MANAGED SERVICE FOR LOGS

Akshay Shetty
Sai Rakesh Ghanta
Sucheta Chatterjee
Sangeetha P H

Solution

- ELK [ElasticSearch, Logstash, Kibana] stack provides an efficient way to collect, manage and visualize system and application logs .
- Linux Containers provide an efficient way to deploy applications and provide isolation and security .
- We are providing a solution of hosting ELK Stack on Linux Containers and deploy the container as an application on server and clients

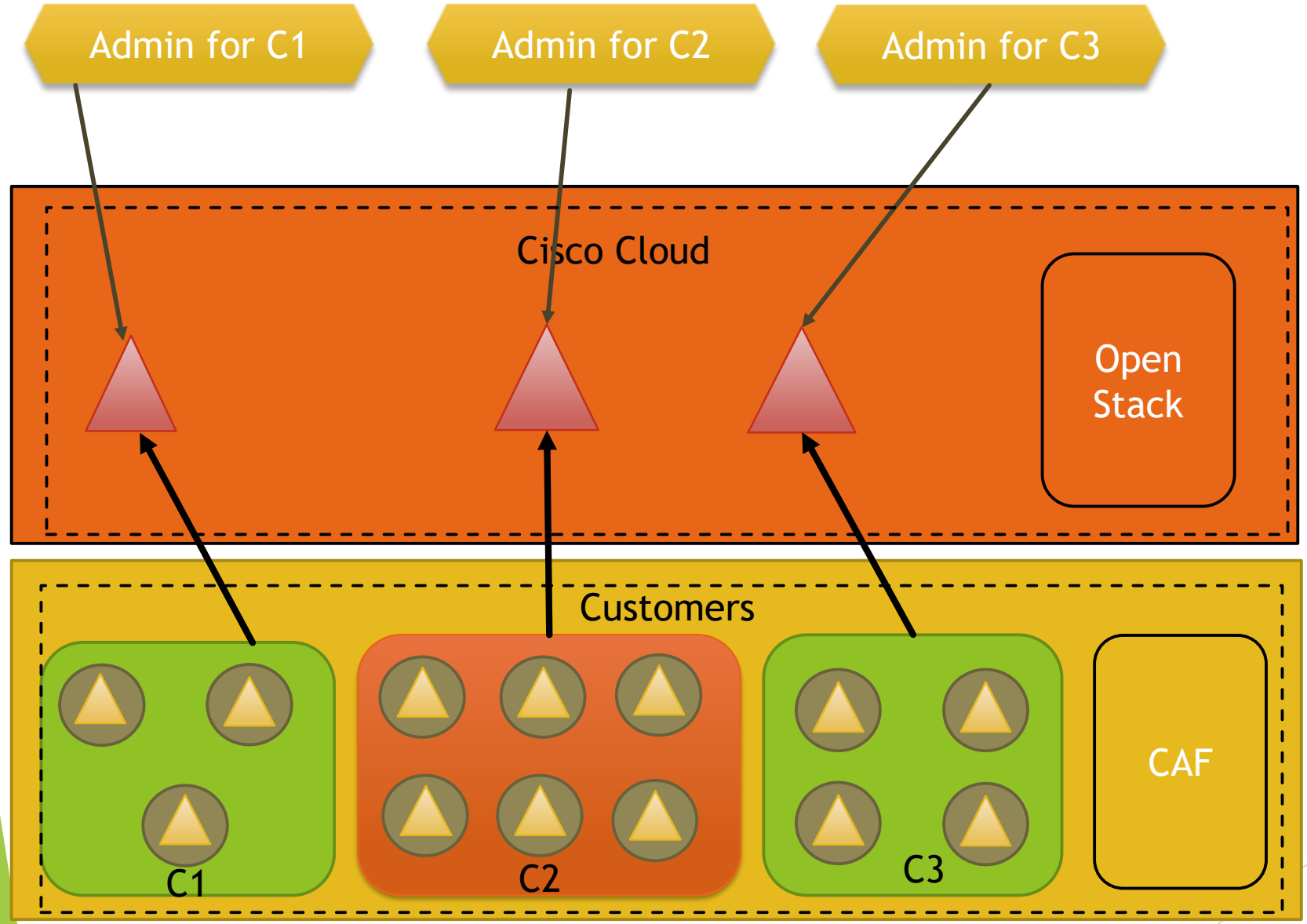
Problem Statement

- Customers face router issues on a daily basis
- Managing large number of routers becomes a hectic job
- Customers need a good log management system to keep track of issues with the routers and take actions based on those logs
- Cisco can help customers by providing them a platform from where they can centrally manage the logs of their routers and pay on subscription basis

Advantages

- ELK Stack is an open source technology and is currently very popular in the IT industry.
- Linux Containers are the next step in virtualization helping to deploy applications on cloud .
- Linux Containers provide the **required isolation and security** to help Cisco provide this solution to multiple customers .
- Customers can pay on subscription as and when they need the tool.

Purposed Model Overview



Container with ELK Server Application

Container with ELK Client Application

Router/Client

Server

System Admin from Customer side who will use the management service

CAF

Cisco Application Interface

Use Cases

- Customer C1 faces issues on its routers at a certain time of the day for a month . They will need to monitor those routers during that time to see the issues. They can enable the ELK log collection on the routers . At the same time , they will request a server(ELK container) from Cisco to store the collected data. The Customer C1 will be provided access to this server to search and visualize the logs. Once they are done with the server , they can request for stopping the service and then pay only for the time they used the servers. Cisco can provide these services to many customers at the same time leveraging on the **security and isolation** provide by the Linux Containers .

- Cisco Internal Testing Team can use this to find out the bugs on the routers . The servers (containers) can be started , froze and stopped whenever the requirement arises . This will help in efficient resource utilization on the main server hosting the containers.

Further Info

- This is an idea that needs further tuning and thinking.
- There are lots of alternatives to ELK Stack like Splunk. The choice of application can be decided based on merits and cost
- Containers are popular in recent times. Docker , Virtual Appliances and other virtualization techniques can be used as alternatives.
- This solution can be classified as a combination of SaaS [Software as a Solution] and PaaS [Platform as a Solution]
- Contact Us
  - Akshay Shetty – akshashe@cisco.com
  - Sai Rakesh Ghanta – sairghan@cisco.com
  - Sucheta Chatterjee – suchecha@cisco.com
  - Sangeetha P H - saph@cisco.com

References

- ELK Stack : http://blog.qbox.io/welcome-to-the-elk-stack-elasticsearch-logstash-kibana
- LXC : https://www.stgraber.org/2013/12/20/lxc-1-0-blog-post-series/
- ELK Stack on LXC : http://technologyconversations.com/2015/05/18/centralized-system-and-docker-logging-with-elk-stack/