Cloud Computing Applications and Services

Monitoring

November 29, 2021

The main goal of this guide is to deploy and use a modular system monitoring tool. The following components will be installed:

- `https://www.elastic.co/downloads/beats/metricbeat`
- `https://www.elastic.co/downloads/elasticsearch`
- `https://www.elastic.co/downloads/kibana`

Steps

1. Create three VMs (VM1, VM2, and VM3). VM1 should have at least 2GB of RAM.
   (a Vagrant file is provided along with this guide if you want to use it).
2. At VM1:
   (a) Download and unpack Elasticsearch (LINUX X86_64 - tar.gz).
   (Explore commands `wget` and `tar`).
   (b) Configure Elasticsearch (config/elasticsearch.yml):
   (note that `VM1_IP` needs to be changed with the VM's ip)
   ```
   network.host: VM1_IP
   discovery.seed_hosts: []
   cluster.initial_master_nodes: ["VM1_IP"]
   ```
   (c) Start the server (`./bin/elasticsearch` - Java is required)
   (d) Increase VM map count if required
   ```
   sudo sysctl -w vm.max_map_count=262144
   ```
   (e) Download and unpack Kibana (LINUX 64-BIT - tar.gz).
   (Explore commands `wget` and `tar`).
   (f) Configure Kibana bind address (config/kibana.yml)
   ```
   server.host: VM1_IP
   elasticsearch.hosts: ["http://VM1_IP:9200"]
   ```
   (g) Start the server (`./bin/kibana`)
3. At VM2 and VM3:
   (a) Download and unpack Metricbeat (LINUX 64-BIT - tar.gz).
   (Explore commands `wget` and `tar`).
   (b) Define Elasticsearch and Kibana addresses to point to VM1 (metricbeat.yml)
   setup.kibana→hosts and output.elasticsearch→hosts configurations.
   (c) Check available modules with: `./metricbeat modules list`
   (d) Install indexes and dashboards with: `./metricbeat setup`
   (e) Start the daemon with `./metricbeat -e`

4. Open Kibana at `http://VM1_IP:5601`
5. Observe summarized data in the Analytics→Dashboard page
   (e.g., [Metricbeat System] overview ECS)
6. Explore the other menus from Kibana.

Extra

1. Install Swap at VM2 and VM3 (guide 2 – *Provisioning and Deployment*).
   Explore ELK for monitoring and checking the resources used by Swap components.
2. Include the steps for installing and provisioning the ELK stack into your Ansible playbook (guide 2 – *Provisioning and Deployment*)
3. Add Packetbeat and Filebeat from
   `https://www.elastic.co/products/beats`
4. Add persistent store and forwarding with Logstash (in another VM)
   `https://www.elastic.co/products/logstash`

Learning Outcomes Recognize different roles in a modular monitoring pipeline. Apply the ELK stack to monitor a distributed system.