Monitoring

System Deployment & Benchmarking

2020/2021

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. In a Virtual Machine (VM1):

   - This VM should have at least 2GB of RAM
   - Download and unpack Elasticsearch (LINUX X86_64 - tar.gz)
   - Configure Elasticsearch (config/elasticsearch.yml):
     - network.host: 0.0.0.0
     - discovery.seed_hosts: []
     - cluster.initial_master_nodes: [”VM1_ip”]
   - Start the server (./bin/elasticsearch - Java is required)
   - Increase VM map count if required
     - sudo sysctl -w vm.max_map_count=262144
   - Download and unpack Kibana (LINUX 64-BIT - tar.gz)
   - Configure Kibana bind address (config/kibana.yml)
     - server.host: 0.0.0.0
   - Start the server (./bin/kibana)

2. In another Virtual Machine (VM2):

   - Download and unpack Metricbeat (LINUX 64-BIT - tar.gz)
   - Define Elasticsearch and Kibana addresses to point to VM1 (metricbeat.yml)
   - Check available modules with: `metricbeat modules list`
   - Install indexes and dashboards with: `metricbeat setup`
   - Start the daemon with `metricbeat -e`

3. Open Kibana at `http://"VM1_ip":5601`

4. Observe individual events in Discover page (e.g., system.cpu.iowait.pct, system.memory.actual.free)

5. Observe summarized data in the Dashboard page (Host overview ECS).

Extra

1. Add Packetbeat, Heartbeat, and Filebeat from `https://www.elastic.co/products/beats`
2. Add persistent store and forwarding with Logstash (in another VM) `https://www.elastic.co/products/logstash`
3. Add beats in more than one server.

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