hostnamectl set-hostname —

Subject
Date

fluentd

/home/siem/nxlog

↳ docker-compose

restart: always

---

docker logs -f fluentd_log --tail 1.

---

ifconfig -a ip a

/etc/net-plan/

db: /etc/fstab umount /home/siem

↳ /dev/sdb /home/siem/ ext4 def 0 1

/dev/sdc /mnt/fast-ssd/ ext4 def 0 1

mount -a

mkfs -t ext4 /dev/sdb

ifconfig ens192 up

ifconfig ens192 promisc

du -hd 1 /var →

docker logs -f -t --tail 1.

make load
make config → db
make up → all
make install

docker exec -it ch1 bash
clickhouse-client
use Default
show tables
drop table ...

web backend → db
config.conf
ip → ip main
final = 1

click-h-backup create
restore → db

cron: docker restart scheduke

/home/siem/database Data/ch1/data
/backup → ...
/mnt/siem/backup/ssd
hdd

main: ens19: 192.168.0.101
db: 192.168.0.100
nqla: 0.99

ip: ens 19

sagjad.conf →

/home/sien/nfla/logmgm/log

1.log 1.pos 777 →chmod

g/etc/rsyslog.d/sagjad.conf

if fromhost_ip = "..." then /...

crontab → docker volume prune -f

cron tab nfla

1 */5 * * * rm -f /var/lg/zeek

/*.log , ... /zeekflg/224*

docker rm -f

{ nfla: kafka-... , 200...

main: sigma2SQL, ksqldb server

docker-compose up -d ,

Subject

Date

/etc/netplan/00-install

network:
  ethernets:
    eth0:
      dhcp: false
      addresses:
        - 172.26.137.110/24
      routes:
        - to: 0.0.0.0/0
          via: 172.26.128.1
      nameservers:
        addresses: [ff,ip]
  version: 2

→ netplan apply

routes:
  - to: default
    via: 3f_gateway

DATE ۱۴۰۳/۰۶/۱۷ SUBJECT: "اتصال لاگ دیتک ها روی سیم NTLA"

```
tcpdump -i ens160 -n port 514 | grep LocalZ

#docker restart rsyslog
#docker restart fluentd_log
```

/home/siem/ntla/rsyslog/ در این مسیر تمام تنظیمات conf لاگ و لاگ های خام وارد

/home/siem/ntla/fluentd.log/ محل ذخیره سازی فایل های لاگ fluentd (پارس ها)

```
#docker logs fluentd_core --tail 10
```

اگر لاگ پارس شود و در DB ذخیره شود با فرمت لاگ ماژول core می توان Import شدن در جداول db را مشاهده کنیم.

```
#docker logs fluentd_log --tail 10
```

اگر لاگ پارس نشود دستور بالا می توان بررسی کرد.

---

ابتدا فایل مورد نظر محتوایش را پاک کنید `echo "" > /home/siem/ntla/rsyslog/paloalto.log`

پس سرویس یا داکر rsyslog ریست شود

اکنون اگر فایل لاگ مورد نظر گیر شد آنگاه داکر fluentd/log ریست شود

در هر صورت بعد از ۳۰۰۰ ثانیه دوتا تیک را نباید سبز شود تا در بخش جداول لاگ مربوطه را ببینید.

چرا اگر لاگ در جدول مورد نظر دیده نشود؟!

/home/regex.log ← محتوا: img → باید کپی شود

: docker_compose → پورت 8...:8...

ابتدا img باید build شود سپس

docker-compose up ← IP سرور گیرنده : 8...

در فایل fluentd مربوطه در بخش exception باید regex اصلاح شده را جایگزین کنیم.

و سپس log را restart نماییم.

محل فایل fluentd → /home/siem/ntla/fluentd_log/etc/config/sw.conf

حرمت regex.log

Sahand

* /home/siamntta/fluentd_core/etc/generate.py

List=["conn", "dns", ... , "sw"] ← داخل فایل بالا (اضافه شود)

* /fluentd_core/etc/

# python3 generate.py ↵

# docker restart fluend_core ↵

/home/siammtta/fluentd_core/etc/generate.py

list=["conn", "dns", ..., "sw"] ← داخل فایل بالا

/fluentd_core/etc/
# python3 generate.py
# docker restart fluentd_core

monitor session 1 source interface gigabitethernet 0/1-11
monitor session 1 destination ... 0/12

mirror

configure terminal
logging on
logging IP ...
logging facility local7
logging trap
debugging

سرور سیسکو

Saband

/etc/rsyslog/rsyslog.conf
auth, authpriv.* @IP:514

سیسکو