Hálózatok szabadon

Nagyméretű hálózatok szabad szoftveres managementje

Pásztor György
pasztor@linux.gyakg.u-szeged.hu
pasztor@fsn.hu

Miről lesz szó?

Ötletek hálózatmanagelési megoldásokra layer 1-től layer 7-ig és azon túl.

- Közös felhasználói adatbázismegoldás hálózati eszközökhöz - freeradius
- Konfigurációs változtatások propagalása egyszerre több eszközbe - bash & netcat
- Mentsünk konfigot - tftp
- Naplózzunk - syslog-ng
- Adjunk IPcímet a gépeknek - DHCP
- Fejlesszük tovább - verziókezelt konfigurációk
- Adjunk nevet a gépeknek - DNS

Freeradius I.

A feladat: jelentkeztessünk be a hálózati eszközökbe

– megoldás v 0.1: statikus konfig:

```
username pasztor password 7 14031B005E102B20
```

– Valódi megoldás: radius szerver:

```
aaa new-model
aaa group server radius adminok
 server 10.1.7.20 auth-port 1812 acct-port 1813
```

/etc/freeradius/clients.conf:

```
client 10.1.0.0/16 {
        secret     = radpas
        shortname  = admin-vlan
        nastype    = cisco
}
```

Freeradius II.

Userek - userdb

– megoldás v 0.1: statikus fájl - /etc/freeradius/users:

```
pasztor Auth-Type := Local, User-Password == "s3cr3t"
        cisco-avpair = "shell:priv-lvl=15",
        Service-Type = Login-User
```

– megoldás - Adatbázist mögé tenni - /etc/freeradius/postgresql.conf:

```
sql {
        driver = "rlm_sql_postgresql"
        login = "freerad"
        password = ""
        radius_db = "radius"
...
}
```

Freeradius III.

userdb management

```
INSERT INTO radcheck VALUES
 ( DEFAULT, 'pasztor', 'Auth-Type', ':=', 'Local' );
INSERT INTO radcheck VALUES
 ( DEFAULT, 'pasztor', 'User-Password', '==', 's3cr3t' );
INSERT INTO radreply VALUES
 ( DEFAULT, 'pasztor', 'Service-Type', '=', 'Login-User' );
INSERT INTO radreply VALUES
 ( DEFAULT, 'pasztor', 'cisco-avpair', '=', 'shell:priv-lvl=15' );
```

Freeradius IV.

accounting

```
aaa group server radius rad_acct
 server 10.1.7.20 auth-port 1812 acct-port 1813
aaa accounting network acct_methods start-stop group rad_acct
```

AP-n:

```
interface Dot11Radio0
 ssid GUEST
    accounting acct_methods
```

Lekérdezések, pl.:

```
SELECT * FROM radacct
 WHERE username='pasztor' AND nasipaddress='10.1.7.1' ;
```

Konfig „broadcast” I.

Előkészület - /usr/local/share/mgmt/common.sh:

```
userbeker () {
read -p "Kérem a usernevet:" CISCOUSER
}

pwbeker () {
stty -echo echonl
read -p "Kérem a jelszót:" CISCOPASS
stty echo
}
...
```

Konfig „broadcast” II.

Előkészület - /usr/local/share/mgmt/common.sh:

```
predo () {
test "x${CISCOUSER}x" = xx && userbeker
test "x${CISCOPASS}x" = xx && pwbeker
}

postdo () {
unset CISCOUSER
unset CISCOPASS
}
...
```

Konfig „broadcast” III.

Előkészület - /usr/local/share/mgmt/common.sh:

```
ALLSWITCH="sw-l1-1 sw-l1-2
sw-l2-1 sw-l2-2 sw-l2-3"
ALLROUTERS="sw-r1 sw-r2"
ALLAPS="ap0 ap1"
ALLNODES="$ALLROUTERS $ALLSWITCH $ALLAPS"
MGMTHOME=/usr/local/share/mgmt
```

Konfig „broadcast” IV. - Mentsünk konfigot

Éles használat - /usr/local/bin/conffel.sh:

```
. /usr/local/share/cisco/common.sh
predo
for i in ${ALLNODES} ; do nc $i 23 <<END
${CISCOUSER}
${CISCOPASS}
ena
3n4s3cr3t
copy start tftp://server.mgmt.intra/$i.cfg
/n/n/n/n/n/n
exit
END
done
postdo
```

syslog-ng I.

```
source s_adm_net {
        udp(ip(10.1.7.20));
};

destination netadmlog { file("/var/admlog/$YEAR.$MONTH/$HOST"
                        owner("root") group("adm") perm(0640)); };

filter f_nadmhosts { not host("fw"); };

log { source(s_adm_net); filter(f_nadmhosts);
      destination(netadmlog); };
```

syslog-ng II.

```
. /usr/local/share/cisco/common.sh
predo
for i in ${ALLNODES} ; do nc $i 23 <<EOF
${CISCOUSER}
${CISCOPASS}
ena
3n4s3cr3t
conf t
logging trap debugging
logging 10.1.7.20
end
EOF
done
postdo
```

DHCP - I.

```
if exists agent.circuit-id
{ log ( info, concat( "Lease for ", binary-to-ascii (10, 8, ".",
    leased-address), " is connected to interface ",
  binary-to-ascii (10, 8, "/", suffix ( option agent.circuit-id, 2)),
    " (add 1 to port number!), VLAN ",
  binary-to-ascii (10, 16, "", substring( option agent.circuit-id, 2,
    2)),  " on switch ",
  binary-to-ascii(16, 8, ":",
    substring( option agent.remote-id, 2, 6))));
  log ( info, concat( "Lease for ", binary-to-ascii (10, 8,
    ".", leased-address),
  " raw option-82 info is CID: ", binary-to-ascii (10, 8, ".",
    option agent.circuit-id), " AID: ",
  binary-to-ascii(16, 8, ".", option agent.remote-id))); }
```

DHCP - II.

```
class "vlan210" {
   match if binary-to-ascii (10, 16, "",
      substring( option agent.circuit-id, 2, 2)) = "210" ;
}

class "no82" {
        match if not exists agent.circuit-id;
}
```

DHCP - III.

```
subnet 10.4.0.0 netmask 255.255.255.0 {
        option routers 10.4.0.1;
        pool {
                allow members of "vlan210";
                range 10.4.0.10 10.4.0.250;

                option broadcast-address 10.4.0.255;
                option domain-name "bibl.u-szeged.hu";
                option domain-name-servers 160.114.159.130;

        }
}
```

CVS I.

Előkészületek - CVSROOT/loginfo:

```
ALL cvs-mailcommit --mailto admins@site --from cvs@site
                   --cvs %1{sVv} --diff --full
dhcp3\/conf.d $CVSROOT/CVSROOT/dhcpcommit
```

Előlészületek - CVSROOT/checkoutlist:

```
dhcpcommit
```

CVS II.

Előlészületek - CVSROOT/dhcpcommit:

```
#!/bin/bash
logfile=‘mktemp‘
idfile=‘mktemp‘
umask 002
install -m 0600 /usr/local/share/mgmt/dhcpkulcs $idfile
echo "A dhcp reloadolása" >>$logfile
ssh -i $idfile root@dhcp.serv.intra \
  "/etc/init.d/dhcp3-server restart 2>&1" >>$logfile
tail /var/srvlog/‘date +%Y.%m‘/dhcp/syslog >>$logfile
rm $idfile
mail -s "DHCP Reload" admins@site <$logfile
rm $logfile
```

CVS III.

Előlészületek - dhcp: /etc/init.d/dhcp3-server:

```
case "$1" in
  start)
    echo "Updating DHCP config files..."
    cd /etc/dhcp3/conf.d ; cvs up -PAd
    echo -n "Generating DHCP config-file.."
    cat ‘find /etc/dhcp3/conf.d/ -maxdepth 1 -type f‘ \
        >/etc/dhcp3/dhcpd.conf
    echo ’. Done!’
    echo -n "Starting DHCP server: "
```

DNS

DNS és CVS együttműködése:

- verziókezelt, mint pl. a fenti DHCP példa
- a commit után, a friss fájlok automatikusan életbe lépnek
- automatikus SOA verzió generálás
- zóna syntaxcheck commit engedélyezése előtt - CVSROOT/commitinfo:

```
dnszones        $CVSROOT/CVSROOT/zonateszt %p %r %s
```

online cím:

`http://linux.gyakg.u-szeged.hu/~pasztor/sfd2k6/`