Now you can recreate exactly the same setup in minutes.

If you have time, create a play to install Metricbeat. After this, you'll have programmed plays to automatically install 25% of the most common Beats.

Bonus: Creating a Play to Install Metricbeat

Note that there are fewer instructions and setup files provided here. However, the process is similar to the one used for the Filebeat installation.

Navigate to your ELK server's IP.

- Click **Add Metric Data**.
- Click **Docker Metrics**.
- Click the **DEB** tab under **Getting Started** for the correct Linux instructions.

Return to your Ansible VM. Update your playbook with tasks that perform the following:

- Download the Metricbeat `.deb` file.
- Use `dpkg` to install the `.deb` file.
- Update and copy the provided Metricbeat config file.
- Run the `metricbeat modules enable docker` command.
- Run the `metricbeat setup` command.
- Run the `metricbeat -e` command.

Verify that your play works as expected:

- On the Metricbeat Installation Page in the ELK server GUI, scroll to **Step 5: Module Status** and click **Check Data**.

If your installation was successful, take a screenshot of what you see before proceeding.

Troubleshooting and Common ELK Container Issues:

Common Issue: When the ELK VM is restarted, the container doesn't restart automatically, ELK doesn't run and logs are not transferred.

Check the following:

- Make sure you have the 'restart_policy' set correctly in the Ansible playbook:

```
restart_policy: always
```

- Make sure you have the `vm_map_max` setting in the Ansible playbook:

```
  # Use command module
- name: Increase virtual memory
  command: sysctl -w vm.max_map_count=262144

  # Use shell module
- name: Increase virtual memory on restart
  shell: echo "vm.max_map_count=262144" >> /etc/sysctl.conf
```