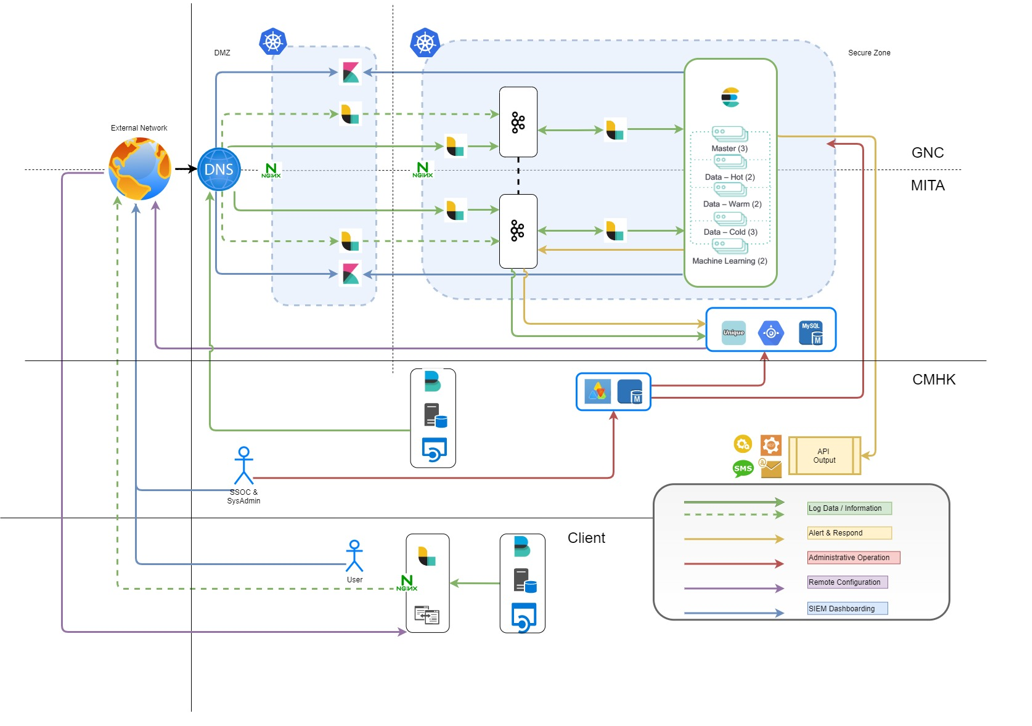
SIEM-K8S 部署文档

1. 架构设计



1. 资源申请



1. 网络打通

思路：

1. 由堡垒机CBH 通过Ansible & Kubectl 统一对K8S-DMZ & K8S SZ 集群进行控制，因此需要打通CBH 到 K8S-DMZ & K8S SZ 所有节点IP，端口为：icmp, 22, 6443,2379
2. 时间同步：GNC-DMZ-K8S-Master-0001 & MIT-DMZ-K8S-Master与集群外部NTP服务器10.250.16.130 & 10.250.0.130进行同步，并作为集群内部NTP服务器为集群内部所有节点提供时间同步服务。端口为123

配置文件 /etc/ntp.conf

Ntp服务 systemctl start ntp

1. Nginx提供LB服务，实现K8S高可用，需要SZ & DMZ集群节点打通6443 & 16443端口
2. 为方便SZ集群节点部署需要的软件，需要打通与Porxy之间网络（10.250.94.98）端口3128
3. 业务数据，需要SZ ELB SN Traffic IP & DMZ集群节点SN Traffic IP打通
4. 路由配置

\*路由配置服务：netplan

\*配置文件：/etc/netplan/50-cloud-init.yaml

DMZ GNC Master

DMZ MIT Master

SZ GNC Master

SZ GNC Worker

1. 堡垒机Ansible安装

apt-get install software-properties-common

apt-add-repository ppa:ansible/ansible

apt-get update

apt-get install ansible

\*配置文件: /etc/ansible/host

ssh 免密登录：

ssh-keygen

ssh-copy-id -i ~/.ssh/id\_rsa.pub root@<node-name>

ansible <group-name> -m script –a “xxxx.sh”

1. Hostname配置

ansible <group> -m script -a “xxxx.sh”

1. 服务器NTP配置

\*配置文件

/etc/ntp.conf

/run/ntp.conf.dhcp

1. 服务器环境初始化
2. K8S集群初始化
3. 开机脚本编写（解决Weave问题）
4. 工作节点添加Label & Taint标签