# Tulip reflex calling sequence

## Top level vtrace0chk.pl

#pinger;300 05 2 * * * /afs/slac/package/pinger/tulip/vtrace0chk.pl

There is no call to reflex.pl in trscontab

I cannot find a call to vtrace0chk via grep vtrace0chk ~cottrell/bin/* or  via  grep vtrace0chk /afs/slac/package/pinger/tulip/*

## Reflex.cgi level

378cottrell@wanmon:~$grep reflex /afs/slac/package/pinger/tulip/*

/afs/slac/package/pinger/tulip/vtrace0chk.pl:  $url='http://www-wanmon.slac.stanford.edu/cgi-wrap/reflex.cgi?target='.$ip;

### Processes runing in wanmon

0 S apache    1032     1  0  78   0 -  4487 pipe_w 05:17 ?        00:00:00 /usr/local/bin/perl -wT /afs/slac/g/www/cgi-wrap-bin/net/offsite_mon/reflex.cgi target=180.87.96.21

0 S apache    1231  1032  0  78   0 -   938 pipe_w 05:17 ?        00:00:00 perl /afs/slac.stanford.edu/g/scs/net/netmon/bin/asn.pl 180.87.96.21

0 S apache    1289  1231  0  78   0 -  2317 wait   05:17 ?        00:00:00 sh -c whois -h whois.radb.net AS6453 2>/dev/null | egrep \(as-name\|descr\)

0 R apache    1291  1289 33  85   0 -  3108 ?      05:17 ?        04:40:34 whois -h whois.radb.net AS6453

reflex.cgi calls asn.pl around line 1588:

```
################################## ASN ##############################
$cmd="/afs/slac.stanford.edu/g/scs/net/netmon/bin/asn.pl $target";
unless($cmd=~/^([\/\w+-\.\s+:]+)$/) {#untaint
die "Tainted invalid cmd=$cmd";
}
$cmd=$1;#untaint
```

## wanmon web log

348cottrell@wanmon:~$grep reflex /var/log/httpd/access_log

134.79.197.197 - - [05/Feb/2017:07:24:03 -0800] "GET /cgi-wrap/reflex.cgi?target=62.78.94.110 HTTP/1.1" 200 9182 "-" "Windows IE 7"
134.79.197.197 - - [05/Feb/2017:07:26:58 -0800] "GET /cgi-wrap/reflex.cgi?target=217.79.60.62 HTTP/1.1" 200 261847 "-" "Windows IE 7"
134.79.197.197 - - [05/Feb/2017:07:28:16 -0800] "GET /cgi-wrap/reflex.cgi?target=84.237.43.50 HTTP/1.1" 200 262878 "-" "Windows IE 7"
134.79.197.197 - - [05/Feb/2017:16:25:07 -0800] "GET /cgi-wrap/reflex.cgi?target=77.37.196.3 HTTP/1.1" 200 8471 "-" "Windows IE 7"
134.79.197.197 - - [05/Feb/2017:16:25:26 -0800] "GET /cgi-wrap/reflex.cgi?target=77.37.254.198 HTTP/1.1" 200 9218 "-" "Windows IE 7"

- wanmon

62.210.80.47 - - [05/Feb/2017:04:59:21 -0800] "GET /cgi-wrap/reflex.cgi?target=192.68.191.233 HTTP/1.1" 200 22111 ...

67.167.170.19 - - [05/Feb/2017:05:16:13 -0800] "POST /cgi-wrap/reflex.cgi HTTP/1.1" 200 7 "http://tulip.slac.stanford.edu/"

- c-67-167-170-19.hsd1.mi.comcast.net.

## asn.pl

### On rhel6-64

asn.pl works on rhel6-64.slac.stanford.edu and pinger.slac.stanford.edu

350cottrell@rhel6-64e:~$/afs/slac.stanford.edu/g/scs/net/netmon/bin/asn.pl 180.87.96.21
Getting ASN for 180.87.96.21...
IPv4: 180.87.96.21
DNS: if-ae-20-2.tcore1.SVQ-Singapore.as6453.net
ASN: 6453
Descr: NA

### On wanmon

However on wanmon.slac.stanford.edu it stalls online 98 of asn.p

352cottrell@wanmon:~$perl -d /afs/slac.stanford.edu/g/scs/net/netmon/bin/asn.pl 180.87.96.21

Loading DB routines from perl5db.pl version 1.28

Editor support available.

Enter h or `h h' for help, or `man perldebug' for more help.

main::(/afs/slac.stanford.edu/g/scs/net/netmon/bin/asn.pl:56):

56:  require IEPM::Tools::ASNWhoIs;

 DB<1> c 98  Getting ASN for 180.87.96.21...

main::(/afs/slac.stanford.edu/g/scs/net/netmon/bin/asn.pl:98):

98:  my $ans = $as->node2ASN( $node );

 DB<2> n

#it stalled here, when I ^c I got

IEPM::Tools::ASNWhoIs::ASnumbertoASText(/afs/slac.stanford.edu/g/scs/net/netmon/iepm/IEPM/Tools/ASNWhoIs.pm:107):

Looking in ASNWhois.pm, I see

```
    my $request = "whois -h whois.radb.net AS" . $asn . ' 2>/dev/null | egrep \(as-name\|descr\)';#$asn=6453
#    print "REQU: '$request'";
    my @req = `$request`;#This results in IEPM::Tools::ASNWhoIs::ASnumbertoASText(/afs/slac.stanford.edu/g/scs/net/netmon/iepm/IEPM/Tools/ASNWhoIs.pm:107): on rhel6-64
    my $asname = ""; #This is line 107,
```

ASNnumbertiASText  is part of ASNWHhois. It appears as:

```
sub ASnumbertoASText
{
    my $self = shift;
    my $asn = shift;
    # deal with nulls
    return "$NA" if ( $a eq $NA );
    my $request = "whois -h whois.radb.net AS" . $asn . ' 2>/dev/null | egrep \(as-name\|descr\)';
#    print "REQU: '$request'";
    my @req = `$request`;
```

## Possible Alternatives

http://search.cpan.org/~adulau/Net-Whois-RIS-0.5/lib/Net/Whois/RIS.pm

### https://mundosubmundo.kaiux.com/2015/02/how-to-use-ip-to-asn-from-team-cymru-using-perl/

E.g. from comand line, if given the reverse IP address (below we were looking for 180.87.96.21) the ASN || the country code |the Registry

347cottrell@wanmon:~$dig +short 21.96.87.180.origin.asn.cymru.com TXT
"6453 | 180.87.0.0/17 | IN | apnic | 2009-07-21"

One can get the dsn using:

363cottrell@wanmon:~$dig +short -x 180.87.96.21
if-ae-20-2.tcore1.SVQ-Singapore.as6453.net.

One can get the ip address from the name using

395cottrell@wanmon:~$dig +short if-ae-20-2.tcore1.SVQ-Singapore.as6453.net
180.87.96.21

## Fix

Replaced asn.pl. The old version is at ~cottrell/bin/asn-old.pl the new is at ~cotttrell/bin/asn.pl

There is also a script ~cottrell/killer.pl to kill stalled processes.