

Sunday, November 29, 2009

## Use ssh port redirection to access VCS hagui and VEA

If you don't have direct access from your PC to the cluster server, but another unix jumphost has, you can do the same as for the dracs and the ilos.

The connectivity is

PC-jumphost-clusternode

in your PC you can do a:

```
ssh -g jumphost -L 14141:clusternode:14141 -L 14150:clusternode:14150
```

Then, open the "Veritas Cluster Manager" software in your PC, and point it to "localhost", and you'll be managing the remote cluster :)

For Veritas Enterprise Administrator (vea), we only need to forward one port:

```
ssh -g jumphost -L 2148:veanode:2148
```

Posted by rdircio in General unix at 16:06

## connect to a HP-ILO or Dell DRAC from your pc using a ssh tunnel

Ok, so your PC connects to a vpn, and there's this one unix host that has access to the ilo's and dracs, but your pc doesn't...

So our participants are, in order of connection:

PC-jumphost-console

that means PC cannot access console, but jumphost does.

If "console" is a HP-ILO, from your PC do:

```
ssh -C -g jumphost -L 443:console:443 -L 3389:console:3389 -L 9300:console:9300 -L 17990:console:17990  
-L 17988:console:17998 -L 3002:console:3002 -L 23:console:23
```

If "console" is a Dell DRAC, from your PC do:

```
ssh -C -g jumphost -L 443:console:443 -L 5900:console:5900 -L 5901:console:5901 -L 3668:console:3668 -L  
3669:console:3669
```

And then, in your pc, use <https://127.0.0.2> to connect to either DRAC or ILO.

Each time you do one of these redirections you're using the ports exclusively, so only one drac or ilo can be redirected at a time.

Posted by rdircio at 02:05

Friday, November 20. 2009

## Performance charts

I made some performance charts from the output of sar and custom scripts, check them out!

<http://www.kraftek.com/perf/>

The source is in

<http://www.kraftek.com/perfsrc/>

they were built using [open flash chart](#) and my own php/ksh scripts.

Posted by rdircio in Linux at 23:05

Tuesday, November 17. 2009

**The kernel still uses the old table. The new table will be used at the next reboot.**

if, when creating partitions with fdisk or cfdisk you get this message on exit:

*WARNING: Re-reading the partition table failed with error 16: Device or resource busy.  
The kernel still uses the old table.  
The new table will be used at the next reboot.  
Syncing disks.*

You don't need to reboot the box, just issue "partprobe"

Posted by rdircio in Linux at 14:23

### **Prevent sudo users to get shells from vi or less with NOEXEC**

If you allow someone to "sudo vi" they could obtain a shell prompt as root if they type ":shell".

If you allow someone to "sudo less" they could also obtain a shell prompt as root if they type "! <enter>"

To avoid that you can tag "less" and "vi" with the NOEXEC tag.

This is an example sudoers that tags "more", "less" and "vi" as noexec, and prevents the group "theusers" from doing "sudo bash" and "sudo su -"

```
Cmnd_Alias NOEXEC_CMDS = /usr/bin/less, /usr/bin/more, /bin/vi
Cmnd_Alias SHELLS = /usr/bin/*sh*, /sbin/*sh*, /bin/*sh*, /bin/su
%theusers ALL=(ALL) NOPASSWD: ALL, !SHELLS, NOEXEC: NOEXEC_CMDS
```

Posted by rdircio at 10:37

## Better searches in s9y

mysql limits you by default to search for strings no smaller than 3 characters, so, if i wanted to look for "dd" in s9y i had no luck.

F\*n grep is better than mysql with that > 3 chars limit.

s9y also uses MATCH and AGAINST which makes searches a bit dumb.

To overcome this i added the parameter "--ft\_min\_word\_len=1" to mysql startup, so we can search strings shorter than 3 chars.

*/usr/bin/mysqld\_safe --ft\_min\_word\_len=1 --datadir=/var/lib/mysql --pid-file=/var/run/mysql/mysql.pid \$SKIP &*  
*To make ft\_min\_word\_len take effect you have to reindex the tables you wish to search with less than 3 chars. To do it:*

```
mysql> repair table serendipity_entries quick;
```

```
+-----+-----+-----+-----+
| Table          | Op   | Msg_type | Msg_text |
+-----+-----+-----+-----+
| serendipity.serendipity_entries | repair | status  | OK      |
+-----+-----+-----+-----+
1 row in set (0.20 sec)
```

```
mysql> repair table serendipity_authors quick;
```

```
+-----+-----+-----+-----+
| Table          | Op   | Msg_type | Msg_text |
+-----+-----+-----+-----+
| serendipity.serendipity_authors | repair | status  | OK      |
+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

```
mysql> repair table serendipity_entrycat quick;
```

```
+-----+-----+-----+-----+
| Table          | Op   | Msg_type | Msg_text |
+-----+-----+-----+-----+
| serendipity.serendipity_entrycat | repair | status  | OK      |
+-----+-----+-----+-----+
```

*around line 773 of s9y include/functions\_entries.inc.php we changed MATCH and AGAINST for LIKE*

```
//-- rdircio, better searches here
```

```
//      $cond["find_part"] = "MATCH(title,body,extended) AGAINST('$term' IN BOOLEAN MODE)";
```

```
        $cond["find_part"] = "(title LIKE '%$term%' OR body LIKE '%$term%' OR extended LIKE
'$term%')";
    } else {
//        $cond["find_part"] = "MATCH(title,body,extended) AGAINST('$term')";
        $cond["find_part"] = "(title LIKE '%$term%' OR body LIKE '%$term%' OR extended LIKE
'$term%')";
    }
}
```

Now, you can enter text in the quicksearch like " tar c " at this blog and it will find entries like " tar cvf" and not entries like "start"

Posted by rdircio at 22:37

Sunday, November 8, 2009

## making ssh brute force attacks life's harder

if you have many of these in your log:

```
Nov 8 13:55:47 www sshd[12571]: Failed password for invalid user webmaster from 189.180.184.89 port 47706 ssh2
```

you can use iptables to stop them for a while, so their brute force will take years to succeed, if ever.

I added some rules so that only 5 connections can be made in a minute to ssh, if one more is attempted the host will be banned for 2 minutes, if more connections are retried, the ban is extended. since the bots can't help themselves they won't stop, so they'll be banned for a real while :)

```
iptables -N SSH_WHITELIST
iptables -A SSH_WHITELIST -s 175.161.21.55 -m recent --remove --name SSH -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --set --name SSH
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j SSH_WHITELIST
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 60 --hitcount 6 --rttl
--name SSH -j ULOG --ulog-prefix SSH_brute_force
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -m recent --update --seconds 120 --hitcount 6 --rttl
--name SSH -j DROP
```

Posted by rdircio at 15:19

Saturday, November 7. 2009

## using mod\_deflate in apache2 to compress everything

We're trying to save bandwidth here, so we added to httpd.conf:

```
LoadModule deflate_module lib64/httpd/modules/mod_deflate.so
SetOutputFilter DEFLATE
DeflateCompressionLevel 9
BrowserMatch ^Mozilla/4 gzip-only-text/html
BrowserMatch ^Mozilla/4.[0678] no-gzip
BrowserMatch !\bMSIE !no-gzip !gzip-only-text/html
DeflateFilterNote Input input_info
DeflateFilterNote Output output_info
DeflateFilterNote Ratio ratio_info
LogFormat "%r" %b (%{input_info}n====>{%output_info}n) (%{ratio_info}n%%)' deflate
CustomLog /var/log/httpd/deflate_log deflate
```

We can see some entries in the /var/log/httpd/deflate\_log

```
"GET /blog/images/magplus.gif HTTP/1.1" 192 (923====>174) (18%)
"GET /blog/ HTTP/1.1" 8044 (50582====>8026) (15%)
"GET /blog/index.php?/serendipity.css HTTP/1.1" 2778 (11987====>2760) (23%)
"GET /blog/templates/translucency/transblue.css HTTP/1.1" 903 (2787====>885) (31%)
"GET /nomove.js HTTP/1.1" 274 (566====>256) (45%)
```

Posted by rdircio in Linux at 11:55

Monday, November 2. 2009

## **mount server reported tcp not available, falling back to udp**

If your nfs client has this:

```
# mount /usr/sap/trans  
mount server reported tcp not available, falling back to udp  
mount: RPC: Program not registered
```

and this:

```
# rpcinfo -p nfsserver  
No remote programs registered.
```

you may have tcpwrappers in the nfs server, so, in the nfs server edit /etc/hosts.allow and add:

```
portmap : usdaapp151,10.21.40.100 : ALLOW  
portmap : ALL : DENY  
nfs-server : 10.21.40.100 : ALLOW  
nfs-server: ALL : DENY
```

do not restart anything, just mount your filesystem in the client

Thanks to Alfredo Rioja

Posted by rdircio in Linux at 20:29