splunk>

.conf 2010

Splunk Worldwide Users' Conference

The Palace Hotel, San Francisco, CA
August 9-11, 2010

splunk>

Enriching your data with Lookups and more.

Or… Splunking a Supercomputer

Jon Stearley

Sandia National Laboratories

jrstear@sandia.gov

Enriching your data with Lookups and more

SUMMARY:

Lookups, subsearches, macros, and field-actions are awesome!

Here's how you do it…

CHARACTERS:

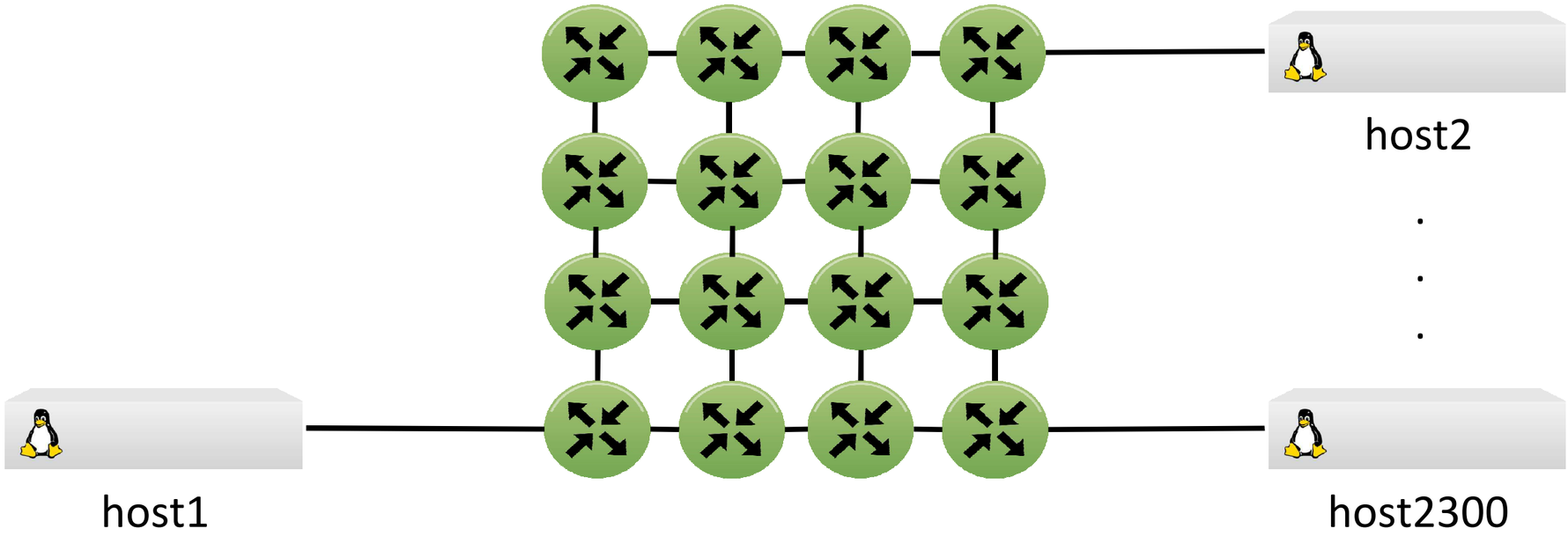
Kaa the cable

and

Bart the user

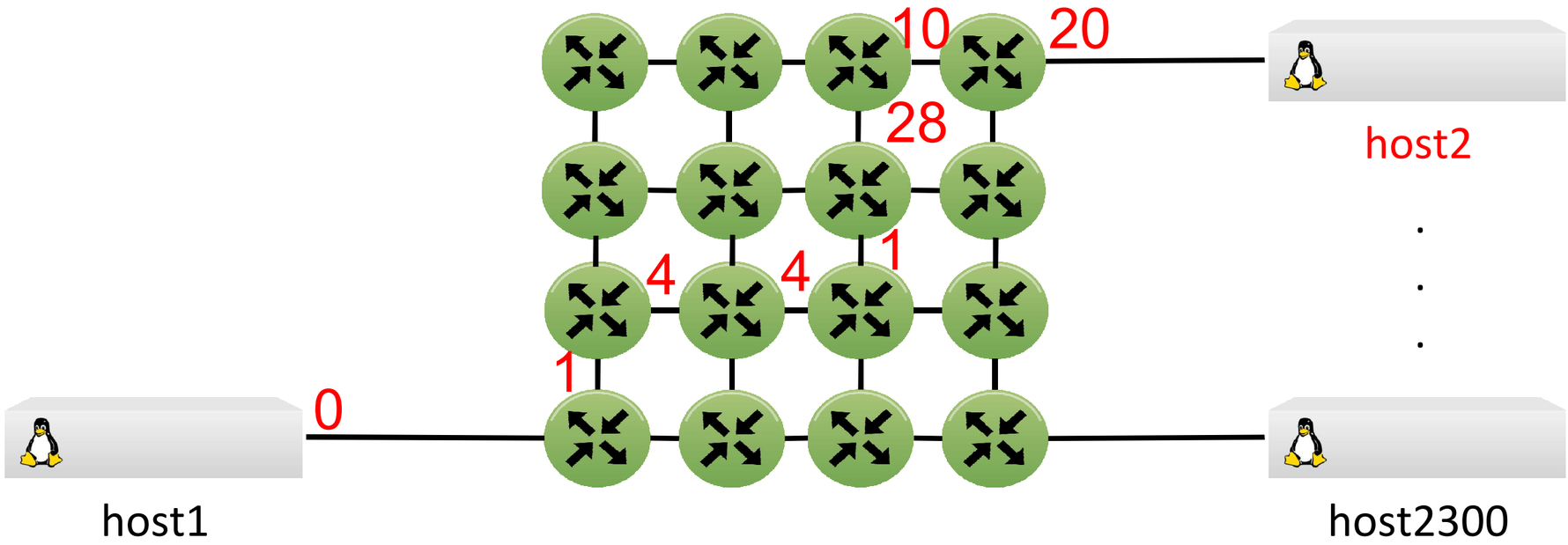
Lookups: host1 network problem

ibwarn: [17841] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,28,10,20)



Lookups: host1 network problem

ibwarn: [17841] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,28,10,20)



Configuring a lookup

ibwarn: [17841] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,28,10,20)

Step #1: Create lookup file splunk/etc/system/lookups/ib.csv

route, destination
”0,1,4,4,1,28,10,20",host2
"0,1,7,7,1,28,7,36",c2-nem1-b
"0,1,7,7,1,28,7,1,25",oss-scratch24
…

Step #2 : Edit transforms.conf

[ib]
filename = ib.csv

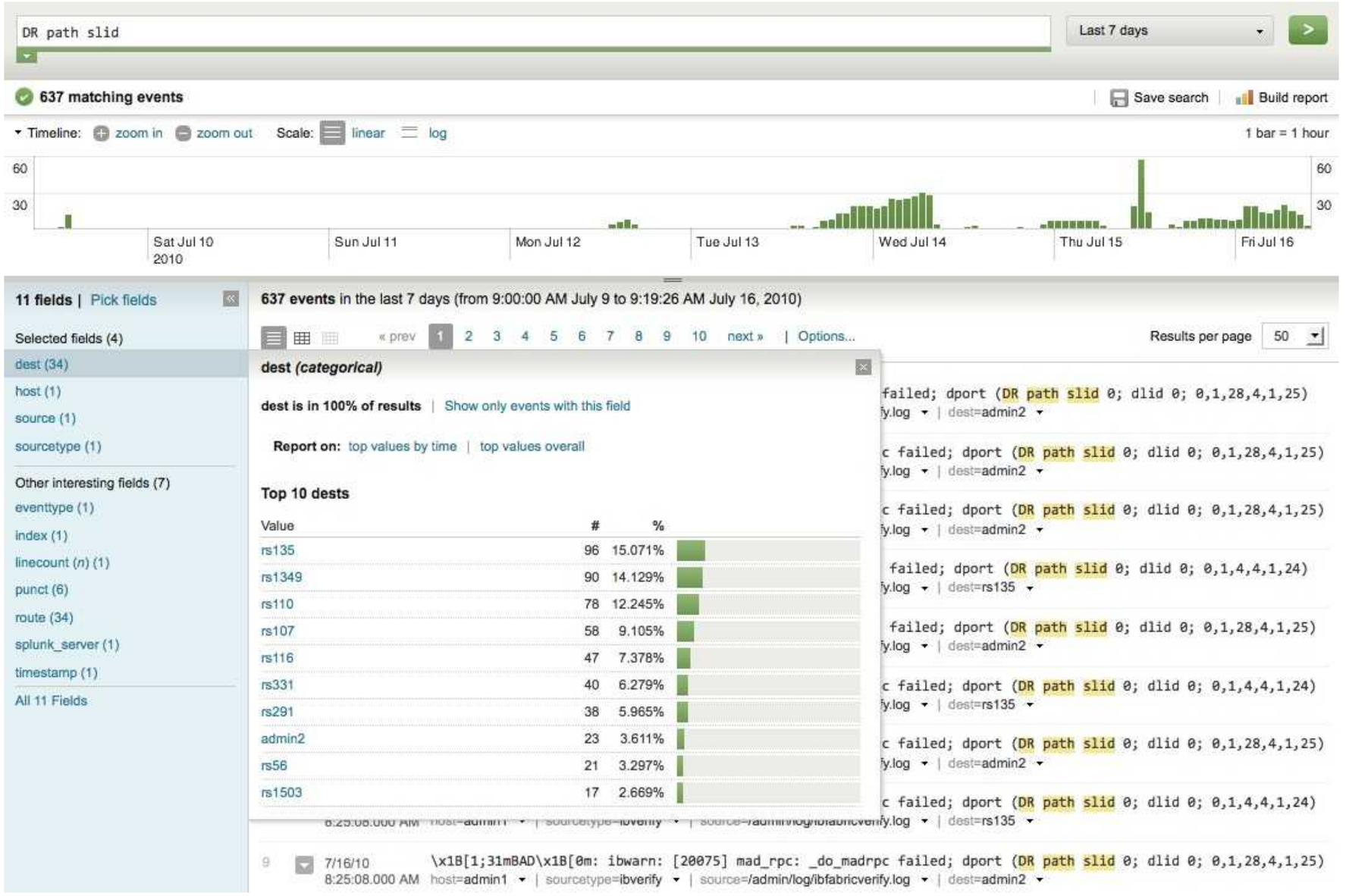
Step #3 : Edit props.conf

[ib]
EXTRACT-route = dlid \d; (?<route>[0-9,]+)
lookup_table = ib route OUTPUT dest
(dest is short for destination)

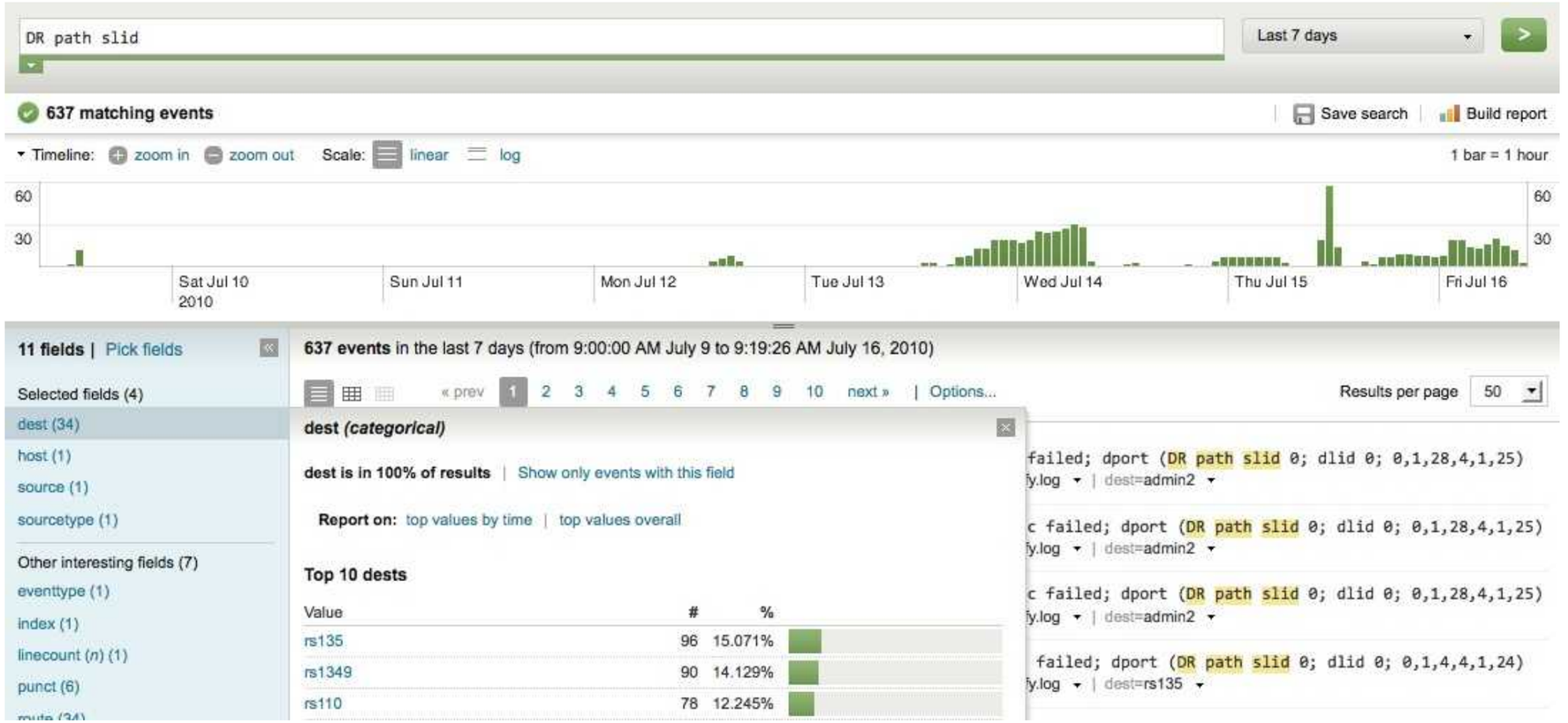
Step #4: Reload (or restart)

| extract reload=TRUE

splunk restart

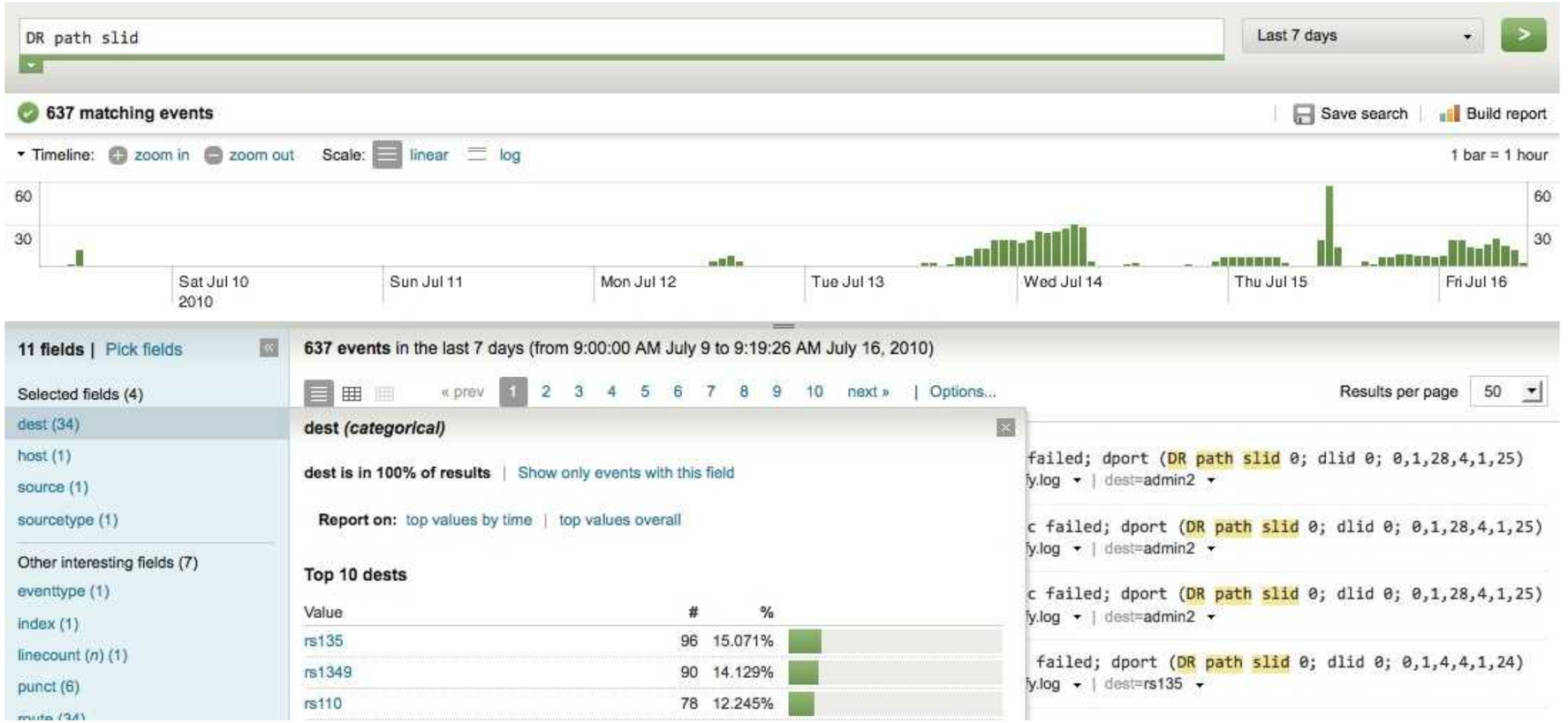


Easy as Pie! And just as tasty!



Or you could do it the old way:

$ tail -1000 /admin/log/infiniband_errors | grok_ibtrackerrors | grep ‘DR path slid’ | perl –ne ‘{/dlid \d; ([0-9,]+)/; $count{$1}++; END {map {print “$_ $count{$_}\n”} sort {$b<=>$a} keys %count;}’



Or you could do it the old way… NOT!!!

So we know WHERE the problem is, let's see the preceding five minutes of logs on that host…

Using a Subsearch

ibwarn: [17841] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,28,10,20)

- ☑ Step #1: Construct new query from search results (“inner search”)

```
DR path slid | eval start=_time-300 | eval end=_time+1 | eval query = " _time>” . start . " _time<" . end . “host=“ dest | fields + query | format
```

Aha - Linux OOM’d!
I wonder who’s process that is…?

query	search
	((_time>1279291208 _time<1279291509 host=rs135))

- ☑ Step #2: Execute it (“outer search”)

```
[search DR path slid | eval start=_time-300 | eval end=_time+1 | eval query = " _time>" . start . " _time<" . end . " " . dest| fields + query | format]
```

« prev 1 2 3 4 5 6 7 8 9 10 next » | Options...

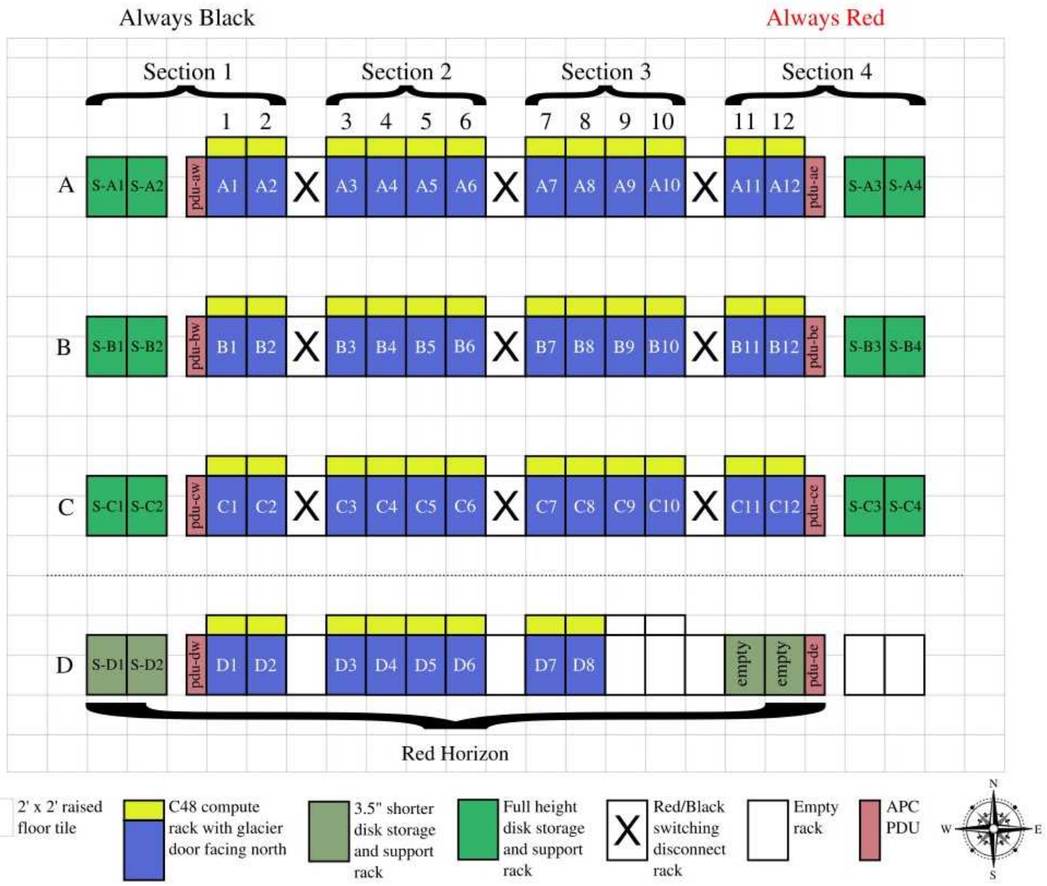
1	7/15/10 10:46:07.000 AM	Jul 15 10:46:07 rs135 Out of memory: Killed process 24400 (adagi host=rs135 | sourcetype=syslog | source=/var/log/messages
2	7/15/10 10:46:07.000 AM	Jul 15 10:46:07 rs135 0 pages swap cached host=rs135 | sourcetype=syslog | source=/var/log/messages
3	7/15/10 10:46:07.000 AM	Jul 15 10:46:07 rs135 74572 pages shared host=rs135 | sourcetype=syslog | source=/var/log/messages

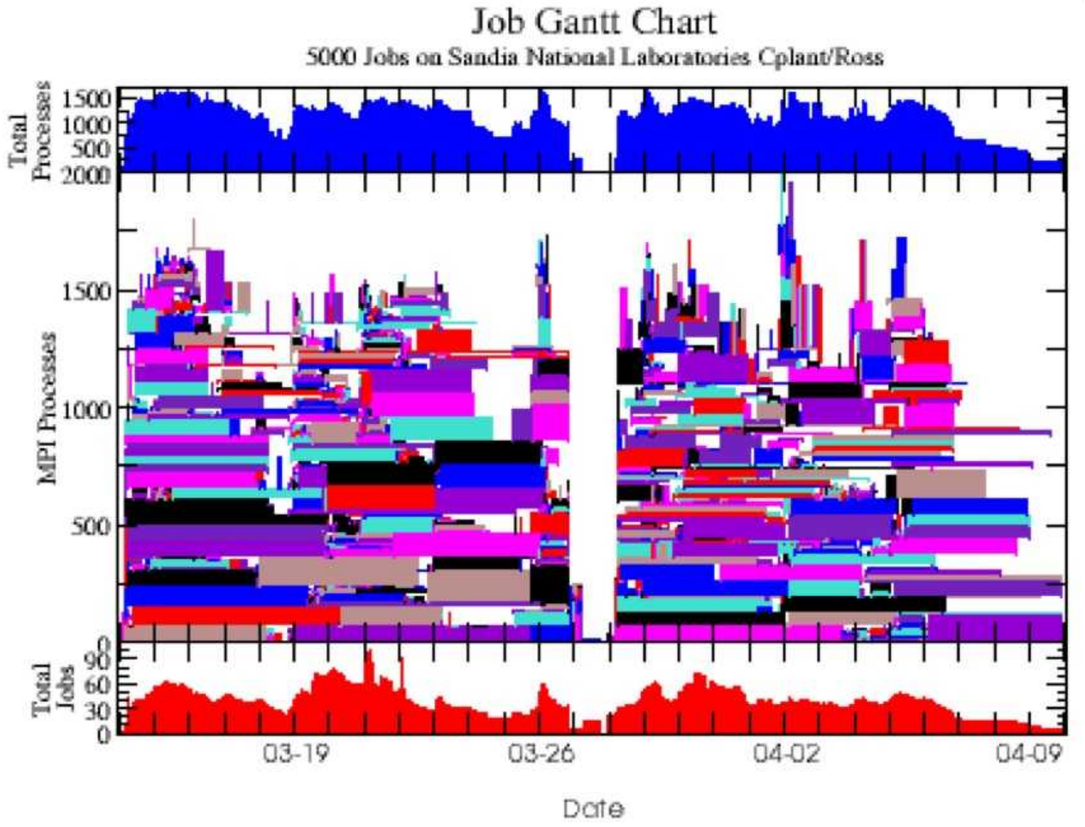
Jobs on a Supercomputer

36 racks

96 hosts per rack

10's of applications
100's of users
1000's of jobs, each involving
1-1000's hosts for 1s-10's days



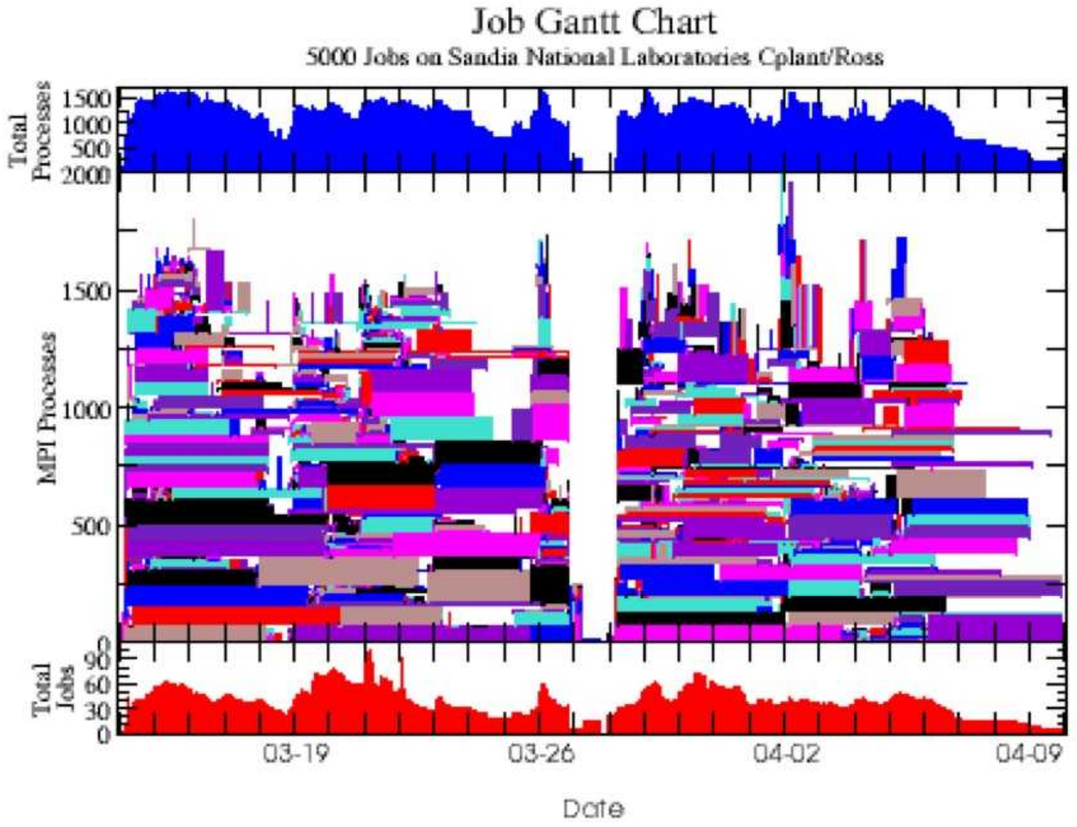


Jobs on a Supercomputer

10's of applications
100's of users
1000's of jobs, each involving
1-1000's hosts for 1s-10's days

Job = a certain set of hosts,
for a certain amount of time,
running a certain application,
for a certain user.

What job ran on which hosts, when?
Where are the corresponding logs?
Which user was running which application?
Is the user a victim or a cause?
What patterns emerge?



Time-dependent Lookups

1 7/15/10 10:46:07.000 AM Jul 15 10:46:07 rs135 Out of memory: Killed process 24400 (adagio_dp_opt_r).
host=rs135 | sourcetype=syslog | source=/var/log/messages

Step #1: Include a time field in job.csv

```
time,job,user,host
2010-07-15 10:11:59,102138,bart,rs135
2010-07-16 15:53:13,201259,fred,rs265
2010-07-16 15:55:25,201252,wilma,rs135
…
```

Step #2 : Edit transforms.conf

```
[job]
filename = job.csv
time_field = time
time_format = %F %T
```

Step #3 : Edit props.conf

```
[syslog]
lookup_table = job host OUTPUT job user
```

Step #4: Reload (or restart)

```
| extract reload=TRUE
```

splunk restart

1 7/15/10 10:46:07.000 AM Jul 15 10:46:07 rs135 Out of memory: Killed process 24400 (adagio_dp_opt_r).
host=rs135 | sourcetype=syslog | source=/var/log/messages | job=102138 | user=bart

Chaining lookups

- ☑ Chain multiple lookups together

```
DR path slid | lookup route host OUTPUT dest | lookup job host OUTPUT user
```

Jobs on a Supercomputer

☑ Meet sourcetype=moab

```
12:32:14 1279305134:3507555 job 700977 JOBCANCEL 16 128 jrstear jrstear 1800 Removed [nw:1] 1279303299 1279303302 1279303302
1279305128 - - - >= 0M >= 0M - 1279303299 128 0 -:- - FY103933 - - 0 0.00 slurm 1 0M 0M 0M 1279303299
2140000000
rs56,rs56,rs56,rs56,rs56,rs56,rs56,rs56,rs57,rs57,rs57,rs57,rs57,rs57,rs57,rs57,rs58,rs58,rs58,rs58,rs58,rs58,rs58,rs58,rs59,rs59,rs59,rs59,rs59,rs59,rs59,rs59,r
s60,rs60,rs60,rs60,rs60,rs60,rs60,rs60,rs51,rs51,rs51,rs51,rs51,rs51,rs51,rs51,rs52,rs52,rs52,rs52,rs52,rs52,rs52,rs52,rs53,rs53,rs53,rs53,rs53,rs53,rs53,rs53,rs
54,rs54,rs54,rs54,rs54,rs54,rs54,rs54,rs103,rs103,rs103,rs103,rs103,rs103,rs103,rs103,rs105,rs105,rs105,rs105,rs105,rs105,rs105,rs105,rs106,rs106,rs106,rs10
6,rs106,rs106,rs106,rs106,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs110,rs110,rs110,rs110,rs110,rs
110,rs110,rs110,rs111,rs111,rs111,rs111,rs111,rs111,rs111,rs111 slurm - - [DEFAULT] - - 0.00 - - - 0,NAccessPolicy=SINGLEJOB - -
```

☑ Configure props.conf to set these fields:

```
job=700977
user=jrstear
start=1279303302
end=1279305128
nodes=rs56,rs56,…rs57… … …rs54…rs106…
```

☑ Cleanup nodes (multivalue) field

```
makemv delim="," nodes | mvexpand nodes |
    dedup nodes


nodes={rs56,rs57,rs58,rs59,rs60,rs51,…rs111}
```

Writing a Macro

12:32:14 1279305134:3507555 job 700977 JOBCANCEL 16 128 jrstear jrstear 1800 Removed [nw:1] 1279303299 1279303302 1279303302 1279305128 - - - >= 0M >= 0M - 1279303299 128 0 -:- - FY103933 - - 0 0.00 slurm 1 0M 0M 0M 1279303299 2140000000
rs56,rs56,rs56,rs56,rs56,rs56,rs56,rs56,rs57,rs57,rs57,rs57,rs57,rs57,rs57,rs57,rs58,rs58,rs58,rs58,rs58,rs58,rs58,rs58,rs59,rs59,rs59,rs59,rs59,rs59,rs59,rs59,rs60,rs60,rs60,rs60,rs60,rs60,rs60,rs60,rs51,rs51,rs51,rs51,rs51,rs51,rs51,rs51,rs52,rs52,rs52,rs52,rs52,rs52,rs52,rs52,rs53,rs53,rs53,rs53,rs53,rs53,rs53,rs53,rs54,rs54,rs54,rs54,rs54,rs54,rs54,rs54,rs103,rs103,rs103,rs103,rs103,rs103,rs103,rs103,rs105,rs105,rs105,rs105,rs105,rs105,rs105,rs105,rs106,rs106,rs106,rs106,rs106,rs106,rs106,rs106,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs110,rs110,rs110,rs110,rs110,rs110,rs110,rs110,rs111,rs111,rs111,rs111,rs111,rs111,rs111,rs111 slurm - - [DEFAULT] - - 0.00 - - - 0,NAccessPolicy=SINGLEJOB - -

☑ Step#1: Write your search

```
[search sourcetype=moab job=700977 | makemv delim="," nodes | mvexpand nodes | dedup nodes | eval
    query = " _time>=" . start . " _time<= " . end .  " " . nodes | fields + query | format maxresults=1000]
```

Which involves a subsearch in this case:

query	search
	((_time>=1279303302 _time<= 1279305128 rs56) OR (_time>=1279303302 _time<= 1279305128 rs57) OR (_time>=1279303302 _time<= 1279305128 rs58) OR (_tim

((time>start time<end node1) OR (time>start time<end node2)…) for all nodes={rs56,…rs111}

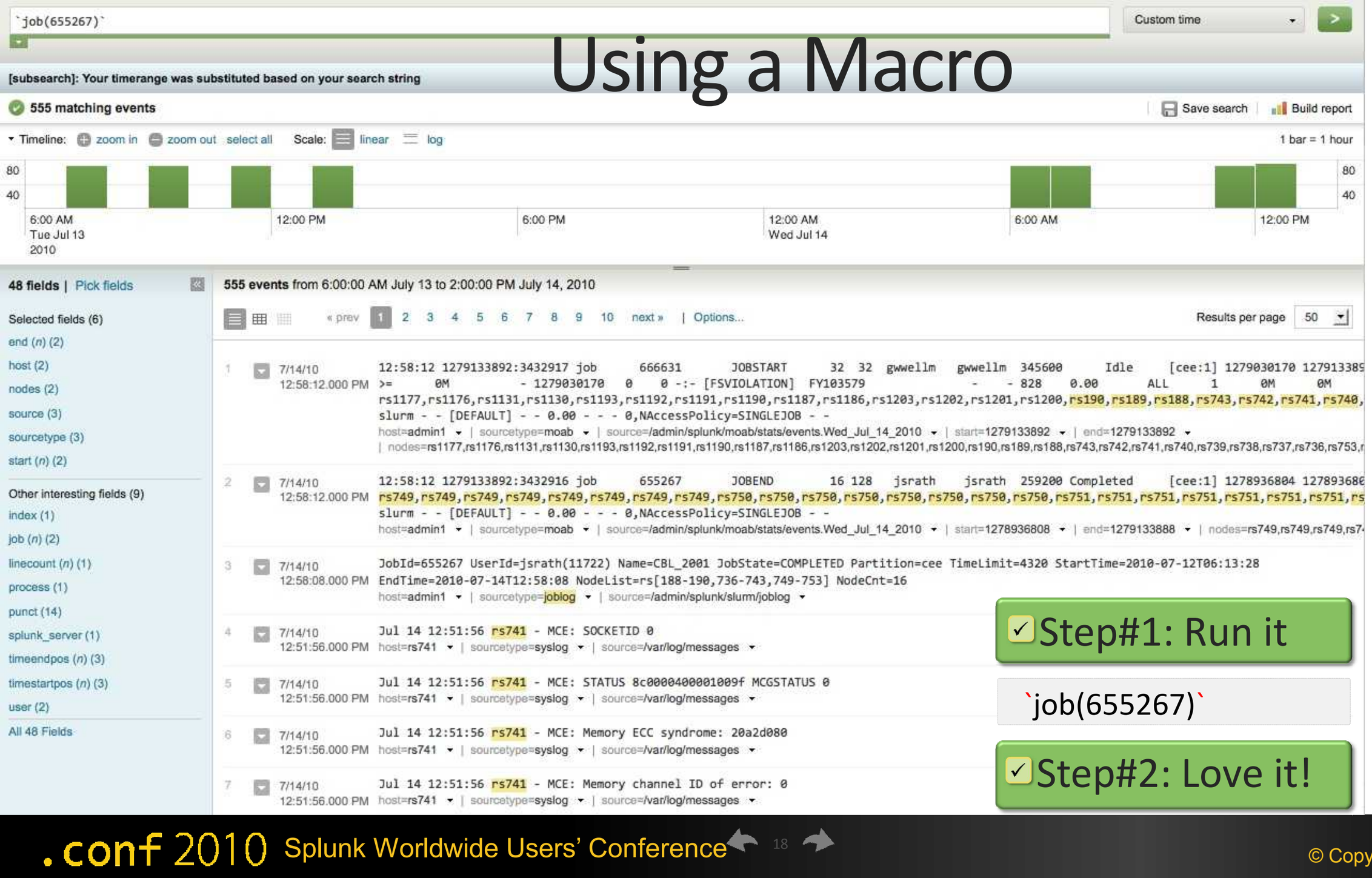
Writing a Macro

12:32:14 1279305134:3507555 job 700977 JOBCANCEL 16 128 jrstear jrstear 1800 Removed [nw:1] 1279303299 1279303302 1279303302 1279305128 - - - >= 0M >= 0M - 1279303299 128 0 -:- - FY103933 - - 0 0.00 slurm 1 0M 0M 0M 1279303299 2140000000
rs56,rs56,rs56,rs56,rs56,rs56,rs56,rs56,rs57,rs57,rs57,rs57,rs57,rs57,rs57,rs57,rs58,rs58,rs58,rs58,rs58,rs58,rs58,rs58,rs59,rs59,rs59,rs59,rs59,rs59,rs59,rs59,rs60,rs60,rs60,rs60,rs60,rs60,rs60,rs60,rs51,rs51,rs51,rs51,rs51,rs51,rs51,rs51,rs52,rs52,rs52,rs52,rs52,rs52,rs52,rs52,rs53,rs53,rs53,rs53,rs53,rs53,rs53,rs53,rs54,rs54,rs54,rs54,rs54,rs54,rs54,rs54,rs103,rs103,rs103,rs103,rs103,rs103,rs103,rs103,rs105,rs105,rs105,rs105,rs105,rs105,rs105,rs105,rs106,rs106,rs106,rs106,rs106,rs106,rs106,rs106,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs110,rs110,rs110,rs110,rs110,rs110,rs110,rs110,rs111,rs111,rs111,rs111,rs111,rs111,rs111,rs111 slurm - - [DEFAULT] - - 0.00 - - - 0,NAccessPolicy=SINGLEJOB - -

☑ Step#2: Make it a macro (macros.conf)

```
[job(1)]
args = jobid
definition = [search sourcetype=moab job=$jobid$| makemv delim="," nodes | mvexpand nodes | dedup
    nodes | eval query = " _time>=" . start . " _time<= " . end .  " " . nodes | fields + query | format
    maxresults=1000]
```

Using a Macro



☑ Step#1: Run it

`job(655267)`

☑ Step#2: Love it!

Adding a Field Action

splunk> Manager » Fields » Workflow actions » job

Label

`job($job$)`

Enter the label that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : $ticketnum$'.

Apply only to the following fields (optional)

job

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it. When fields are specified, the workflow action only appears in the field menus for those fields; otherwise it appears in all field menus.

Apply only to the following event types (optional)

Specify a comma-separated list of event types that an event must be associated with for the workflow action to apply to it.

Show action in

Both

Action type

search

Search configuration

Search string

`job($job$)`

Enter the search for this action. Optionally, specify fields as $fieldname$, e.g. sourcetype=rails controller=$controller$ error=.*

Run in app

Choose an app for the search to run in. Defaults to the current app.

Open in view (optional)

Enter the name of a view for the search to open in. Defaults to the current view.

Run search in

New window

Time range

Earliest time (optional) Latest time (optional)

☑ Use the same time range as the search that created the field listing

Cancel Save

Done

11 7/18/10 8:26:48.000 AM Jul 18 08:26:48 rs957 Out of memory: Killed process 1933 (alegra_3D_opt_r). host=rs957 | sourcetype=syslog | source=/var/log/messages | user=bart | job=677690

12 7/18/10 8:24:28.000 AM Jul 18 08:24:28 rs386 Out of memory: Killed process 20032 (alegra_3D_opt_r). host=rs386 | sourcetype=syslog | source=/var/log/messages | user=bart | job=677690

13 7/18/10 8:24:28.000 AM Jul 18 08:24:28 rs953 Out of memory: Killed process 13593 (alegra_3D_opt_r). host=rs953 | sourcetype=syslog | source=/var/log/messages

14 7/18/10 8:24:21.000 AM Jul 18 08:24:21 rs955 Out of memory: Killed process 7076 (alegra_3D_opt_r). host=rs955 | sourcetype=syslog | source=/var/log/messages | user=fred | job=678062

15 7/18/10 8:24:20.000 AM Jul 18 08:24:20 rs955 Out of memory: Killed process 7075 (alegra_3D_opt_r). host=rs955 | sourcetype=syslog | source=/var/log/messages | user=fred | job=678062

16 7/18/10 8:24:20.000 AM Jul 18 08:24:20 rs954 Out of memory: Killed process 13212 (alegra_3D_opt_r). host=rs954 | sourcetype=syslog | source=/var/log/messages | user=fred | job=678062

17 7/18/10 8:24:19.000 AM Jul 18 08:24:19 rs1531 Out of memory: Killed process 5799 (alegra_3D_opt_r). host=rs1531 | sourcetype=syslog | source=/var/log/messages | user=fred | job=678062

18 7/18/10 8:23:35.000 AM Jul 18 08:23:35 rs818 - MCE: CPU 3 BANK 8 TSC 8ffd6793b6f14 host=rs818 | sourcetype=syslog | source=/var/log/messages | user=wilma | job=535537

19 7/18/10 8:23:35.000 AM Jul 18 08:23:35 rs818 - MCE: CPU 2 BANK 8 TSC 8ffd6793b6e80 host=rs818 | sourcetype=syslog | source=/var/log/messages | user=wilma | job=535537

20 7/18/10 8:23:35.000 AM Jul 18 08:23:35 rs818 - MCE: CPU 1 BANK 8 TSC 8ffd6793b6d14 host=rs818 | sourcetype=syslog | source=/var/log/messages | user=wilma | job=535537

Tag job=678062
Report on field
`job(678062)`

Putting it all together: Job Dashboard

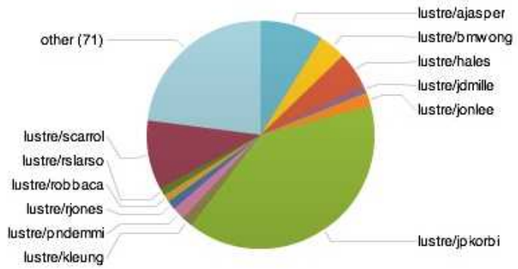
splunk> Search

Logged in as jrstear | App | Manager | Jobs | Logout

Summary | Search | Status | Views | Searches & Reports | Help | About

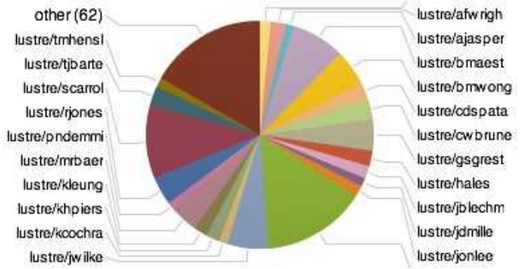
Alerts in Jobs | Actions

Number of jobs per type/user refreshed: today at 8:01:02 AM.



View results

Number of nodes per type/user refreshed: today at 8:01:02 AM.

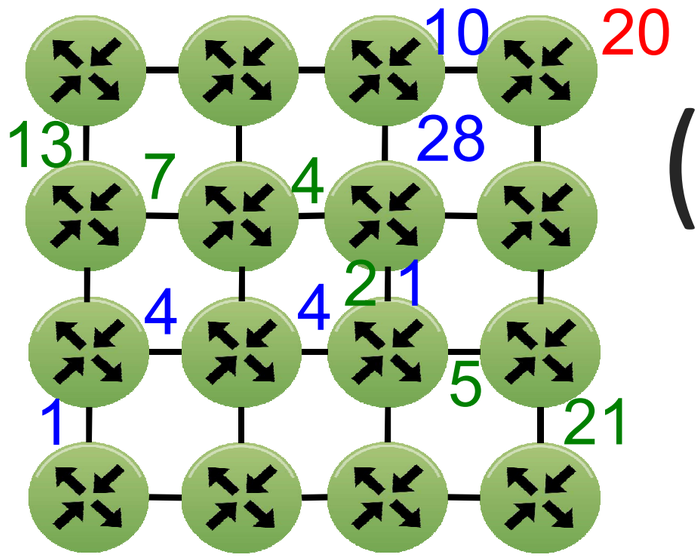


View results

Number of alerts per type, user, job refreshed: today at 8:01:02 AM.

	eventtype	user	job	count
1	lustre	kleung	714750	684
2	lustre	kleung	714749	12
3	lustre	afwrigh	714748	5118
4	lustre	kleung	714747	520
5	lustre	cdspata	714746	1076
6	lustre	cdspata	714745	1068
7	lustre	cdspata	714744	1658
8	lustre	cdspata	714743	1674
9	lustre	cdspata	714742	1708
10	lustre	hxm	714741	46
11	lustre	hxm	714740	2
12	lustre	dakota	714739	20
13	lustre	dakota	714738	20
14	lustre	pndemmi	714706	552
15	lustre	pndemmi	714705	558
16	lustre	kleung	714704	520

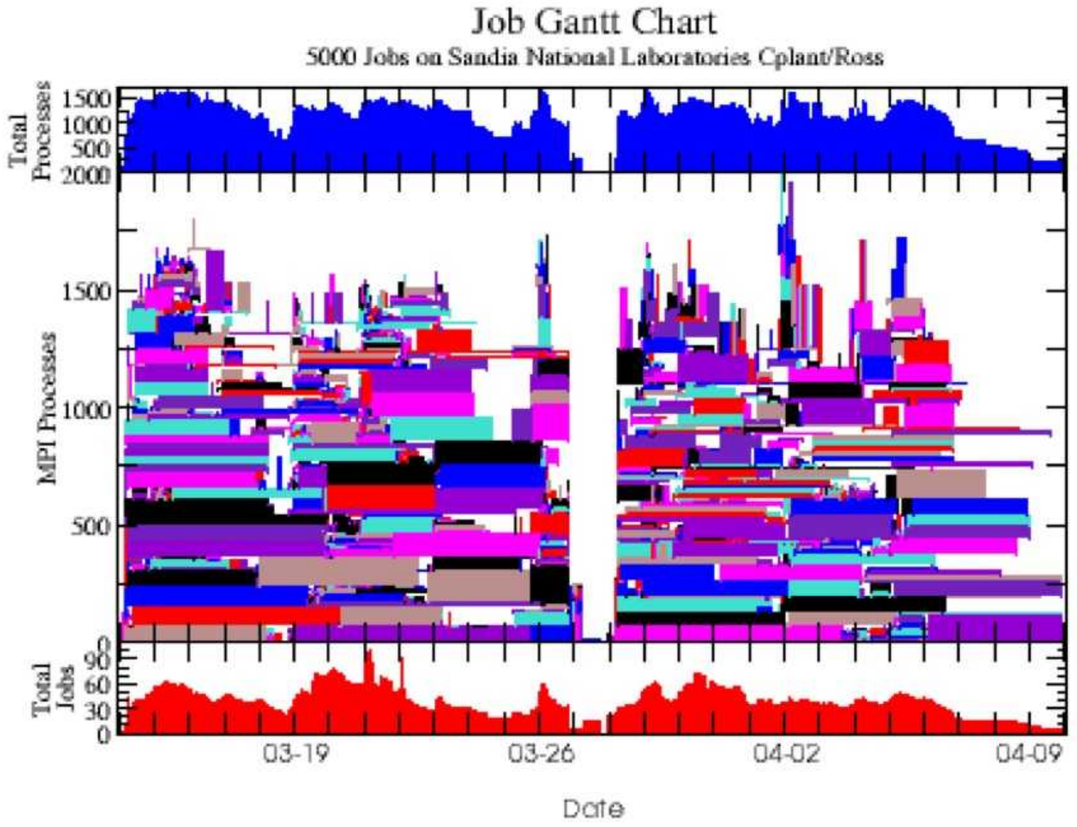
Future Work (Shared Components)



ibwarn: [17841] mad_rpc: _do_madrpc failed; dport
(DR path slid 0; dlid 0; 0,1,4,4,1,28,10,20)

We assumed that the problem is at the destination.
What if it is instead somewhere along the path?

Infer the root cause among shared components,
given multiple indirect symptoms.



splunk>

THE END

Extra Slides Follow

Jon Stearley

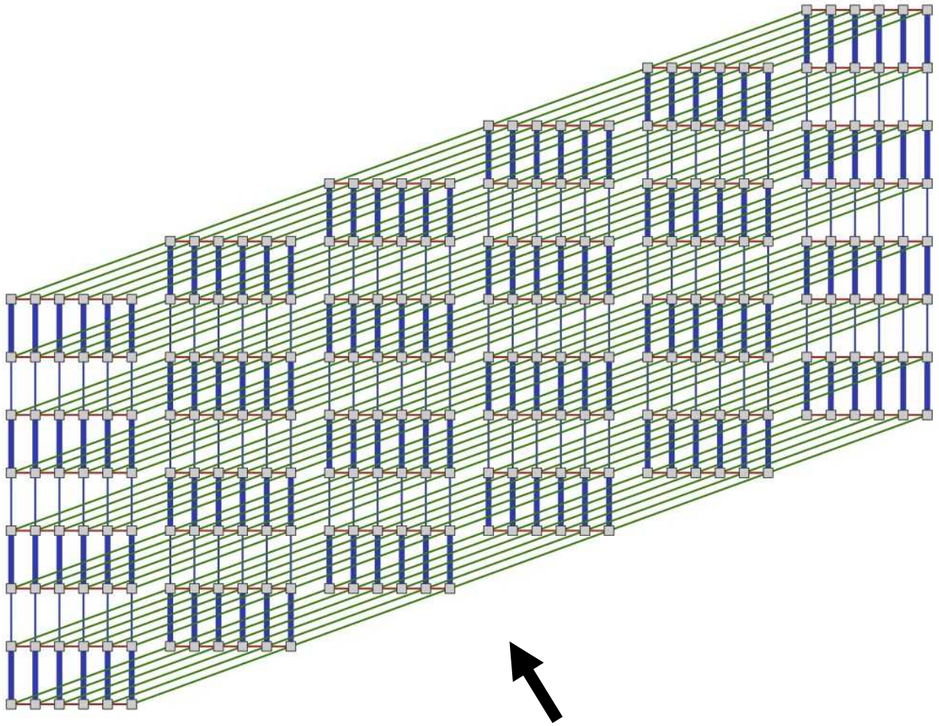
Sandia National Laboratories

jrstear@sandia.gov

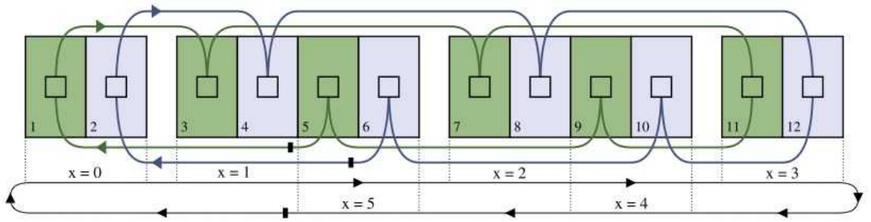
Enriching your data with Lookups and more

Sandia National Labs is Splunking logs from a 2300-node supercomputer (about 5000 logging components). They make extensive use of lookups (up to several chained lookups) to associate log messages of interest with user jobs and specific nodes (mostly via tables and charts). They also use macros and subsearches to isolate time windows around faults. Several features in Splunk reduce manual effort from hours to seconds. Jon Stearley did it, and you can too! Join this customer use case to learn easy ways to power up your Splunk instance and save loads of time.

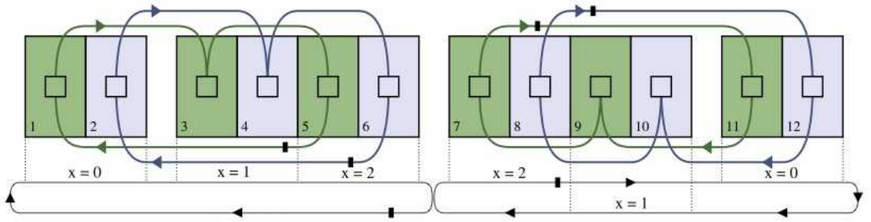
Supercomputer Network



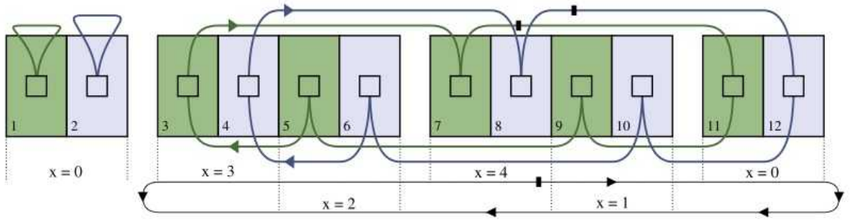
6X6X8 network of switches,
wired together like this



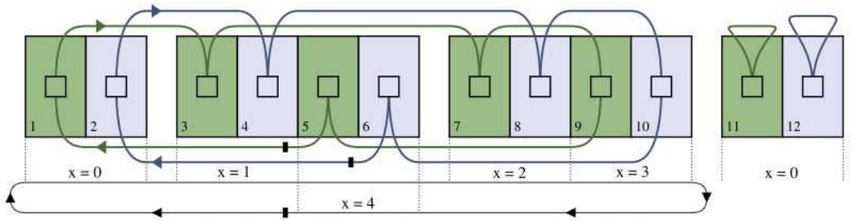
(a) Swing A: X Dimension Pattern A – Full Black Connectivity



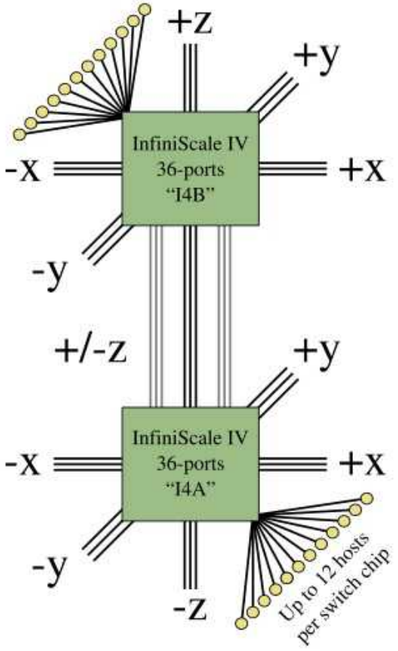
(b) Swing B: X Dimension Pattern B – 50/50 Split



(c) Swing C: X Dimension Pattern C – 1/6 to 5/6 Split



(d) Swing D: X Dimension Pattern D – 5/6 to 1/6 Split



Each switch wired to
24 hosts like this

Machine-generated IT Data Contains A Categorical Record of Activity and Behavior

Logfiles | Configs | Messages | Traps Alerts | Metrics | Scripts | Changes | Tickets

Windows
- Registry
- Event logs
- File system
- sysinternals

Linux/Unix
- Configurations
- syslog
- File system
- ps, iostat, top

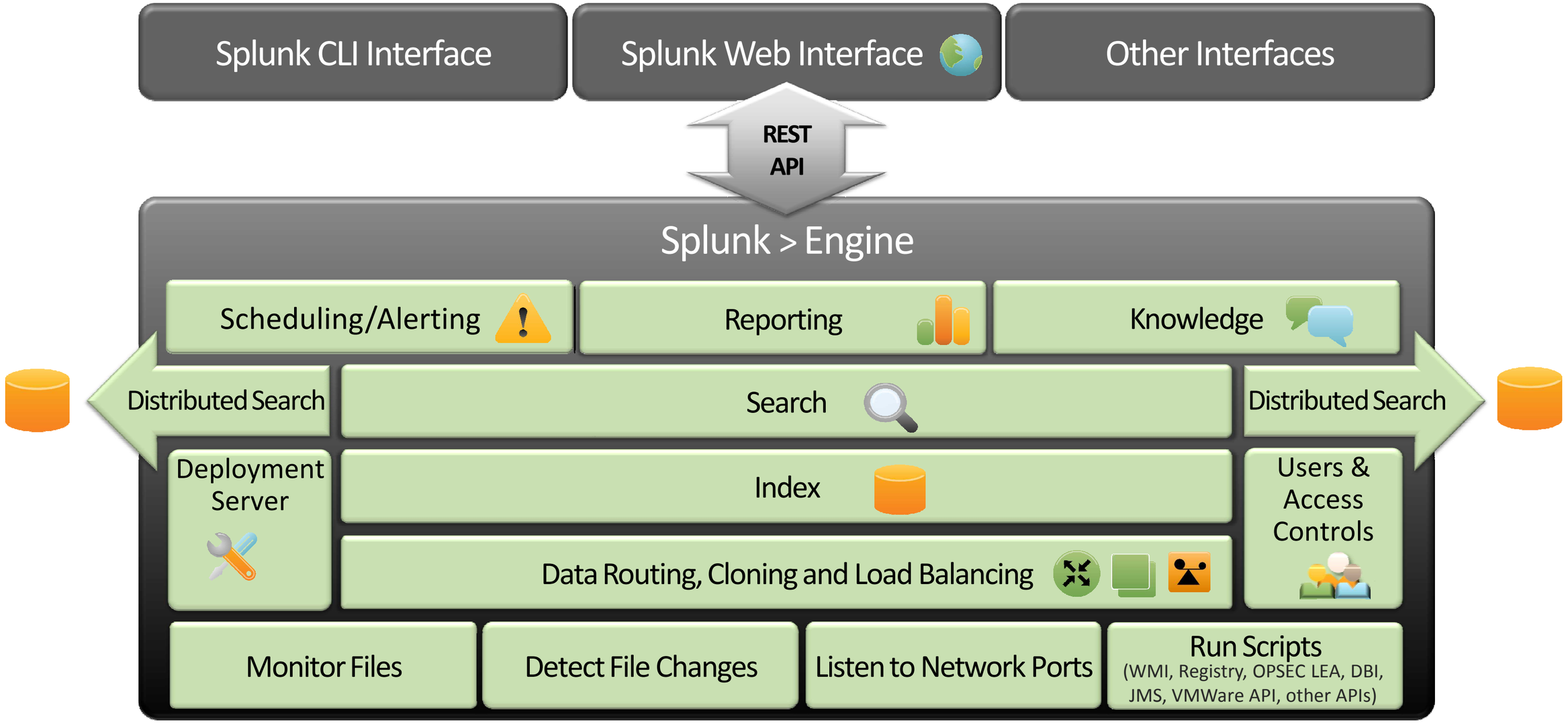
Virtualization
- Hypervisor
- Guest OS
- Guest Apps

Applications
- Web logs
- Log4J, JMS, JMX
- .NET events
- Code and scripts

Databases
- Configurations
- Audit/query logs
- Tables
- Schemas

Networking
- Configurations
- syslog
- SNMP
- netflow

Splunk Architecture



Graphics for Description

Table Slide for Comparisons

Subhead goes here.

Subject Title	Comparison #1	Splunk
Subject #1	Facts supporting	Facts supporting
Subject #2	Facts supporting	Facts supporting
Subject #3	Facts supporting	Facts supporting
Subject #4	Facts supporting	Facts supporting

Background Screen (place images on top)

- Bullet #1

- Bullet #2

Bulleted List

- Bullet #1
- Bullet #2
- Bullet #3
- Bullet #4
- Bullet #5
- Bullet #6
- Bullet #7