Sessão 5: Registro e correlacionamento de eventos

1) Criação da máquina

Clonar `debian-template` para `log`, IP 10.0.42.4/24. Alterar *hostname* e realizar integração LDAP/SSH-CA como usual.

Criar entrada para o novo *host* no DNS (não esqueça de aumentar o serial), assinar zona e reiniciar *daemons*. Testar.

```
# hostname ; whoami
fw
root
```

```
# grep log /etc/nsd/intnet.zone
log     IN    A                 10.0.42.4
```

```
# grep log /etc/nsd/10.0.42.zone
4       IN   PTR                log.intnet.
```

```
# bash /etc/nsd/signzone-intnet.sh
reconfig start, read /etc/nsd/nsd.conf
ok
ok
ok
```

```
# systemctl reload unbound
```

```
# nslookup log
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name:   log.intnet
Address: 10.0.42.4
```

2) Configuração do NTP

Logar como `root` na máquina `log`. Instalar o OpenNTPD.

```
# hostname ; whoami
log
root
```

```
# apt-get install openntpd
```

Fazer o backup do arquivo original e configurar o OpenNTPD.

```
# mv /etc/openntpd/ntpd.conf /etc/openntpd/ntpd.conf.orig
```

```
# cat /etc/openntpd/ntpd.conf
listen on 127.0.0.1
listen on 10.0.42.4
servers pool.ntp.br
```

Pare o OpenNTPD, sincronize o relógio imediatamente.

```
# systemctl stop openntpd.service
```

```
# mkdir /var/run/openntpd ; ntpd -s -d -f /etc/openntpd/ntpd.conf -p
/var/run/openntpd.pid
adjtimex returns frequency of 0.000000ppm
/var/lib/openntpd/db/ntpd.drift is empty
listening on 127.0.0.1
listening on 10.0.42.4
ntp engine ready
reply from 200.160.7.186: offset -0.003035 delay 0.018363, next query 8s
set local clock to Sat Nov  3 17:25:41 -03 2018 (offset -0.003035s)
reply from 200.160.7.193: offset -0.003952 delay 0.019983, next query 5s
reply from 200.160.0.8: offset -0.003851 delay 0.020152, next query 7s
reply from 200.186.125.195: offset -0.002323 delay 0.023158, next query 7s
reply from 200.20.186.76: offset -0.003652 delay 0.027538, next query 6s
```

Após a sincronização, pare o processo com `CTRL + C`, apague o diretório `/var/run/openntpd` e inicie o OpenNTPD. Cheque se está escutando como esperado.

```
^C ntp engine exiting
Terminating
dispatch_imsg in main: pipe closed
```

```
# rmdir /var/run/openntpd
```

```
# systemctl start openntpd.service
```

```
# ss -unlp | grep 123
UNCONN     0      0      10.0.42.4:123                    *:*
users:(("ntpd",pid=1643,fd=8))
UNCONN     0      0      127.0.0.1:123                    *:*
users:(("ntpd",pid=1643,fd=7))
```

Configurar todos os servidores de uma única vez: como `han@client`, crie o *script* `/home/han/scripts/install-openntpd.sh` com o seguinte conteúdo:

```
1 #!/bin/bash
2
3 # instalacao
4 DEBIAN_FRONTEND=noninteractive apt-get -yq install openntpd
5
6 # configuracao
7 mv /etc/openntpd/ntpd.conf /etc/openntpd/ntpd.conf.orig
8 echo "server 10.0.42.4" > /etc/openntpd/ntpd.conf
9
10 # reiniciar ntpd
11 systemctl restart openntpd.service
```

Executar com:

```
$ for server in fw ldap nfs; do scp ~/scripts/install-openntpd.sh ${server}:~ && ssh
han@${server} 'echo seg10han | sudo -S bash /home/han/install-openntpd.sh' && ssh
${server} rm ~/install-openntpd.sh; done
```

Verifique a correta instalação:

```
$ echo '---'; for server in fw ldap nfs; do ssh han@${server} 'hostname ; dpkg -l |
grep openntpd ; cat /etc/openntpd/ntpd.conf; ps auxwm | pgrep ntpd'; echo '---'; done
---
fw
ii  openntpd                       1:6.0p1-2                      amd64        OpenBSD
NTP daemon
server 10.0.42.4
4950
4954
4956
---
ldap
ii  openntpd                       1:6.0p1-2                      amd64        OpenBSD
NTP daemon
server 10.0.42.4
1354
1364
1366
---
nfs
ii  openntpd                       1:6.0p1-2                      amd64        OpenBSD
NTP daemon
server 10.0.42.4
5192
5193
5194
---
```

7) Registro de comandos digitados com SnoopyLog

Syslog centralizado Criptografia no envio via stunnel (ou outro) Graylog