TP 2 Compte rendu Fabien Mauhourat

Gestion des logs :

1) Rsylog

apt install rsyslog/apk add rsyslog
rc-update add rsyslog

rsyslogd -N1 → check de la configuration

Configuration du serveur rsyslog :

vim /etc/rsyslog.conf :

```
$ModLoad imudp
$UDPServerRun 514
$ModLoad imtcp
$InputTCPServerRun 514

$template RemoteLogs,"/var/log/%HOSTNAME%/%PROGRAMNAME%.log"

if $hostname<>"debian-tp2" then {
        *.* ?RemoteLogs
        stop
}
```

Configuration des clients rsyslog :

vim /etc/rsyslog.conf :

```
if $programname=="sudo" and re_match($msg,"pam_unix.*(failure|failed|not identify)")
or re_match($msg,'.*: [0-9]* incorrect password [a-z]* ;') then {
      /var/log/err.log
      @@172.18.10.10
      stop
}
```

```
if $programname==["sshd","login","su"] and $msg contains("failed") or $msg
contains("not allowed") or $msg contains("invalid") or $msg contains("failure") or $msg
contains("Failed") or $msg contains("FAILED") or $msg contains("not identify") then {
        /var/log/err.log
        @@172.18.10.10
        stop
}

if $programname==["sshd","su","login","sudo"]  then     /var/log/ok.log
```

2) Syslog-ng

yum install epel-release && yum install syslog-ng

syslog-ng -s → check de la configuration

Configuration du serveur syslog :

Modification du fichier hosts pour la résolution de nom dans syslog vim /etc/hosts :

```
127.0.1.1       debian-tp2
172.18.10.12    centos-tp2
172.18.10.11    alpine-tp2
```

vim /etc/syslog-ng/syslog-ng.conf :

```
options {
   use-dns(persist_only);
   dns-cache-hosts(/etc/hosts);
};

source s_net {
        syslog(
        ip("172.18.10.10")
        transport("udp")
        port(514)
        );
};
destination d_net { file("/var/log/$HOST/$PROGRAM.log" create-dirs(yes)); };
log { source(s_net); destination(d_net); };
```

Configuration des clients rsyslog :

Modification de la facility du serveur ssh vim /etc/ssh/sshd_config :

SyslogFacility AUTHPRIV

vim /etc/syslog-ng/syslog-ng.conf :

```
destination d_error {
	file("/var/log/err.log");
	syslog(
	"172.18.10.10"
	port(514)
	transport("udp")
	);
};
destination d_ok { file("/var/log/ok.log"); };

filter f_error_sudo { facility(authpriv) and program(sudo) and
(message("pam_unix.*(failure|failed|not identify)") or message(".*: [0-9]* incorrect
password [a-z]* ;")); };
filter f_ok_sudo { facility(authpriv) and program(sudo) and not
(message("pam_unix.*(failure|failed|not identify)") or not message(".*: [0-9]* incorrect
password [a-z]* ;")); };
filter f_error { facility(authpriv) and (program(sshd) or program(login) or program(su))
and (message("failed") or message("not allowed") or message("invalid") or
message("failure") or message("FAILED") or message("Failed") or message("not
identify")); };
filter f_ok { facility(authpriv) and (program(sshd) or program(login) or program(su)) and
not (message("failed") or message("not allowed") or message("invalid") or
message("failure") or message("FAILED") or message("Failed") or message("not
identify")); };

log { source(s_sys); filter(f_error); destination(d_error); };
log { source(s_sys); filter(f_error_sudo); destination(d_error); };
log { source(s_sys); filter(f_ok); destination(d_ok); };
log { source(s_sys); filter(f_ok_sudo); destination(d_ok); };
```

Supervision :

Installation debian :

vim /etc/apt/sources.list
deb http://deb.debian.org/debian buster main contrib non-free
deb http://security.debian.org/debian-security buster/updates main contrib non-free

apt install snmp snmpd snmp-mibs-downloader
download-mibs
systemctl enable snmpd && systemctl start snmpd

vim /etc/snmp/snmpd.conf :

agentAddress udp:172.18.10.10:161
rocommunity secret 172.18.10.0/24

sysLocation Reims
sysContact admin <tp@reims.com>

disk / 10000

exec listpaquet /usr/bin/dpkg -l
exec userloggedon /userlogged.sh
exec rmlog /bin/rm /var/log/ok.log

Installation centos :

yum install net-snmp net-snmp-utils

systemctl enable snmpd && systemctl start snmpd

vim /etc/snmp/snmpd.conf :

com2sec mynetwork 172.18.10.0/24 secret
group RWGroup v2c mynetwork
view all included .1 80
access MyRWGroup "" any noauth 0 all all all

syslocation Reims
syscontact admin <tp@reims.com>

disk / 10000

exec listpaquet /usr/bin/rpm -qa
exec userloggedon /userlogged.sh
exec rmlog rm /var/log/ok.log

Installation alpine :

apk add net-snmp-tools net-snmp
rc-update add snmpd
service snmpd start

vim /etc/snmp/snmpd.conf :

agentAddress udp:172.18.10.11:161
rocommunity secret 172.18.10.0/24

sysLocation Reims
sysContact admin <tp@reims.com>

disk / 10000

exec listpaquet ?
exec userloggedon /userlogged.sh
exec rmlog /bin/rm /var/log/ok.log

Requête snmp :

snmpwalk -v 2c -c community ip oid

Script : userlogged.sh

#!/bin/bash
/usr/bin/w | awk 'NR!=1 && NR!=2 {print $1}'
exit 0

chmod +x /userlogged.sh

Load: 1.3.6.1.4.1.2021.10.1.3.1.x

CPU Idle : 1.3.6.1.4.1.2021.11.11.0
CPU User time : 1.3.6.1.4.1.2021.11.9.0
CPU System time : 1.3.6.1.4.1.2021.11.10.0

Total RAM used: 1.3.6.1.4.1.2021.4.6.0
Total RAM Free: 1.3.6.1.4.1.2021.4.11.0

Available space on the disk: 1.3.6.1.4.1.2021.9.1.7.x → ou x correspond à la partition
Used space on the disk: 1.3.6.1.4.1.2021.9.1.8.1.x → ou x correspond à la partition

snmpwalk -v 2c -c secret 172.18.10.12 NET-SNMP-EXTEND-MIB::nsExtendObjects

snmptranslate -On NET-SNMP-EXTEND-MIB::nsExtendOutputFull.\"nom commande\" → récupérer l'oid du résultat de la commande

snmpwalk -v 2c -c secret 172.18.10.12 NET-SNMP-EXTEND-MIB::nsExtendOutputFull.\"listpaquet\"

snmpwalk -v 2c -c secret 172.18.10.12 NET-SNMP-EXTEND-MIB::nsExtendOutputFull.\"userloggedon\"

snmpwalk -v 2c -c secret 172.18.10.12 NET-SNMP-EXTEND-MIB::nsExtendOutputFull.\"rmlog\" → exécute la commande de suppression