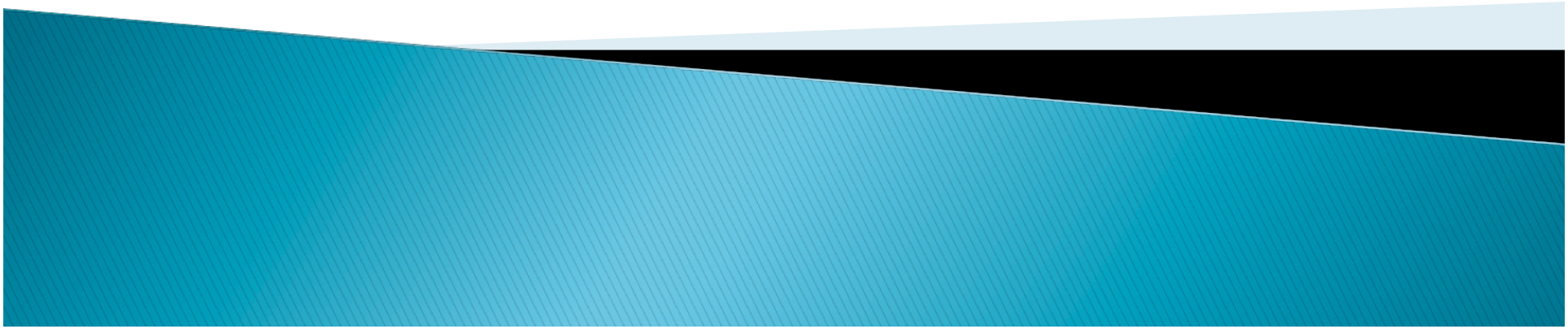
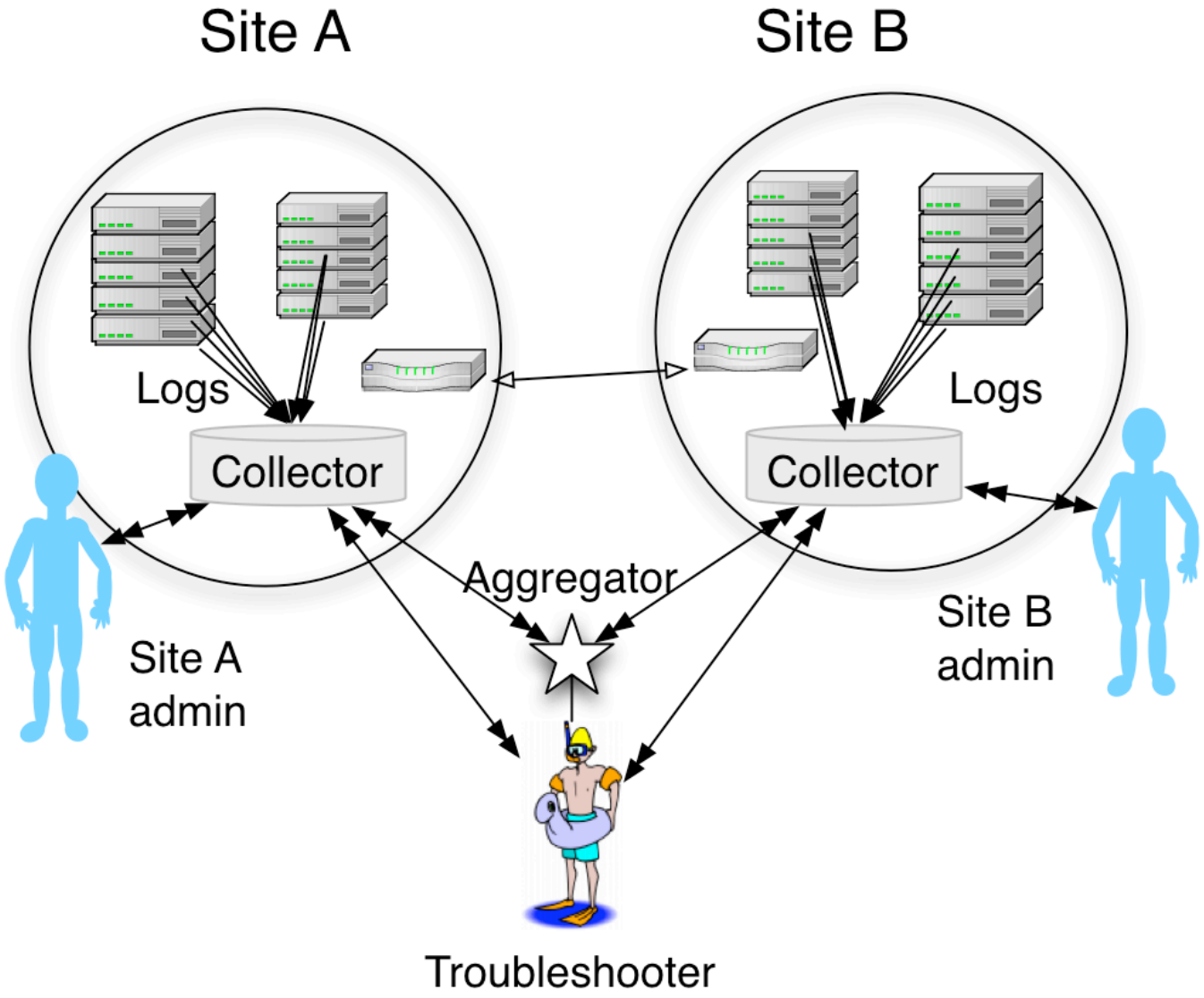
Center for Enabling Distributed Petascale Science (CEDPS)

A SciDAC Center for Enabling Technology

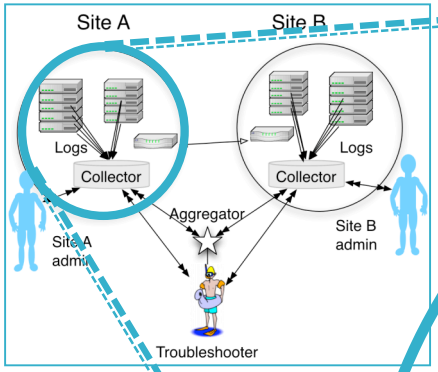
OSG Site Adminstrator Workshop

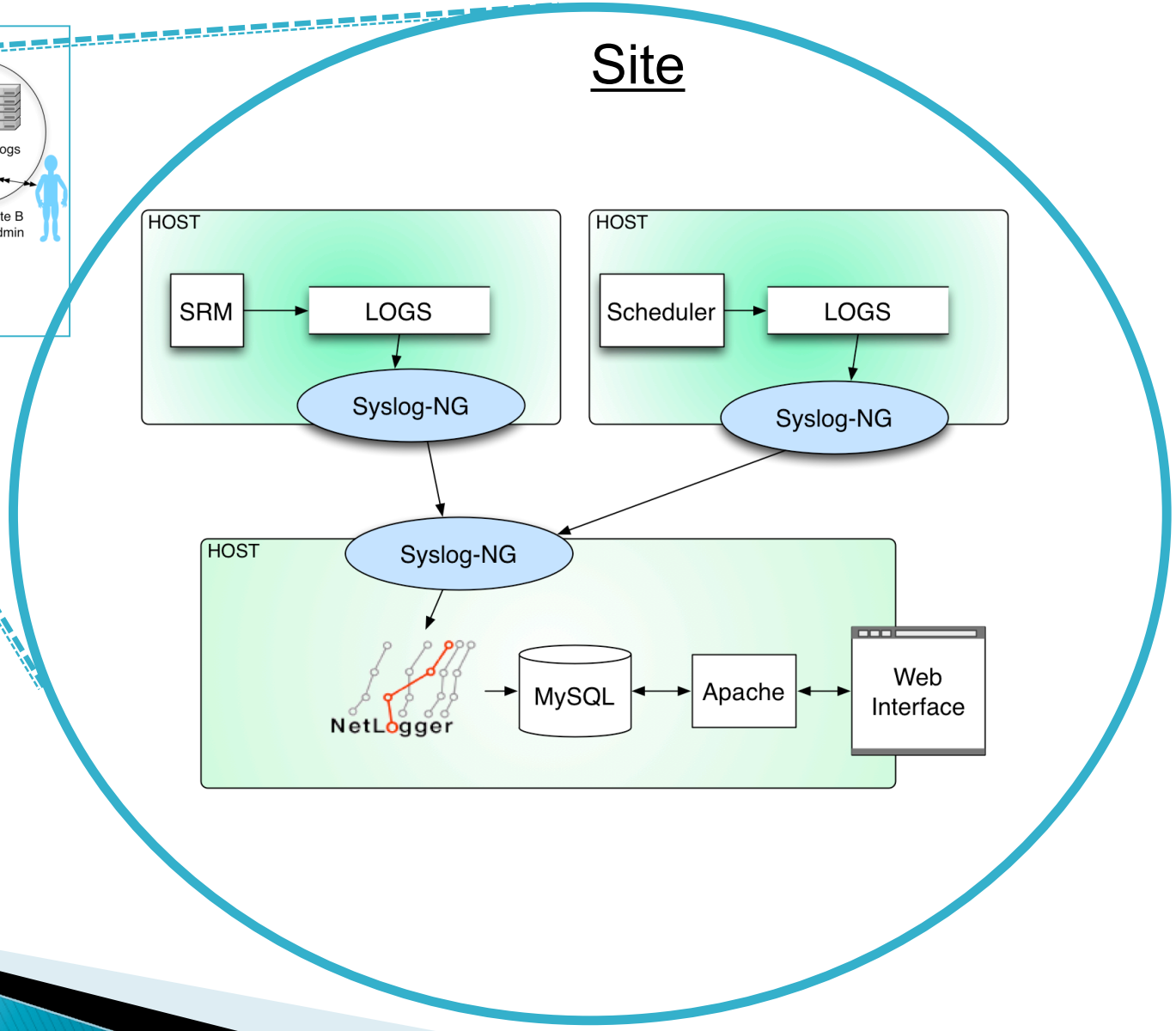


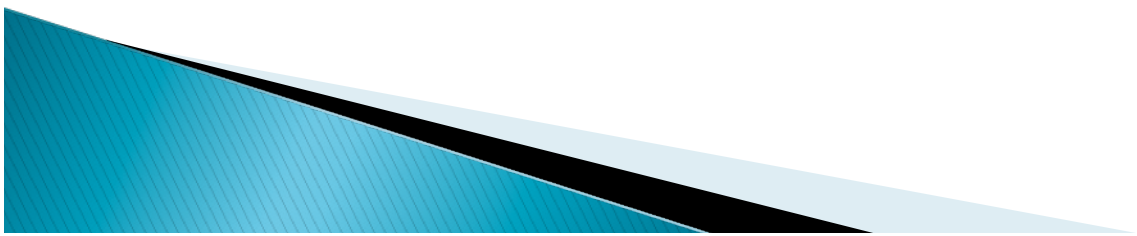
Cross-site Architecture



Site Architecture







Syslog-ng configuration

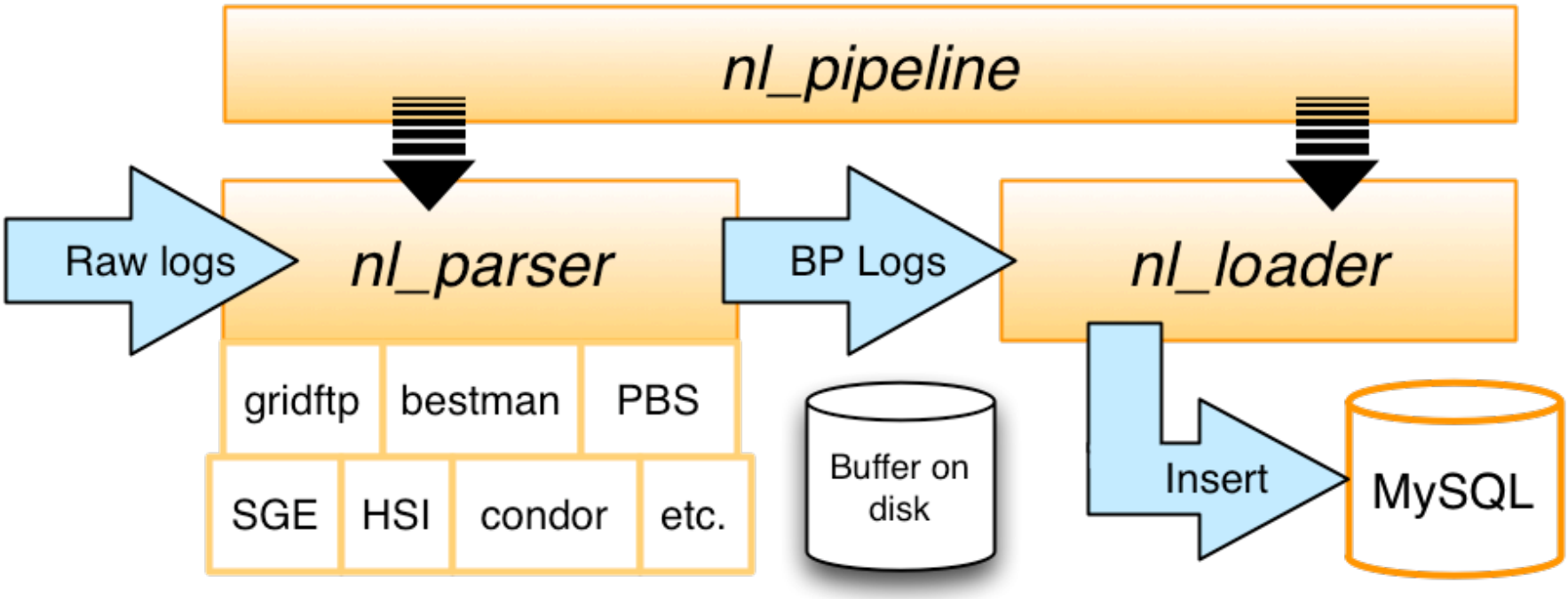
Syslog-ng is a part of the OSG/VDT Bestman package

```
[root@pdsfgrid2 ~]# vdt-control --list
Service            | Type   | Desired State
-------------------+--------+--------------
fetch-crl          | cron   | do not enable
vdt-rotate-logs    | cron   | enable
vdt-update-certs   | cron   | do not enable
gsiftp             | inetd  | enable
gratia-gridftp-tran| cron   | do not enable
bestman            | init   | enable
edg-mkgridmap      | cron   | do not enable
gums-host-cron     | cron   | do not enable
syslog-ng-sender   | init   | enable
[root@pdsfgrid2 ~]# vdt-version
You have installed a subset of VDT version 1.10.1v:
Software
Berkeley Storage Manager (BeStMan)
EDG Make Gridmap 3.0.0
Fetch CRL 2.6.6
GPT 3.2autotools2004-NMI-9.0
Gratia GridFTP Probe 1.02.1-5
Grid User Management System (GUMS) Client
Java 5 SDK 1.5.0_17
Java 6 SDK 1.6.0_11
Logrotate 3.7
PRIMA Authorization Module 0.8.3
syslog-ng 2.0.8
vdt-update-certs 2.2
Wget 1.11.4
```

Syslog-ng configuration

```
[root@pdsfgrid2 etc]# cat syslog-ng-sender.conf
# WARNING!
# Use the script at $VDT_LOCATION/vdt/setup/configure_syslog_ng_sender to edit
# this file.  Manual editing of this file is discouraged.  Manual changes may
# be lost when using the automatic configuartion script, or they may severely
# confuse the configure_syslog_ng_sender script during future edits.
options {
   time_sleep(500);  # polling interval, in ms (make this once per second)
   use_fqdn(yes);    # use fully qualified domain names
   ts_format(iso);   # use ISO8601 timestamps
   # for normal load
   flush_lines (10); # number of lines to buffer before writing to disk
   log_fifo_size(100);
   stats_freq(3600);  # number of seconds between syslog-ng internal stats events; these are useful
                      # for ensuring syslog-ng is not getting overloaded
};
# Sources
source gridftp_auth_log { file ("/export/data/OSG-1.0.1/globus/var/log/gridftp-auth.log" follow-freq(1) flags(no-parse)
    log_prefix('gridftp_auth_log ') ); };
source gridftp_log { file ("/export/data/OSG-1.0.1/globus/var/log/gridftp.log" follow-freq(1) flags(no-parse)
    log_prefix('gridftp_log ') ); };
source event_srm_log { file ("/export/data/OSG-1.0.1/vdt-app-data/bestman/logs/event.srm.log" follow-freq(1) flags(no-parse)
    log_prefix('event_srm_log ') ); };
source syslog_ng { internal(); };
source test_src  { unix-stream("/tmp/syslog-ng-test");  };
# Destinations
destination local_collector   { udp("osp.nersc.gov" port(5145) ); };
destination syslog_ng_dest { file ("/export/data/syslog-ng/syslog-ng.log" perm(0644) ); };
# Define what should be forwarded to the destinations
# Definitions
log { source(gridftp_auth_log); destination(local_collector); flags(flow-control); };
log { source(gridftp_log); destination(local_collector); flags(flow-control); };
log { source(event_srm_log); destination(local_collector); flags(flow-control); };
```

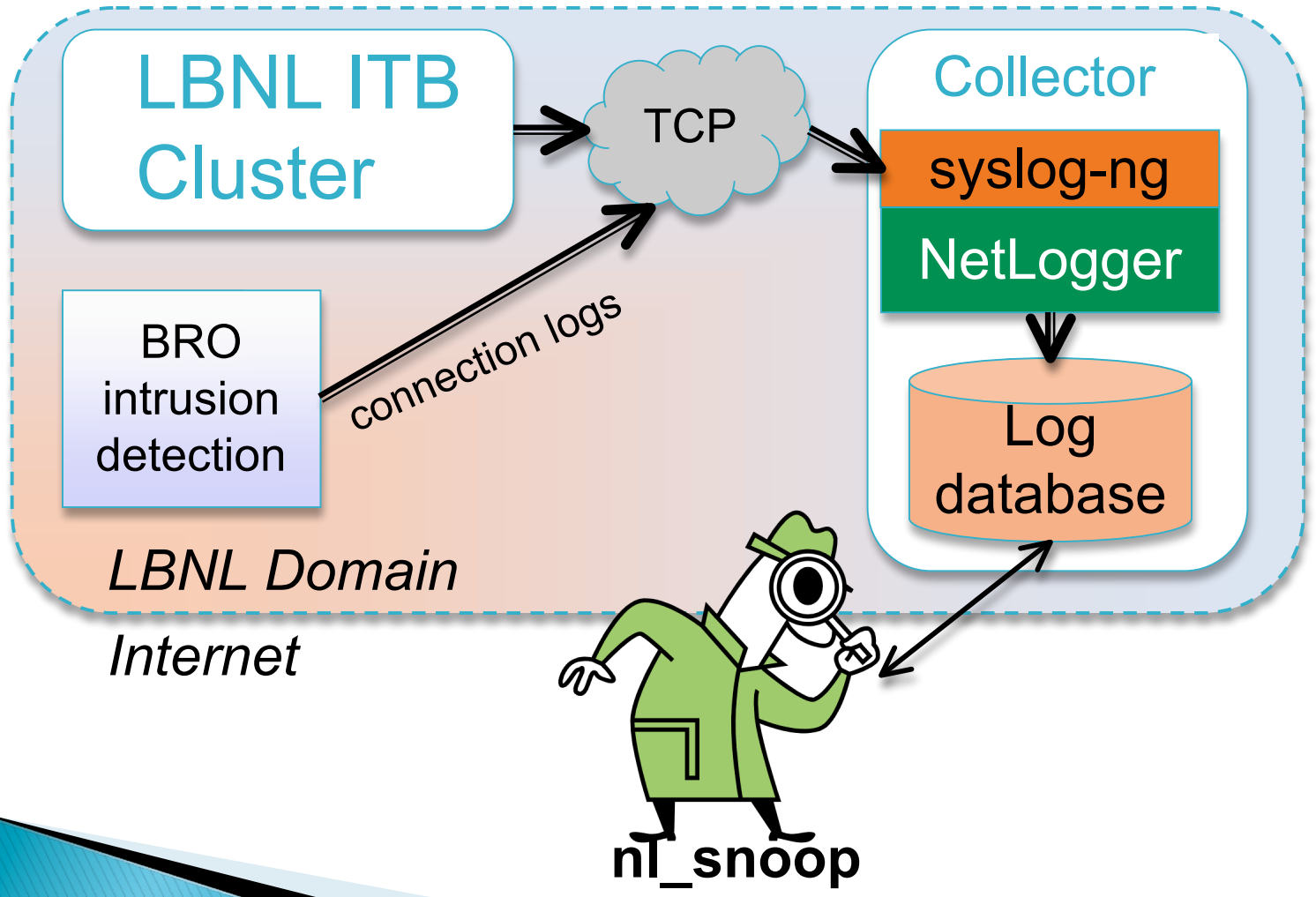
NetLogger “Pipeline”



Use-Case for OSG Security: *nl_snoop*

- Scenario
  - An OSG user's account is compromised; all jobs in last week are suspect
- Current approach
  - Each site admin needs to find jobs run and resources accessed by that user's DN
- Improvement
  - A command-line tool, *nl_snoop*, queries the NetLogger site log database and reports all information for that DN
- Status
  - Being tested by OSG Security team

nl_snoop Deployment Example

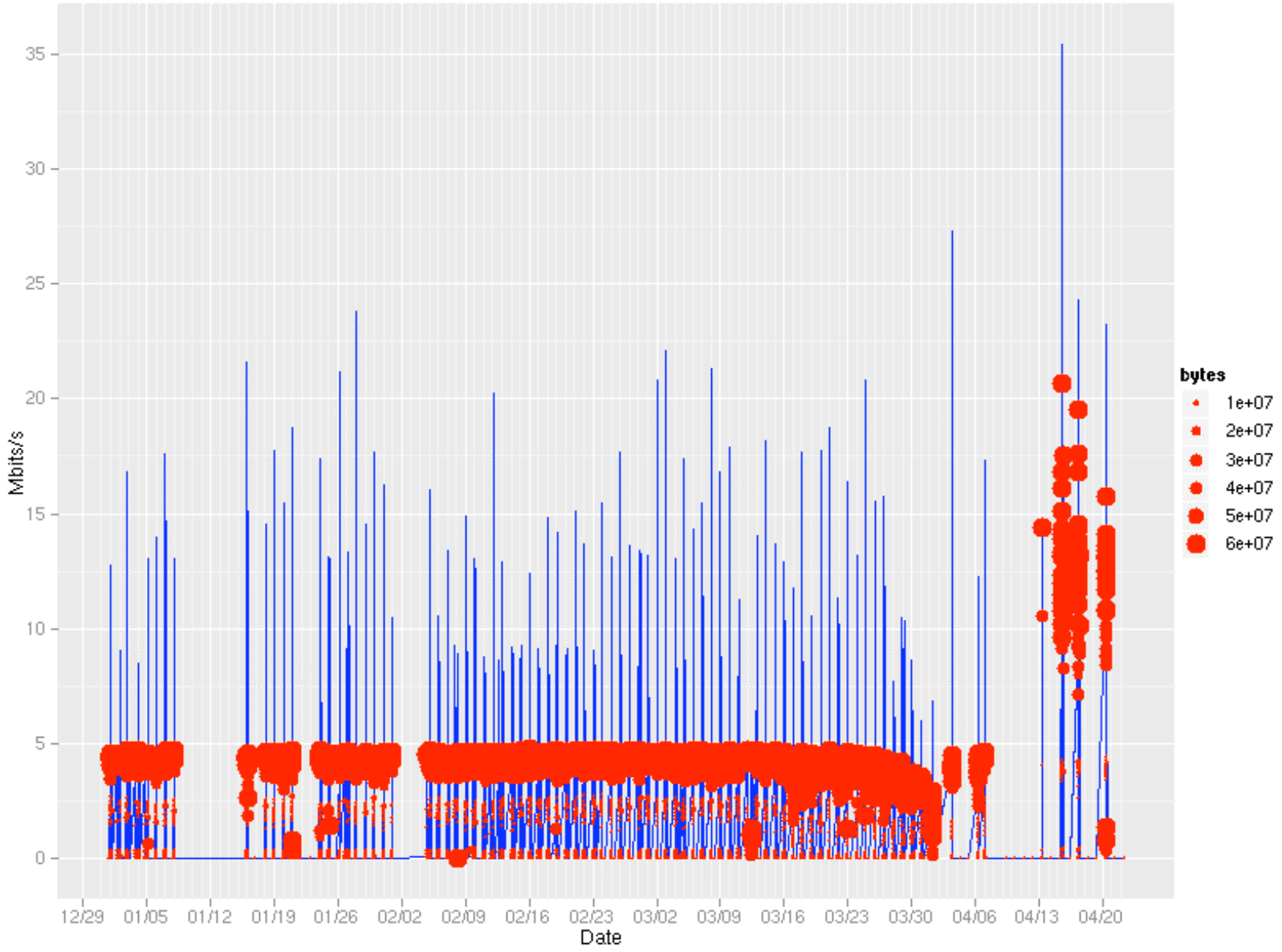


nl_snoop sample output

```
$ nl_snoop -d netlogger -u mysql://netlogger@localhost:49152 -t "1 week
   ago"::now -p "/DC=org/DC=doegrids/OU=People/CN=James Alan Basney 710056"
Password:

Activity for '/DC=org/DC=doegrids/OU=People/CN=James Alan Basney 710056'
between 2009-05-28T14:10:11.429331-05:00 and 2009-06-04T14:10:11.429636-05:00

* Jobs:
   Start time (-05:00)  End time    Host    User (UID,GID)  Sched  Exec
   -------------------  --------    ----    --------------  -----  -----
   2009-06-04T13:15:49  ...13:15:50 foo.edu mis (65002,2)   fork   unknown

* GridFTP Transfers:
   Start time (-05:00)  End time   Host     Port   User Filename
   -------------------  --------   ----     ----   ---- --------
   2009-06-04T14:09:59 ...14:09:59 foo.edu  52383  mis  /tmp/jim.log
```

https://twiki.grid.iu.edu/bin/view/Security/Logging2009#Example_nl_snoop_output

BeStMan performance



More information

- NetLogger
  - http://acs.lbl.gov/NetLoggerWiki/
  - Downloads, documentation, etc.
- CEDPS Troubleshooting
  - http://www.cedps.net/index.php/Troubleshooting
- Contact
  - Dan Gunter - dkgunter@lbl.gov
  - Keith Beattie - ksbeattie@lbl.gov