John the Ripper á Ubuntu 10.04 MPI Cluster

Pétur Ingi Egilsson
petur [at] petur [.] eu

Efnisyfirlit

Inngangur

Fyrst skal tekið fram að ég er ekki sérfræðingur í MPICH, þetta skjal er skrifað af áhugamanni. Klasinn sem er útfærður hér er ekki ætlaður til nota í umhverfum þar sem krafist er öryggis og áreiðanleika.

Saga

Ég kom mér í þau vandræði að týni lykilorði sem ég þurfi mjög á að halda, að geta brotið það upp hefði tekið of langann tíma. Þar sem ég hef aðgang að nokkuð mörgum tölvum fór ég að leita að aðferð til að fá þær allar til að vinna saman með það að huga að brjóta upp lykilorðið.

Þetta skjal er afrakstur ringulreiði, ofneyslu koffeins og svefnlausrar nætur.

Kröfur

Að minnsta kosti tvær net tengdar tölvur, eg miða við Ubuntu Linux útgáfu 10.04.

> Ég notaðist við 802.11g (54Mbit WiFi), John þarf ekki mikla bandvídd.

Stillingar netþjóns

Kröfur

Föst IP tala eða frátekin í DHCP.

Pakka kröfur

Eftirfarandi pakkar verða notaðir:

- libmpich1.0-dev - mpich static libraries and development files
- libmpich-mpd1.0-dev - mpich static libraries and development files
- libmpich-shmem1.0-dev - mpich static libraries and development files
- mpich2 - Implementation of the MPI Message Passing Interface standard
- mpich2-doc - Documentation for MPICH2
- john - active password cracking tool
- openssh-server - secure shell (SSH) server, for secure access from remote machines
- build-essentials - Informational list of build-essential packages

```
petur@server:~$ sudo apt-get install libmpich1.0-dev libmpich-mpd1.0-dev libmpich-shmem1.0-dev mpich2 mpich2-doc john openssh-server build-essentials
```

Net stillingar

Sjálfgefna /etc/hosts skráin /etc/hosts lýtur svona út

```
127.0.0.1       localhost
127.0.1.1       server.petur.eu server

# The following lines are desirable for IPv6 capable hosts
::1             localhost ip6-localhost ip6-loopback
fe00::0         ip6-localnet
ff00::0         ip6-mcastprefix
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
```

Þú þarft að breyta 127.0.1.1 í IP töluna þína
<server.petur.eu> á að vera FQDN og <server> er hostname á vélinni.

Þú getur fundið út IP töluna þína með því að keyra:

```
petur@server:~$ ifconfig|grep "inet addr"
          inet addr:10.0.0.1      Bcast:10.255.255.255          Mask:255.0.0.0
          inet addr: 127.0.0.1    Mask:255.0.0.0
```

/etc/hosts á að líta svona út eftir að hún hefur verið löguð:

```
127.0.0.1       localhost
10.0.0.1        server.petur.eu server

# The following lines are desirable for IPv6 capable hosts
::1             localhost ip6-localhost ip6-loopback
fe00::0         ip6-localnet
ff00::0         ip6-mcastprefix
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
```

Stillingar notanda

Búðu til nýjann notanda 'cluster' og bættu ~/bin/ við í PATH.

Mér finnst þægilegt að nota sama lykilorð á allar vélarnar.

```
petur@server:~$ sudo useradd -m -s /bin/bash cluster
petur@server:~$ sudo passwd cluster
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

```
petur@server:~$ sudo su - cluster -c "mkdir ~/bin;export PATH=~/bin:$PATH"
```

Stillingar á MPICH

MPI notast við eftirfarandi stýriskrár:

- ~/.mpd.conf
  ATH: Skráin byrjar á .
  Skráin verður að vera chmod 600
  Þessi skrá inniheldur eina staka línu sem er “secretword=<password>” (skiptu út <password> fyrir þitt lykilorð, sem VERÐUR að vera það sama í öllum ~/.mpd.conf skrám í klasanum).
- ~/mpd.hosts
  Inniheldur lista yfir allar tölvurnar í klasanum, einnig þjóninn.
  Sniðið á skránni er "host:kjarna-fjöldi", t.d. 10.0.0.2:4 ef 10.0.0.2 hefur 4 kjarna á örgjörvanum.
  Hægt er að þvinga MPICH til að keyra ekki á öllum kjörnum, það er gert með því að velja lægri kjarnatölu heldur en fjöldi kjarna á örgjörvanum.
  T.d. ef þjónninn hefur 4 kjarna getur verið gott að nota einungis 3 svo hægt sé að nota vélina í eitthvað annað. Þá sérstaklega ef hún er sett upp fyrir fleiri þjónustur.
  EKKI NOTA localhost eða 127.0.0.1 sem vélarnafn, þú verður að notast við IP tölu sem hægt er að hafa samskipti við frá neti.

Athugaðu kjarnafjölda á vélinni og búðu svo til stýriskrárnar.

```
cluster@server:~$ touch ~/.mpd.conf
cluster@server:~$ chmod 600 ~/.mpd.conf
cluster@server:~$ echo secretword=pass>~/.mpd.conf
cluster@server:~$ /sbin/ifconfig|grep "inet addr"
          inet addr:10.0.0.1  Bcast:10.255.255.255  Mask:255.0.0.0
          inet addr:127.0.0.1  Mask:255.0.0.0
cluster@server:~$ cat /proc/cpuinfo|grep processor|wc -l
1
cluster@server:~$ echo 10.0.0.1:1>~/mpd.hosts
```

Athugaðu hvort allt sé í lagi með því að keyra eftirtaldar skipanir:

- mpdboot – keyrir klasann upp.
- mpdtrace - gefur lista yfir allar tölvur í klasanum.
- mpdallexit – keyrir klasann niður.

```
cluster@server:~$ mpdboot
cluster@server:~$ mpdtrace
server
cluster@server:~$ mpdallexit
```

Uppsetning á John the Ripper

Það má finna MPI sniðna útgáfu af John The Ripper www.bindshell.net/tools/johntheripper

```
cluster@server:~$ mkdir source
cluster@server:~$ cd source
cluster@server:~/source$ wget http://www.bindshell.net/tools/johntheripper/john-1.7.2-bp17-mpi8.tar.gz
```

Afpakkaðu henni og keyrðu 'make' úr 'src' möppunni.

```
cluster@server:~/source$ tar -zxf john-1.7.2-bp17-mpi8.tar.gz
cluster@server:~/source$ cd john-1.7.2-bp17-mpi8/src/
cluster@server:~/source/john-1.7.2-bp17-mpi8/src$ make
```

Þú værð lista yfir valmöguleika.

```
To build John the Ripper, type:
        make clean SYSTEM
where SYSTEM can be one of the following:
linux-x86-mmx           Linux, x86 with MMX
linux-x86-sse           Linux, x86 with SSE2 (best)
linux-x86-any           Linux, x86
linux-x86-64            Linux, AMD x86-64, 64-bit native w/SSE2 (best)
linux-x86-64-mmx        Linux, AMD x86-64, 32-bit with MMX
```

Mér finnst 'linux-x86-sse2' virka best á intel based vélum.

```
cluster@server:~/source/john-1.7.2-bp17-mpi8/src$ make clean linux-x86-sse2
```

Athugaðu hvort forritið sé í lagi þó þú náir að þýða það.

```
cluster@server:~/source/john-1.7.2-bp17-mpi8/src$ ../run/john -format=DES -test
Benchmarking: Traditional DES [128/128 BS SSE2]... DONE
Many salts:             1994K c/s real, 1994K c/s virtual

Only one salt:          1658 c/s real, 1654K c/s virtual
```

Færðu nýþýdda forritið yfir í ~/bin möppuna.

```
cluster@server:~/source/john-1.7.2-bp17-mpi8/src$ mv ../run/* ~/bin
```

Keyrðu upp 'john' og vissaði þig um að þú hafir _MPI sniðna útgáfu.

```
cluster@server:~/source/john-1.7.2-bp17-mpi8/src$ john|grep version
John the Ripper password cracker, version 1.7.2_bp17_mpi
```

Að bæta við tölvum

Gerðu eftirfarandi í hvert skipti sem þú bætur við tölvu í klasann:
(Í sýnidæminu hefur nýja talvan IP töluna 10.0.0.2)

Forkröfur

Föst IP tala eða frátekin í DHCP.

Net stillingar

Fylgdu sömu leiðbeiningum og farið var í gegnum í stillingu netþjóns, mundu að nota rétta IP.

Pakka kröfur

Sama og á netþjóni.

Stillingar notanda

Veldu sama lykilorðið á þessari tölvu fyrir 'cluster' og á netþjóninum.

```
petur@node1:~$ sudo useradd -m -s /bin/bash cluster
petur@node1:~$ sudo passwd cluster
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
petur@node1:~$ sudo su - cluster -c "mkdir ~/bin;export PATH=~/bin:$PATH"
```

Stillingar á MPICH

Eftirfarandi skipanir á að keyra á netþjóninum og **ekki** vélinni sem á að bætast við.

Opnum fyrir SSH án lykilorðs frá þjóni.

```
cluster@server:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/cluster/.ssh/id_rsa):
Created directory '/home/cluster/.ssh'
Enter passpharse (empty for no passpharse):
Enter same passpharse again:
Your identification has been saved in /home/cluster/.ssh/id_rsa.
Your public key has been saved in /home/cluster/.ssh/id_rsa.pub.
The key fingerprint is:
0f:d7:c4:14:cf:06:11:d5:80:ec:1f:c3:f3:3b:7f:22 cluster@server
The key's randomart image is:
```

[picture omitted]

```
cluster@server:~$ ssh cluster@10.0.0.2 mkdir -p .ssh
cluster@10.0.0.2's password:
cluster@server:~$ cat .ssh/id_rsa.pub | ssh cluster@10.0.0.2 'cat>>.ssh/authorized_keys'
cluster@10.0.0.2's password:
cluster@server:~$ ssh cluster@10.0.0.2 'cat /proc/cpuinfo|grep processor|wc -l'
2
cluster@server:~$ echo 10.0.0.2:2 >> ~/mpd.hosts
```

```
cluster@server:~$  for i in `cut --delimiter=: -f1 ~/mpd.hosts`;do scp ~/.mpd.conf cluster@$i:~;scp
~/mpd.hosts cluster@$i:~;done
The authenticity of host '10.0.0.1 (10.0.0.1)' can't be established.
RSA key fingerprint is 2d:94:c6:40:b0:02:04:d9:86:c8:16:f3:e6:a7:9f:35.
Are you sure you want to countinue connecting (yes/no)? Yes
Warning: Permanently added '10.0.0.1' (RSA) to the list of known hosts.
cluster@10.0.0.1's password:
.mpd.conf       100%  16       0.0KB/s       00:00
cluster@10.0.0.1's password:
mpd.hosts       100%  22       0.0KB/s       00:00
.mpd.conf       100%  16       0.0KB/s       00:00
mpd.hosts       100%  22       0.0KB/s       00:00
```

Bættu við línunni

```
10.0.0.2        node1
```

í /etc/hosts skránna á þjóninum.

Lokaskrefið er að skipta út /etc/hosts á öllum tölvum sem eru tengdar klasanum með nýju /etc/hosts skránni á þjóninum. Sé þetta ekki gert kemur eftirfarandi villa upp þegar þú reynir að keyra 'mpdboot':

mpdboot_server (handle_mpd_output 407): failed to handshake with mpd on 10.0.0.2; recvd output={}

Uppsetning á John the Ripper

Eins og á þjóni.

Skipanir

Keyrðu upp klasann með skipuninni "mpdboot --verbose --ncpus=1 -n 2"

- --verbose :: gefur okkur betra yfirlit yfir hvað er að gerast
- --ncpus=1 :: segir þjóninum að notast aðeins við 1 kjarna
- -n 2 :: keyra upp klasann með 2 tölvum (þjónn + 1 vinnuvél)

```
cluster@server:~$ mpdboot --verbose --ncpus=1 -n 2
running mpdallexit on server
LAUNCHED mpd on server via
RUNNING: mpd on server
LAUCNHED mpd on 10.0.0.2 via server
RUNNING: mpd on 10.0.0.2
```

Athugaðu ef klasinn svarar skipunum

mpdtrace - gefir lista yfir allar tölvur í klasanum

mpiexec -np 3 hostname, þýðir “keyrðu skipunina 'hostname' á 3 kjörnum”

```
cluster@server:~$ mpdtrace
server
node1
cluster@server:~$ mpiexec -np 3 hostname
server
node1
node1
```

mpdallexit - Keyrir niður klasann

```
cluster@server:~$ mpdallexit
```

Að nota klasann til að brjóta upp lykilorð.

Ég notast við einfald MD5 hash

```
cluster@server:~$ echo user:47584a15f1ba6c65da3a2ef8e43e606b > crackme1.md5
cluster@server:~$ mpdboot --ncpus=2 -n 2
```

```
cluster@server:~$ for i in `cut --delimiter=: -f1 ~/mpd.hosts`;do scp ~/crackme1.mp5
cluster@$1:~;done
```

Skipunin að ofan er notuð til að dreifa skjölum á vinnutölvurnar. Það er nauðsinlegt þar sem við erum ekki að nota sameigilegt ~. Þetta er hægt að laga t.d. með NFS.

Hér er skripta sem hægt er að nota til að dreyfa skrám:

```
--- distributer.sh begins ---

#!/bin/bash
# usage: ./distributer.sh filename
for x in `cut –delimiter=: -f1 ~/mpd.hosts`;do scp $1 cluster@$i:~;done

--- distributer.sh ends ---
```

Sláðu á 'ctrl+c' þegar lykilorðið hefur verið fundið.
Þess er þörf því við erum ekki með sameigilega ~

```
cluster@server:~$ mpiexec -np 3 john --format:raw-MD5 crackme1.md5
Loaded 1 password hash (Raw MD5 [raw-md5 SSE2])
Loaded 1 password hash (Raw MD5 [raw-md5 SSE2])
Loaded 1 password hash (Raw MD5 [raw-md5 SSE2])
petur1           (user)
Process 2 completed loop.
Threat: 2 guesses: 1    time     0:00:00:02 (3)  c/s: 5616K trying: petciL – petusc
^Ccluster@server:~$
```

Mundu að keyra niður klasann eftir notkun.

```
cluster@server:~$ mpdallexit
```

If you have any questions, comments or would like to contribute to this document please send me an email to petur [at] petur [dot] eu