Enriching your data with Lookups and more
Or… Splunking a Supercomputer

.conf 2010

Splunk Worldwide Users' Conference

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

Sandia National Laboratories

Jon Stearley

Enriching your data with Lookups and more

Or… Splunking a Supercomputer

Jon Stearley

Sandia National Laboratories

jrstear@sandia.gov

© Copyright Splunk 2010

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

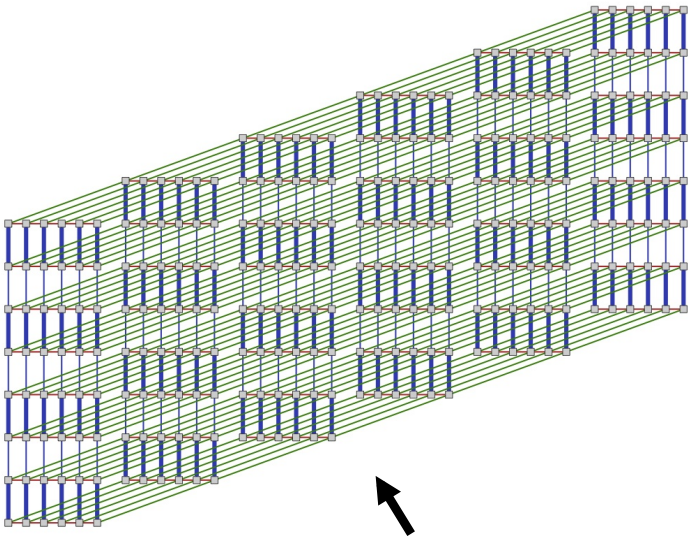
and

Bart

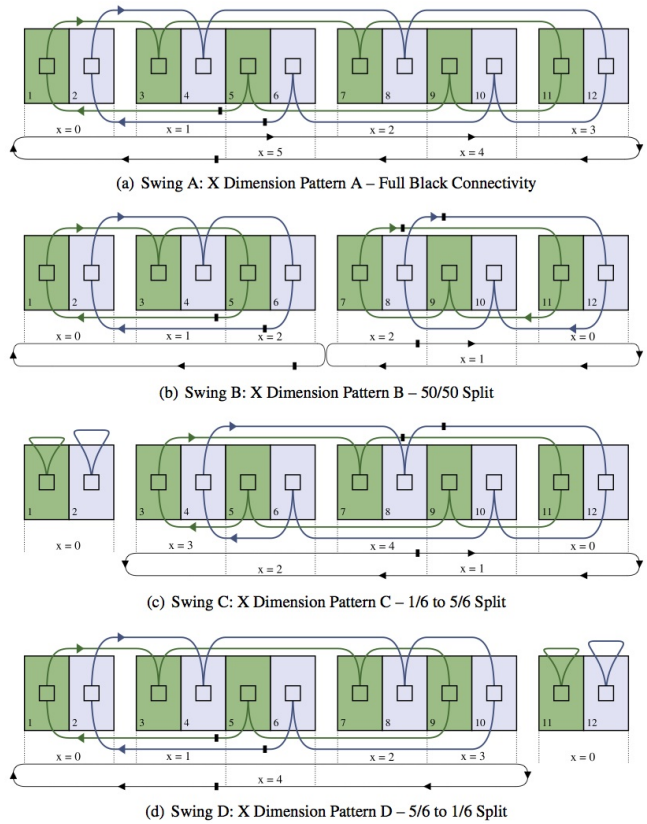
the user

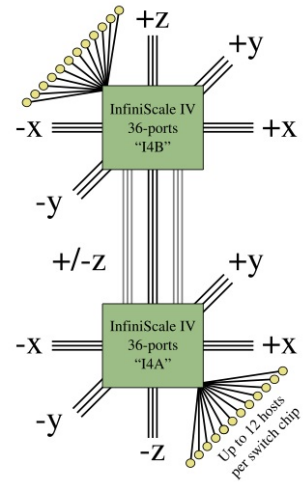
© Copyright Splunk 2010

Supercomputer Network



6X6X8 network of switches,
wired together like this



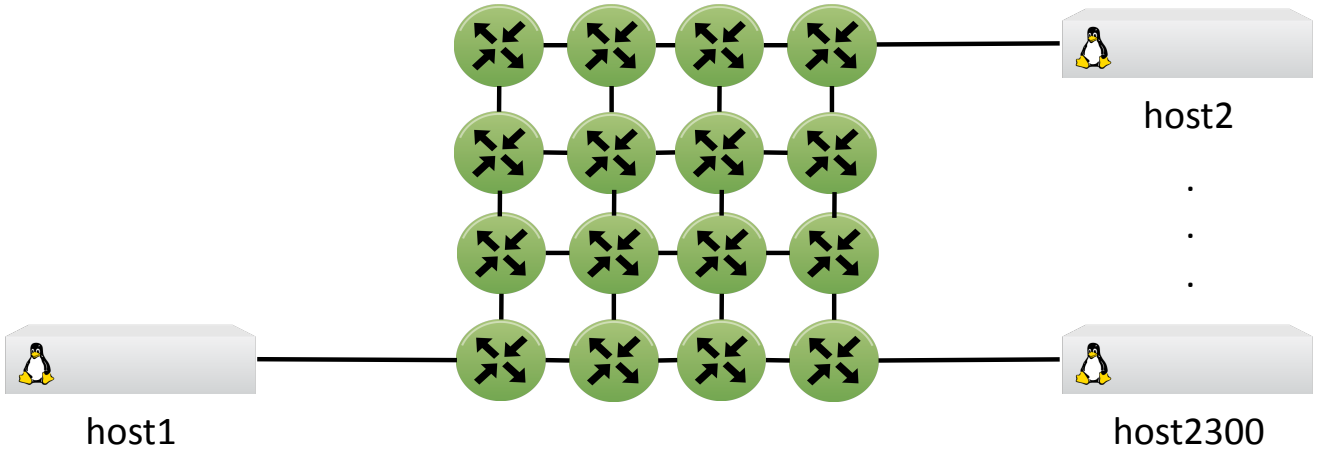


Each switch wired to
24 hosts like this

© Copyright Splunk 2010

Lookups: host1 network problem

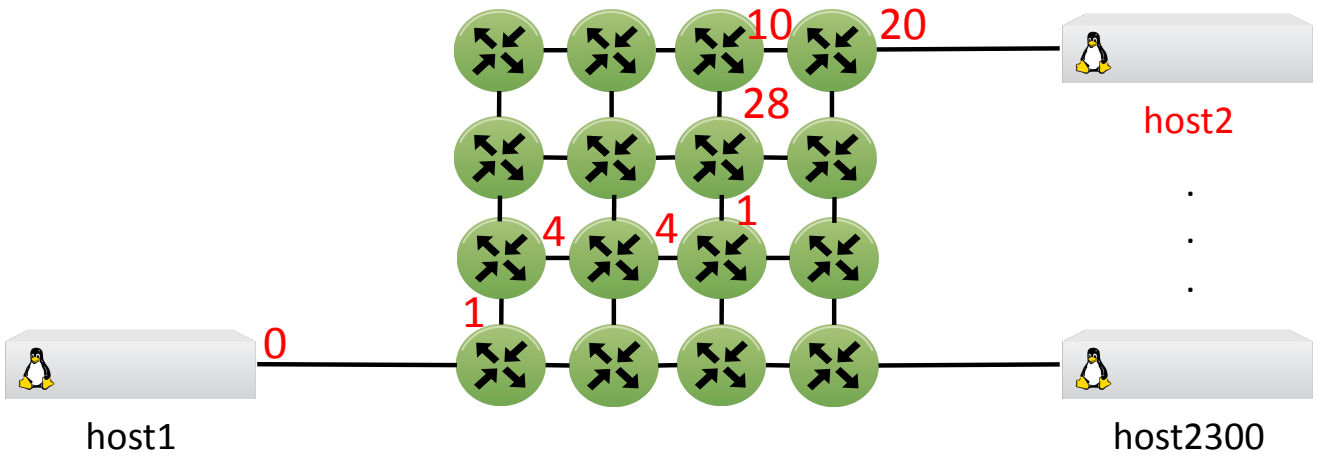
ibwarn: [17841] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,28,10,20)



© Copyright Splunk 2010

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)



© Copyright Splunk 2010

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, dest          # dest is short for 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
```


© Copyright Splunk 2010

DR path slid

Last 7 days

637 matching events

Save search | Build report

Timeline: zoom in zoom out Scale: linear log 1 bar = 1 hour

Sat Jul 10 2010 | Sun Jul 11 | Mon Jul 12 | Tue Jul 13 | Wed Jul 14 | Thu Jul 15 | Fri Jul 16

11 fields | Pick fields

Selected fields (4)
- dest (34)
- host (1)
- source (1)
- sourcetype (1)

Other interesting fields (7)
- eventtype (1)
- index (1)
- linecount (n) (1)
- punct (6)
- route (34)
- splunk_server (1)
- timestamp (1)

All 11 Fields

637 events in the last 7 days (from 9:00:00 AM July 9 to 9:19:26 AM July 16, 2010)

« prev 1 2 3 4 5 6 7 8 9 10 next » | Options... Results per page 50

dest (categorical)

dest is in 100% of results | Show only events with this field

Report on: top values by time | top values overall

Top 10 dests

Value	#	%
rs135	96	15.071%
rs1349	90	14.129%
rs110	78	12.245%
rs107	58	9.105%
rs116	47	7.378%
rs331	40	6.279%
rs291	38	5.965%
admin2	23	3.611%
rs56	21	3.297%
rs1503	17	2.669%

failed; dport (DR path slid 0; dlid 0; 0,1,28,4,1,25)
y.log | dest=admin2

c failed; dport (DR path slid 0; dlid 0; 0,1,28,4,1,25)
y.log | dest=admin2

c failed; dport (DR path slid 0; dlid 0; 0,1,28,4,1,25)
y.log | dest=admin2

failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,24)
y.log | dest=rs135

failed; dport (DR path slid 0; dlid 0; 0,1,28,4,1,25)
y.log | dest=admin2

c failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,24)
y.log | dest=rs135

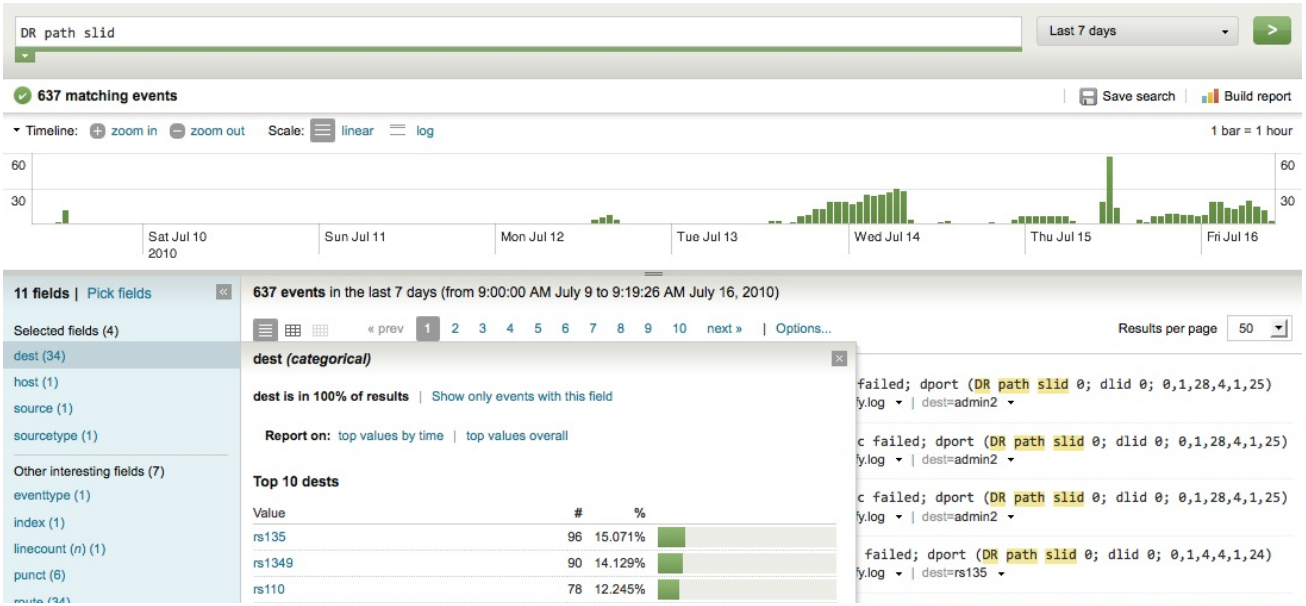
c failed; dport (DR path slid 0; dlid 0; 0,1,28,4,1,25)
y.log | dest=admin2

c failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,24)
y.log | dest=rs135

9 7/16/10 8:25:08.000 AM \x1B[1;31mBAD\x1B[0m: ibwarn: [20075] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,28,4,1,25)
host=admin1 | sourcetype=ibverify | source=/admin/log/ibfabricverify.log | dest=admin2

Easy as Pie! And just as tasty!

© Copyright Splunk 2010



Or you could do it the old way:

```
$ tail -1000f /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;}'
```


© Copyright Splunk 2010

DR path slid

Last 7 days

637 matching events

Save search | Build report

Timeline: zoom in zoom out Scale: linear log 1 bar = 1 hour

Sat Jul 10 2010 | Sun Jul 11 | Mon Jul 12 | Tue Jul 13 | Wed Jul 14 | Thu Jul 15 | Fri Jul 16

11 fields | Pick fields

Selected fields (4)
- dest (34)
- host (1)
- source (1)
- sourcetype (1)

Other interesting fields (7)
- eventtype (1)
- index (1)
- linecount (n) (1)
- punct (6)

637 events in the last 7 days (from 9:00:00 AM July 9 to 9:19:26 AM July 16, 2010)

« prev 1 2 3 4 5 6 7 8 9 10 next » | Options... Results per page 50

dest (categorical)

dest is in 100% of results | Show only events with this field

Report on: top values by time | top values overall

Top 10 dests

Value	#	%
rs135	96	15.071%
rs1349	90	14.129%
rs110	78	12.245%

failed; dport (DR path slid 0; dlid 0; 0,1,28,4,1,25)
y.log | dest=admin2

c failed; dport (DR path slid 0; dlid 0; 0,1,28,4,1,25)
y.log | dest=admin2

c failed; dport (DR path slid 0; dlid 0; 0,1,28,4,1,25)
y.log | dest=admin2

failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,24)
y.log | dest=rs135

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…

© Copyright Splunk 2010

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]
```

« 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 (adagio 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

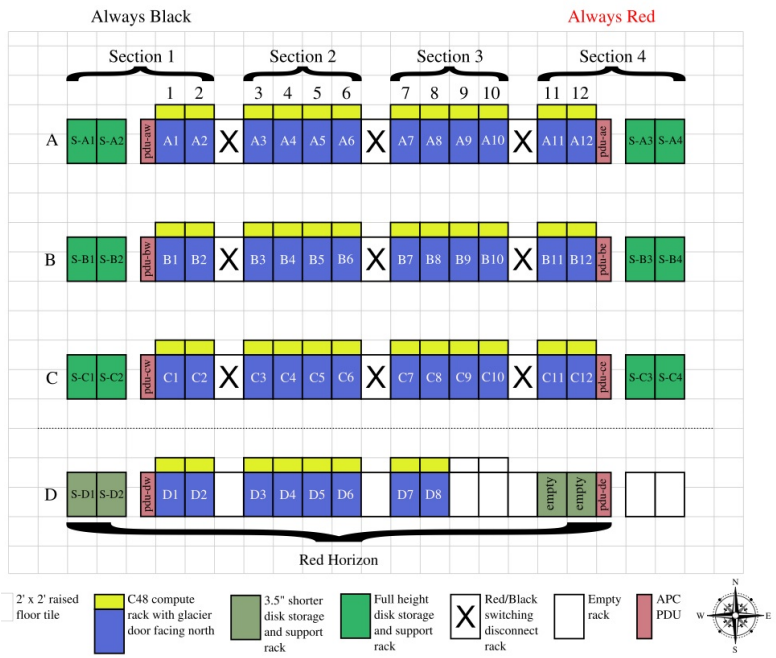
© Copyright Splunk 2010

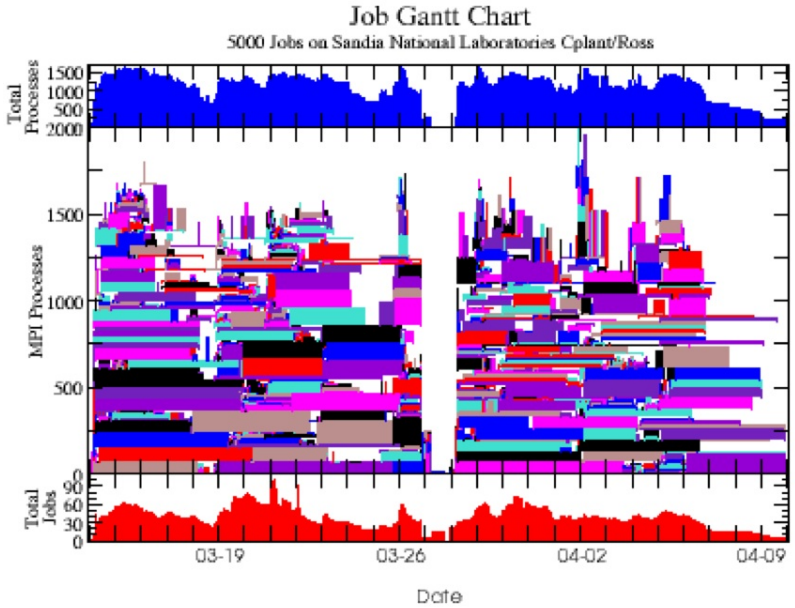
Jobs on a Supercomputer

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





© Copyright Splunk 2010

Jobs on a Supercomputer

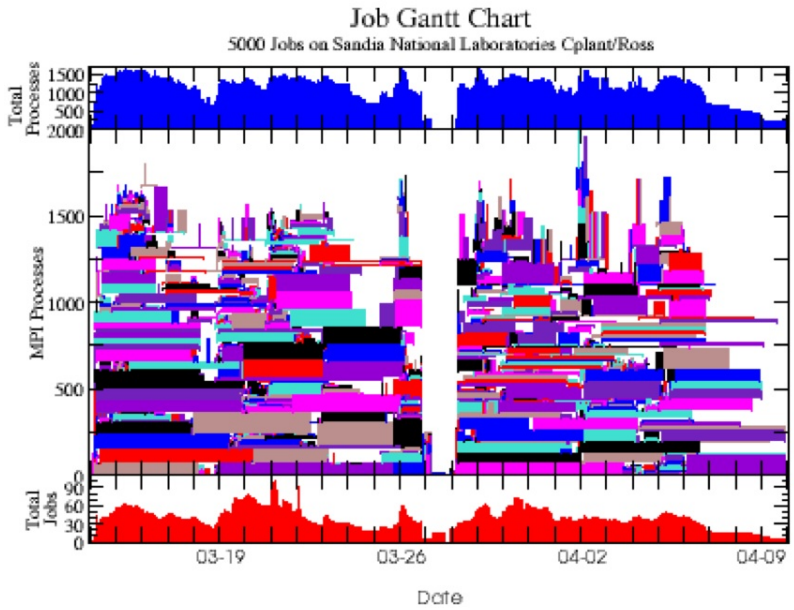
Job = a certain set of hosts,

for a certain amount of time,

running a certain application,

for a certain user.

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



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?

© Copyright Splunk 2010

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
```

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

© Copyright Splunk 2010

Chaining lookups

- ☑ Chain multiple lookups together

```
DR path slid | lookup ib route OUTPUT dest | lookup job host as dest OUTPUT user
  | stats count by user
```

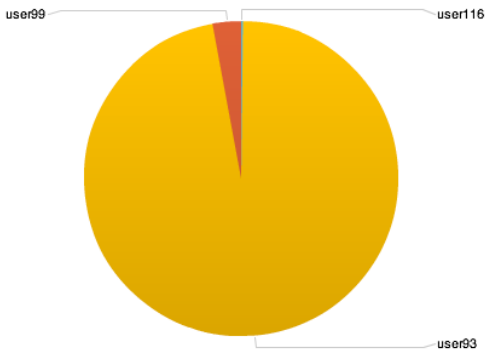
Ingredients → **Table** → **Pie**

4,740 events in the last 24 hours (from 1:00:00 PM July 25 to 1:42:12 PM July 26, 2010)

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

1	7/26/10 12:45:01.000 PM	\x1B[1;31mBAD\x1B[0m: ibwarn: [27198] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,1,28,4,1,28,18) host=localhost | sourcetype=ibverify | source=/Users/jrstear/data/splunk/demo/data/ibfabricverify
2	7/26/10 12:35:02.000 PM	\x1B[1;31mBAD\x1B[0m: ibwarn: [19819] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,1,28,4,1,28,18) host=localhost | sourcetype=ibverify | source=/Users/jrstear/data/splunk/demo/data/ibfabricverify
3	7/26/10 12:25:03.000 PM	\x1B[1;31mBAD\x1B[0m: ibwarn: [12526] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,1,28,4,1,28,18) host=localhost | sourcetype=ibverify | source=/Users/jrstear/data/splunk/demo/data/ibfabricverify
4	7/26/10 12:15:01.000 PM	\x1B[1;31mBAD\x1B[0m: ibwarn: [4101] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,1,28,4,1,28,18) host=localhost | sourcetype=ibverify | source=/Users/jrstear/data/splunk/demo/data/ibfabricverify
5	7/26/10 11:55:01.000 AM	\x1B[1;31mBAD\x1B[0m: ibwarn: [21753] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,13,4,28,4,1,4,28,1,17) host=localhost | sourcetype=ibverify | source=/Users/jrstear/data/splunk/demo/data/ibfabricverify
6	7/26/10 11:55:01.000 AM	\x1B[1;31mBAD\x1B[0m: ibwarn: [21753] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,10,7,28,7,1,7,28,1,17) host=localhost | sourcetype=ibverify | source=/Users/jrstear/data/splunk/demo/data/ibfabricverify
7	7/26/10 11:55:01.000 AM	\x1B[1;31mBAD\x1B[0m: ibwarn: [21753] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,7,7,1,28,7,1,10,7,27) host=localhost | sourcetype=ibverify | source=/Users/jrstear/data/splunk/demo/data/ibfabricverify
8	7/26/10 11:55:01.000 AM	\x1B[1;31mBAD\x1B[0m: ibwarn: [21753] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,7,7,1,28,7,1,10,7,17) host=localhost | sourcetype=ibverify | source=/Users/jrstear/data/splunk/demo/data/ibfabricverify
9	7/26/10 11:55:01.000 AM	\x1B[1;31mBAD\x1B[0m: ibwarn: [21753] mad_rpc: _do_madrpc failed; dport (DR path slid 0; dlid 0; 0,1,4,4,1,28,4,1,13,27) host=localhost | sourcetype=ibverify | source=/Users/jrstear/data/splunk/demo/data/ibfabricverify

	user	count
1	user93	4589
2	user99	138
3	user116	8



© Copyright Splunk 2010

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,rs
   59,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,rs
   106,rs106,rs106,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs110,rs11
   0,rs110,rs110,rs110,rs110,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}
```


© Copyright Splunk 2010

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,rs
   59,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,rs
   106,rs106,rs106,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs110,rs11
   0,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}

© Copyright Splunk 2010

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,rs
   59,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,rs
   106,rs106,rs106,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs107,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs109,rs110,rs11
   0,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]
```


© Copyright Splunk 2010

`job(655267)`

Custom time

[subsearch]: Your timerange was substituted based on your search string

555 matching events

Save search | Build report

Timeline: zoom in zoom out select all Scale: linear log 1 bar = 1 hour

6:00 AM Tue Jul 13 2010 | 12:00 PM | 6:00 PM | 12:00 AM Wed Jul 14 | 6:00 AM | 12:00 PM

48 fields | Pick fields

Selected fields (6)
- end (n) (2)
- host (2)
- nodes (2)
- source (3)
- sourcetype (3)
- start (n) (2)

Other interesting fields (9)
- index (1)
- job (n) (2)
- linecount (n) (1)
- process (1)
- punct (14)
- splunk_server (1)
- timeendpos (n) (3)
- timestartpos (n) (3)
- user (2)

All 48 Fields

555 events from 6:00:00 AM July 13 to 2:00:00 PM July 14, 2010

« prev 1 2 3 4 5 6 7 8 9 10 next » | Options... Results per page 50

1 7/14/10 12:58:12.000 PM
```
12:58:12 1279133892:3432917 job 666631 JOBSTART 32 32 jrstear jrstear 345600 Idle [cee:1] 1279030170 127913389
>= 0M - 1279030170 0 0 -:- [FSVIOLATION] FY103579 - - 828 0.00 ALL 1 0M 0M
rs1177,rs1176,rs1131,rs1130,rs1193,rs1192,rs1191,rs1190,rs1187,rs1186,rs1203,rs1202,rs1201,rs1200,rs190,rs189,rs188,rs743,rs742,rs741,rs740,
slurm - - [DEFAULT] - - 0.00 - - - 0,NAccessPolicy=SINGLEJOB - -
host=admin1 | sourcetype=moab | source=/admin/splunk/moab/stats/events.Wed_Jul_14_2010 | start=1279133892 | end=1279133892
| nodes=rs1177,rs1176,rs1131,rs1130,rs1193,rs1192,rs1191,rs1190,rs1187,rs1186,rs1203,rs1202,rs1201,rs1200,rs190,rs189,rs188,rs743,rs742,rs741,rs740,rs739,rs738,rs737,rs736,rs753,r
```

2 7/14/10 12:58:12.000 PM
```
12:58:12 1279133892:3432916 job 655267 JOBEND 16 128 jrstear jrstear 259200 Completed [cee:1] 1278936804 12789368
rs749,rs749,rs749,rs749,rs749,rs749,rs749,rs749,rs750,rs750,rs750,rs750,rs750,rs750,rs750,rs750,rs751,rs751,rs751,rs751,rs751,rs751,rs751,rs
slurm - - [DEFAULT] - - 0.00 - - - 0,NAccessPolicy=SINGLEJOB - -
host=admin1 | sourcetype=moab | source=/admin/splunk/moab/stats/events.Wed_Jul_14_2010 | start=1278936808 | end=1279133888 | nodes=rs749,rs749,rs749,rs7
```

3 7/14/10 12:58:08.000 PM
```
JobId=655267 UserId=jsrath(11722) Name=CBL_2001 JobState=COMPLETED Partition=cee TimeLimit=4320 StartTime=2010-07-12T06:13:28
EndTime=2010-07-14T12:58:08 NodeList=rs[188-190,736-743,749-753] NodeCnt=16
host=admin1 | sourcetype=joblog | source=/admin/splunk/slurm/joblog
```

4 7/14/10 12:51:56.000 PM
```
Jul 14 12:51:56 rs741 - MCE: SOCKETID 0
host=rs741 | sourcetype=syslog | source=/var/log/messages
```

5 7/14/10 12:51:56.000 PM
```
Jul 14 12:51:56 rs741 - MCE: STATUS 8c0000400001009f MCGSTATUS 0
host=rs741 | sourcetype=syslog | source=/var/log/messages
```

6 7/14/10 12:51:56.000 PM
```
Jul 14 12:51:56 rs741 - MCE: Memory ECC syndrome: 20a2d080
host=rs741 | sourcetype=syslog | source=/var/log/messages
```

7 7/14/10 12:51:56.000 PM
```
Jul 14 12:51:56 rs741 - MCE: Memory channel ID of error: 0
host=rs741 | sourcetype=syslog | source=/var/log/messages
```

☑ Step#1: Run it

`job(655267)`

☑ Step#2: Love it!

© Copyright Splunk 2010

Adding a Workflow Action

splunk> Manager » Fields » Workflow actions » job

Label

`job($job$)` **1**

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 **2**

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 ap

Show action in

Both

Action type

search

Search configuration

Search string

`job($job$)` **3**

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

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

```
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)`

4

© Copyright Splunk 2010

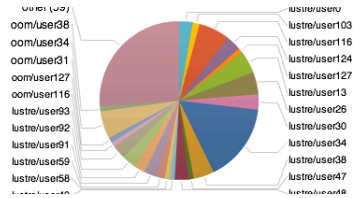
Putting it all together: Job Dashboard

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

Alerts in Jobs | Actions

Number of jobs per type/user — refreshed: **today at 4:19:12 PM.**

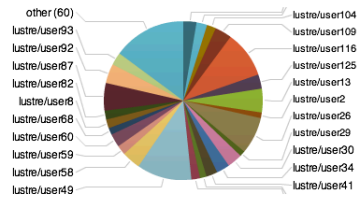
Loading... 6.09%



View results

Number of nodes per type/user — refreshed: **today at 4:19:13 PM.**

Loading... 1.88%



View results

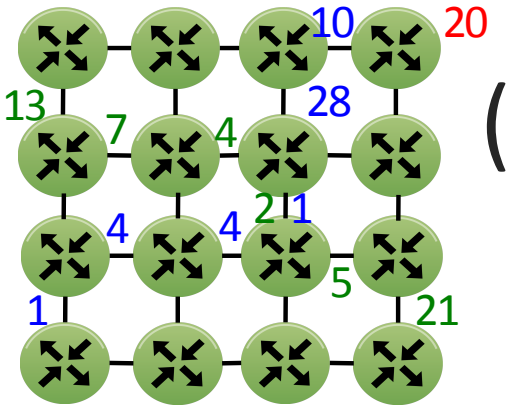
Number of alerts per type, user, job — refreshed: **today at 4:19:13 PM.**

Loading... 1.88%

	eventtype	user	job	count
1	lustre	user127	806190	134
2	oom	user127	806190	2
3	lustre	user127	806189	132
4	oom	user127	806189	11
5	oom	user35	806187	1
6	lustre	user116	806184	813
7	oom	user116	806184	13
8	lustre	user127	806182	167
9	oom	user127	806182	18
10	test1	user127	806182	11
11	lustre	user126	806178	309
12	oom	user126	806178	13
13	test1	user126	806178	11
14	lustre	user35	806177	268
15	lustre	user120	806175	492

© Copyright Splunk 2010

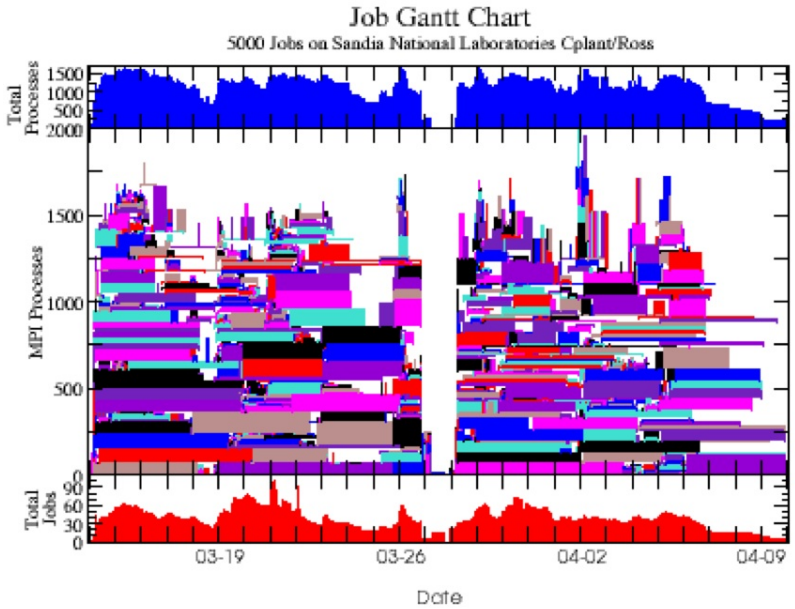
Future Work (Shared Components)



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.



© Copyright Splunk 2010

THE END

Extra Slides Follow

Jon Stearley

Sandia National Laboratories

jrstear@sandia.gov

© Copyright Splunk 2010

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.

© Copyright Splunk 2010

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

© Copyright Splunk 2010