BCNET ANNUAL HIGHER EDUCATION IT CONFERENCE

LEARN
ENGAGE
SHARE

FLARE!

Stapling together syslog-ng, elk, alerting, and incident tracking – with metadata!

Jeff Albert | University of Victoria

Hi, I'm Jeff

- UNIX Systems Administrator at UVic

Hi, I'm Jeff

- UNIX Systems Administrator at UVic
- "Internal Web Tools" guy on the UNIX team

Hi, I'm Jeff

- UNIX Systems Administrator at UVic
- "Internal Web Tools" guy on the UNIX team
- "Say, maybe you'd like to work on this all-singing, all-dancing log-processor-aggregator-monitor-alerter-event-manager thing?"

Too much of a good thing

Logs from a single host, stored locally? Easy! Read ‘em by hand!

Too much of a good thing

A few dozen hosts, centrally aggregated via syslog? Okay, we can manage that – probably with some scripts to look for known-bad conditions.

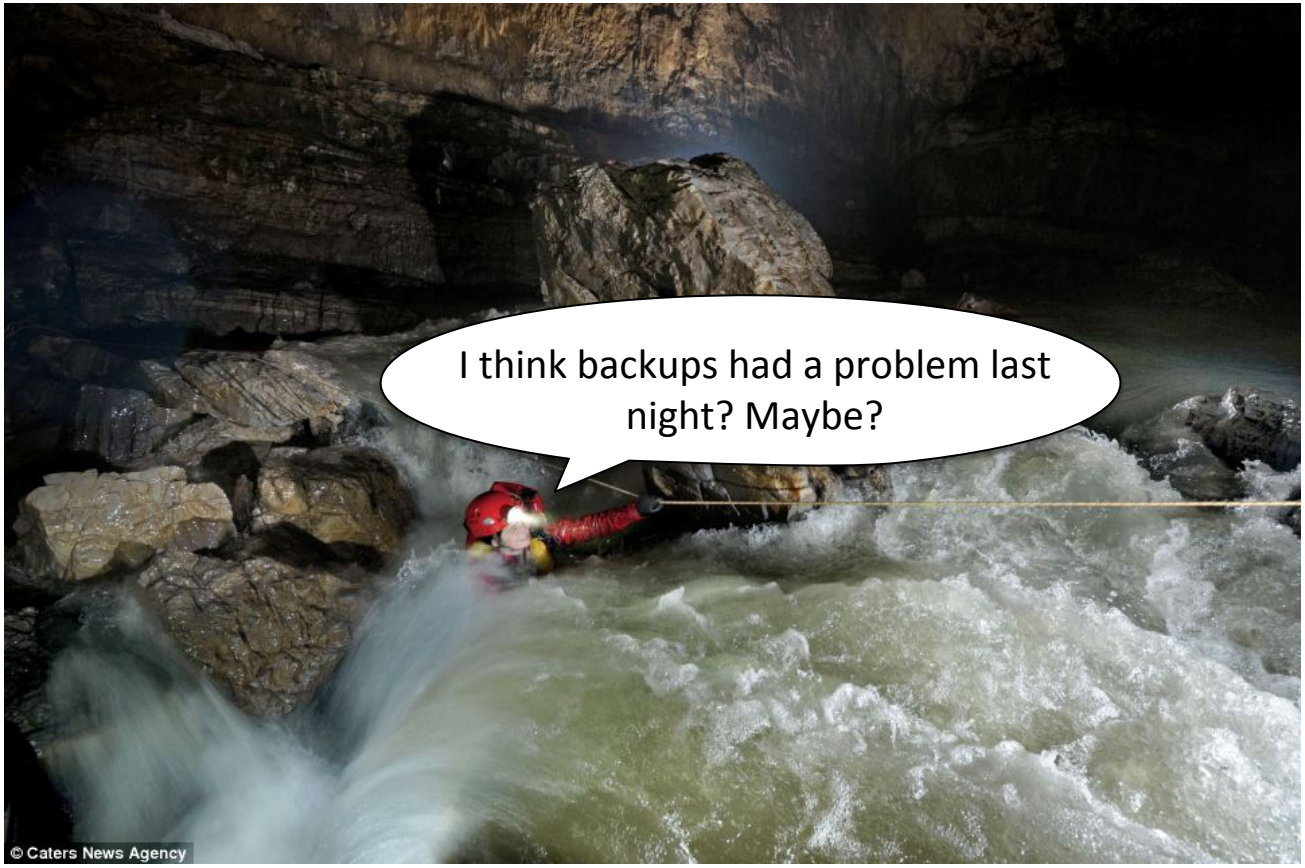
Too much of a good thing

Hundreds upon hundreds of hosts? Tons of different apps, OSes, configs?

Log processing scripts bogged down in the volume, and way too slow to alert?

Too much of a good thing

Too much of a good thing



Filtering What's Actionable

Even with log parsing scripts, most of the "is this a real problem I need to fix" filtering was done manually by human sysadmins.

Filtering What's Actionable

Even with log parsing scripts, most of the "is this a real problem I need to fix" filtering was done manually by human sysadmins.

Response to identified issues was also mostly driven by individual sysadmins' experience

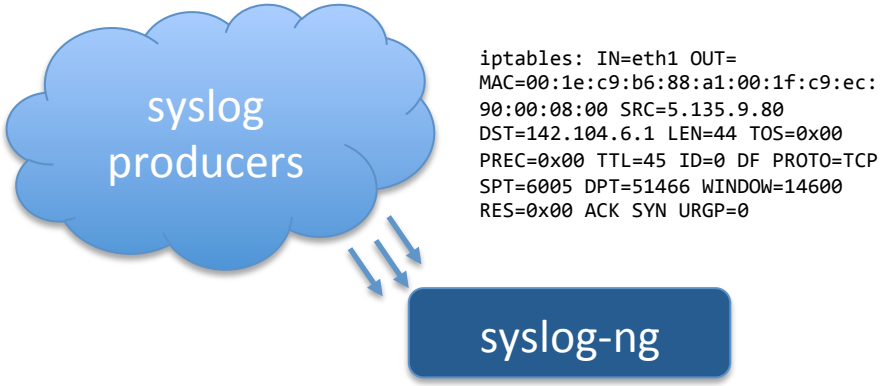
Filtering What's Actionable

Even with log parsing scripts, most of the "is this a real problem I need to fix" filtering was done manually by human sysadmins.

Response to identified issues was also mostly driven by individual sysadmins' experience

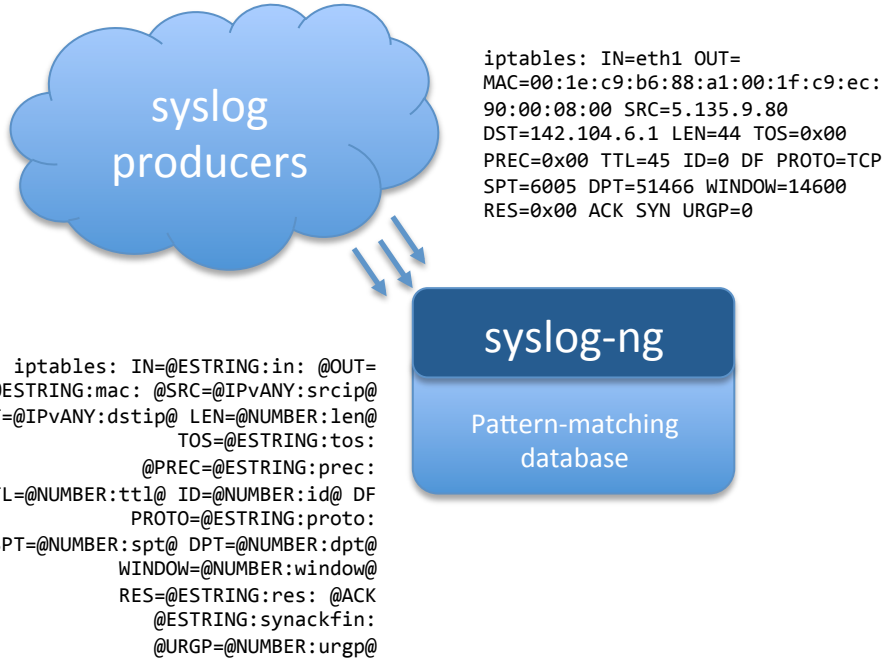
We needed a system that let our sysadmins turn their filtering and response knowledge into automation to cope with the flood of log data

Introducing FLARE

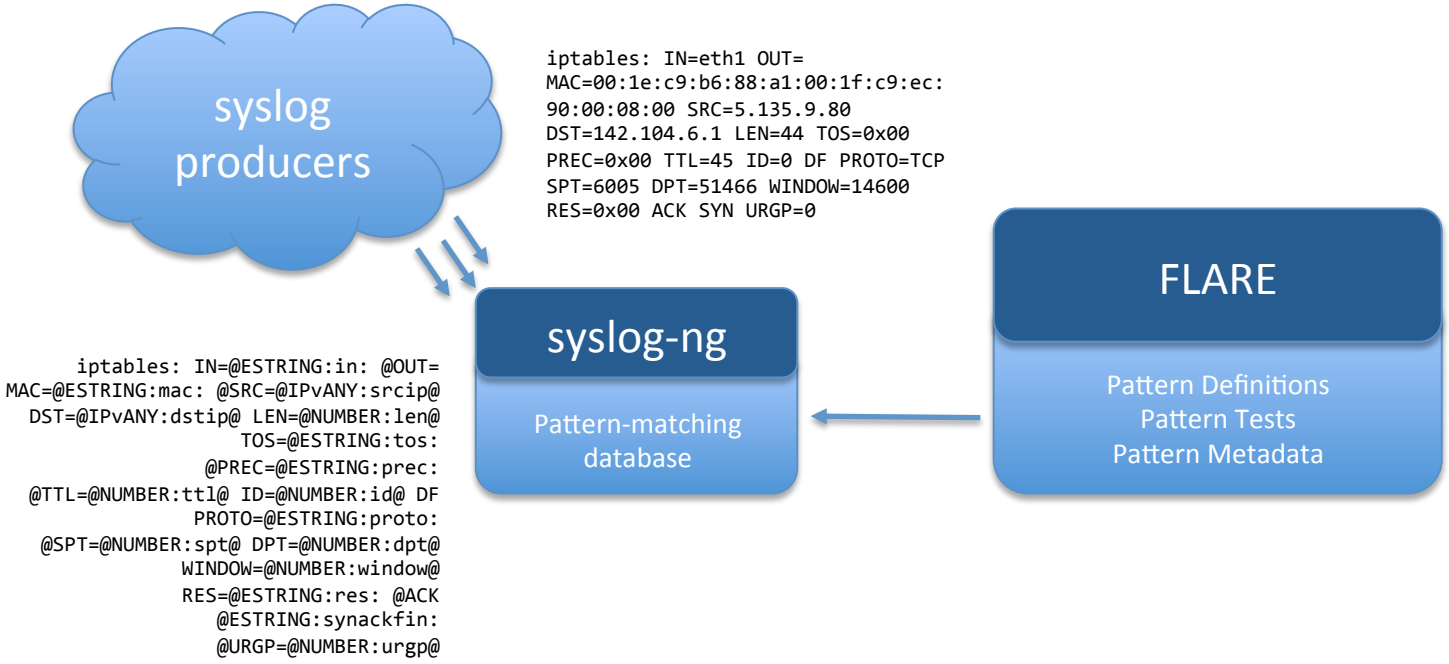



```
iptables: IN=eth1 OUT=
MAC=00:1e:c9:b6:88:a1:00:1f:c9:ec:
90:00:08:00 SRC=5.135.9.80
DST=142.104.6.1 LEN=44 TOS=0x00
PREC=0x00 TTL=45 ID=0 DF PROTO=TCP
SPT=6005 DPT=51466 WINDOW=14600
RES=0x00 ACK SYN URGP=0
```

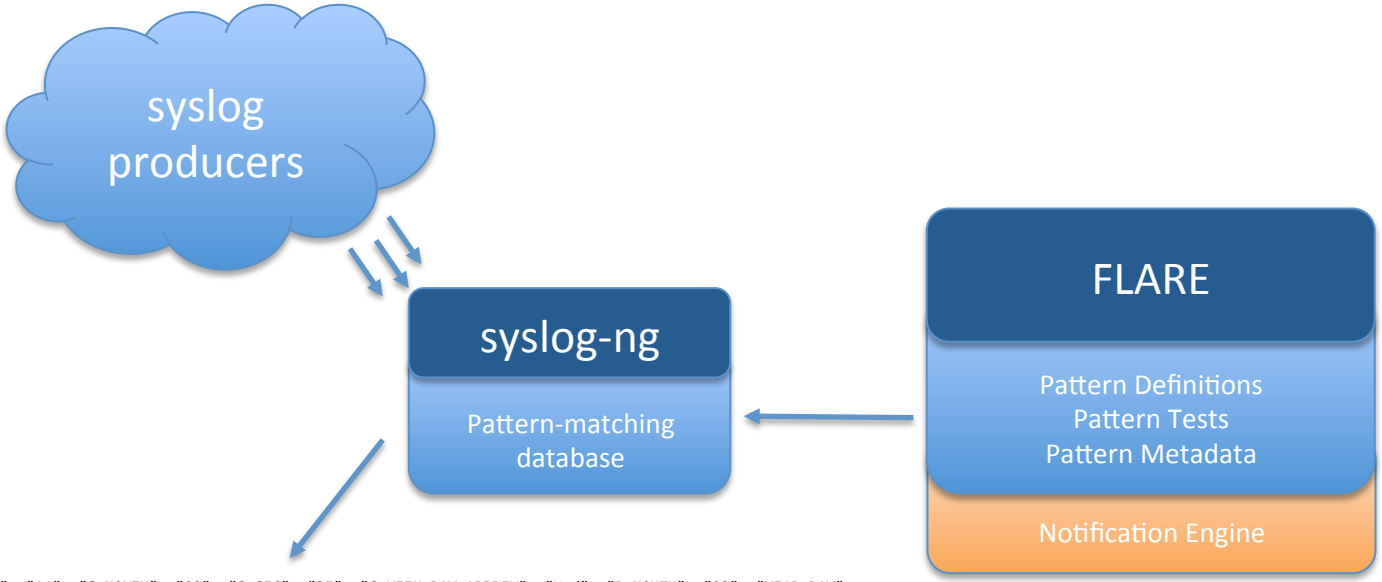
Introducing FLARE



Introducing FLARE

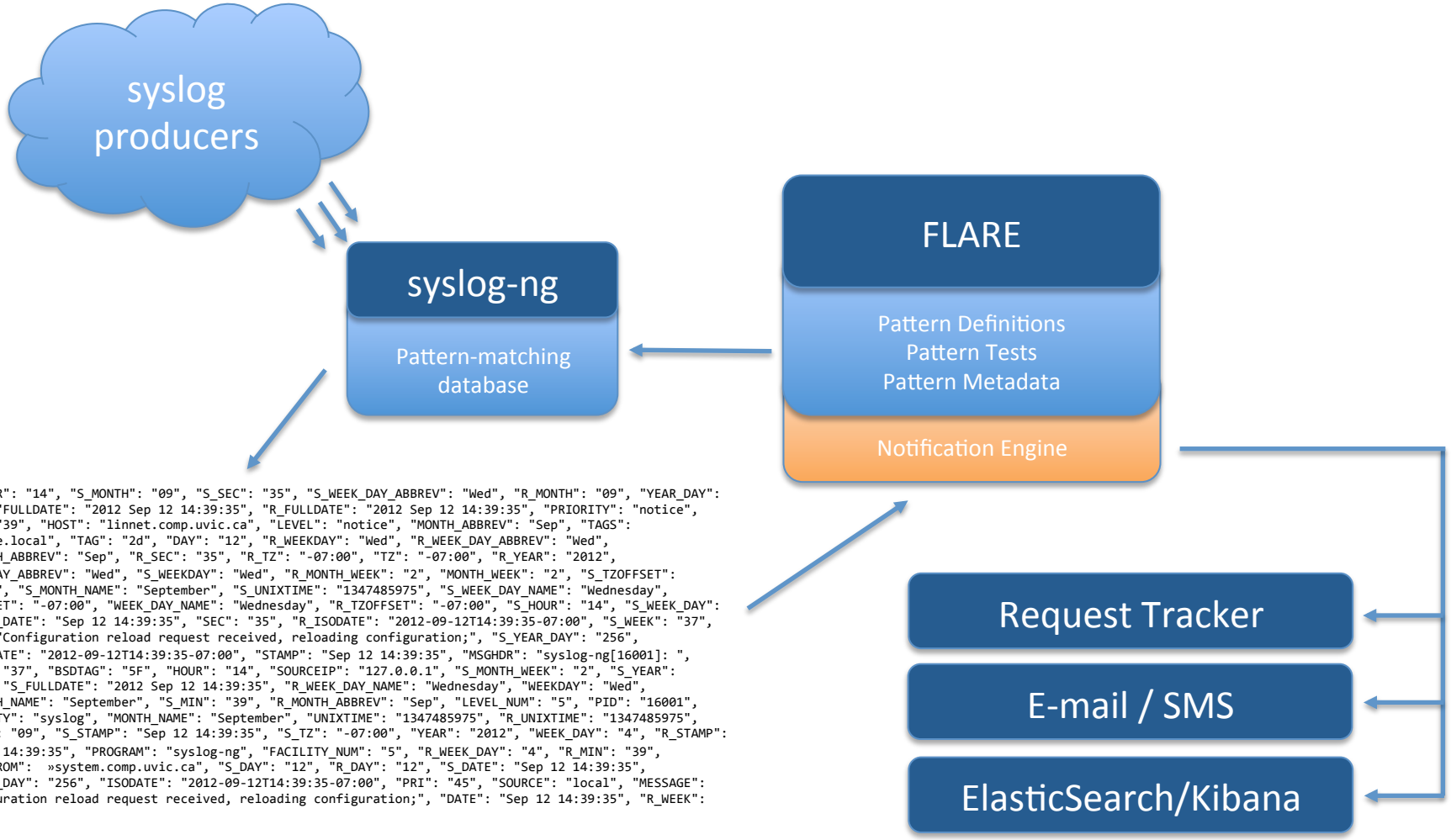


Introducing FLARE



{"R_HOUR": "14", "S_MONTH": "09", "S_SEC": "35", "S_WEEK_DAY_ABBREV": "Wed", "R_MONTH": "09", "YEAR_DAY": "256", "FULLDATE": "2012 Sep 12 14:39:35", "R_FULLDATE": "2012 Sep 12 14:39:35", "PRIORITY": "notice", "MIN": "39", "HOST": "linnet.comp.uvic.ca", "LEVEL": "notice", "MONTH_ABBREV": "Sep", "TAGS": ".source.local", "TAG": "2d", "DAY": "12", "R_WEEKDAY": "Wed", "R_WEEK_DAY_ABBREV": "Wed", "S_MONTH_ABBREV": "Sep", "R_SEC": "35", "R_TZ": "-07:00", "TZ": "-07:00", "R_YEAR": "2012", "WEEK_DAY_ABBREV": "Wed", "S_WEEKDAY": "Wed", "R_MONTH_WEEK": "2", "MONTH_WEEK": "2", "S_TZOFFSET": "-07:00", "S_MONTH_NAME": "September", "S_UNIXTIME": "1347485975", "S_WEEK_DAY_NAME": "Wednesday", "TZOFFSET": "-07:00", "WEEK_DAY_NAME": "Wednesday", "R_TZOFFSET": "-07:00", "S_HOUR": "14", "S_WEEK_DAY": "4", "R_DATE": "Sep 12 14:39:35", "SEC": "35", "R_ISODATE": "2012-09-12T14:39:35-07:00", "S_WEEK": "37", "MSG": "Configuration reload request received, reloading configuration;", "S_YEAR_DAY": "256", "S_ISODATE": "2012-09-12T14:39:35-07:00", "STAMP": "Sep 12 14:39:35", "MSGHDR": "syslog-ng[16001]: ", "WEEK": "37", "BSDTAG": "5F", "HOUR": "14", "SOURCEIP": "127.0.0.1", "S_MONTH_WEEK": "2", "S_YEAR": "2012", "S_FULLDATE": "2012 Sep 12 14:39:35", "R_WEEK_DAY_NAME": "Wednesday", "WEEKDAY": "Wed", "R_MONTH_NAME": "September", "S_MIN": "39", "R_MONTH_ABBREV": "Sep", "LEVEL_NUM": "5", "PID": "16001", "FACILITY": "syslog", "MONTH_NAME": "September", "UNIXTIME": "1347485975", "R_UNIXTIME": "1347485975", "MONTH": "09", "S_STAMP": "Sep 12 14:39:35", "S_TZ": "-07:00", "YEAR": "2012", "WEEK_DAY": "4", "R_STAMP": "Sep 12 14:39:35", "PROGRAM": "syslog-ng", "FACILITY_NUM": "5", "R_WEEK_DAY": "4", "R_MIN": "39", "HOST_FROM": »system.comp.uvic.ca", "S_DAY": "12", "R_DAY": "12", "S_DATE": "Sep 12 14:39:35", "R_YEAR_DAY": "256", "ISODATE": "2012-09-12T14:39:35-07:00", "PRI": "45", "SOURCE": "local", "MESSAGE": "Configuration reload request received, reloading configuration;", "DATE": "Sep 12 14:39:35", "R_WEEK": "37" }

Introducing FLARE



{"R_HOUR": "14", "S_MONTH": "09", "S_SEC": "35", "S_WEEK_DAY_ABBREV": "Wed", "R_MONTH": "09", "YEAR_DAY": "256", "FULLDATE": "2012 Sep 12 14:39:35", "R_FULLDATE": "2012 Sep 12 14:39:35", "PRIORITY": "notice", "MIN": "39", "HOST": "linnet.comp.uvic.ca", "LEVEL": "notice", "MONTH_ABBREV": "Sep", "TAGS": ".source.local", "TAG": "2d", "DAY": "12", "R_WEEKDAY": "Wed", "R_WEEK_DAY_ABBREV": "Wed", "S_MONTH_ABBREV": "Sep", "R_SEC": "35", "R_TZ": "-07:00", "TZ": "-07:00", "R_YEAR": "2012", "WEEK_DAY_ABBREV": "Wed", "S_WEEKDAY": "Wed", "R_MONTH_WEEK": "2", "MONTH_WEEK": "2", "S_TZOFFSET": "-07:00", "S_MONTH_NAME": "September", "S_UNIXTIME": "1347485975", "S_WEEK_DAY_NAME": "Wednesday", "TZOFFSET": "-07:00", "WEEK_DAY_NAME": "Wednesday", "R_TZOFFSET": "-07:00", "S_HOUR": "14", "S_WEEK_DAY": "4", "R_DATE": "Sep 12 14:39:35", "SEC": "35", "R_ISODATE": "2012-09-12T14:39:35-07:00", "S_WEEK": "37", "MSG": "Configuration reload request received, reloading configuration;", "S_YEAR_DAY": "256", "S_ISODATE": "2012-09-12T14:39:35-07:00", "STAMP": "Sep 12 14:39:35", "MSGHDR": "syslog-ng[16001]: ", "WEEK": "37", "BSDTAG": "5F", "HOUR": "14", "SOURCEIP": "127.0.0.1", "S_MONTH_WEEK": "2", "S_YEAR": "2012", "S_FULLDATE": "2012 Sep 12 14:39:35", "R_WEEK_DAY_NAME": "Wednesday", "WEEKDAY": "Wed", "R_MONTH_NAME": "September", "S_MIN": "39", "R_MONTH_ABBREV": "Sep", "LEVEL_NUM": "5", "PID": "16001", "FACILITY": "syslog", "MONTH_NAME": "September", "UNIXTIME": "1347485975", "R_UNIXTIME": "1347485975", "MONTH": "09", "S_STAMP": "Sep 12 14:39:35", "S_TZ": "-07:00", "YEAR": "2012", "WEEK_DAY": "4", "R_STAMP": "Sep 12 14:39:35", "PROGRAM": "syslog-ng", "FACILITY_NUM": "5", "R_WEEK_DAY": "4", "R_MIN": "39", "HOST_FROM": »system.comp.uvic.ca", "S_DAY": "12", "R_DAY": "12", "S_DATE": "Sep 12 14:39:35", "R_YEAR_DAY": "256", "ISODATE": "2012-09-12T14:39:35-07:00", "PRI": "45", "SOURCE": "local", "MESSAGE": "Configuration reload request received, reloading configuration;", "DATE": "Sep 12 14:39:35", "R_WEEK": "37" }

Events

FLARE

PATTERNS » CROND | NOTIFICATION MEMBERS | NOTIFICATION PROFILES

Activate | Add New Pattern | Help

could not identify user (from getpwnam(erempel))

```
could not identify user (from getpwnam@QSTRING:login:()@)
```

BASICS

Program: crond

Comment: (none)

Enabled: ☑

Documentation: https://twiki.comp.uvic.ca/twiki/bin/view/COMP/33eaef0f0c4e4218a9355def77bbe85a

TAGS DEFER | IGNORE | EVENT | COLLECTION | TIMER | EXTPROG

event: (none)

eventid: cron:unknownuser:$login

severity: notice

subject: $HOST unknown user $login has cron tasks

synopsis: Cron can not find the password entry for the user's cron task entry. Host: $HOST File: /var/spool/cron/$login

throttle: 60

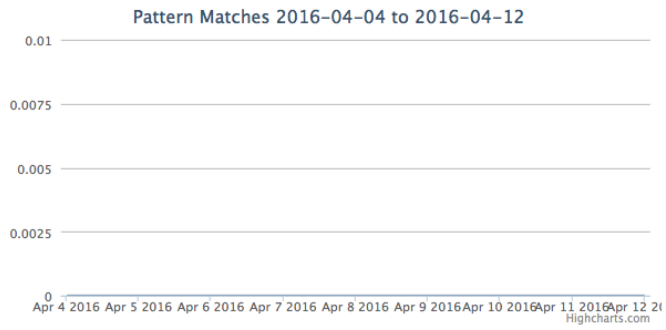
url: (none)

TESTS

`could not identify user (from getpwnam(erempel))`

login: `erempel`

STATS DAY | WEEK | MONTH | YEAR



AUDIT LOG

erempel: Updated Pattern Tag 'subject': changed tag_value from 'unknown user $login has cron tasks' to '$HOST unknown user $login has cron tasks' (2015-05-01 11:01:50.101048)

erempel: Updated Pattern Tag 'synopsis': changed tag_value from 'Cron can not find the password entry for the user's cron task entry. See file /var/spool/cron/$login' to 'Cron can not find the password entry for the user's cron task entry. Host: $HOST File: /var/spool/cron/$login' (2015-05-01 11:01:30.27216)

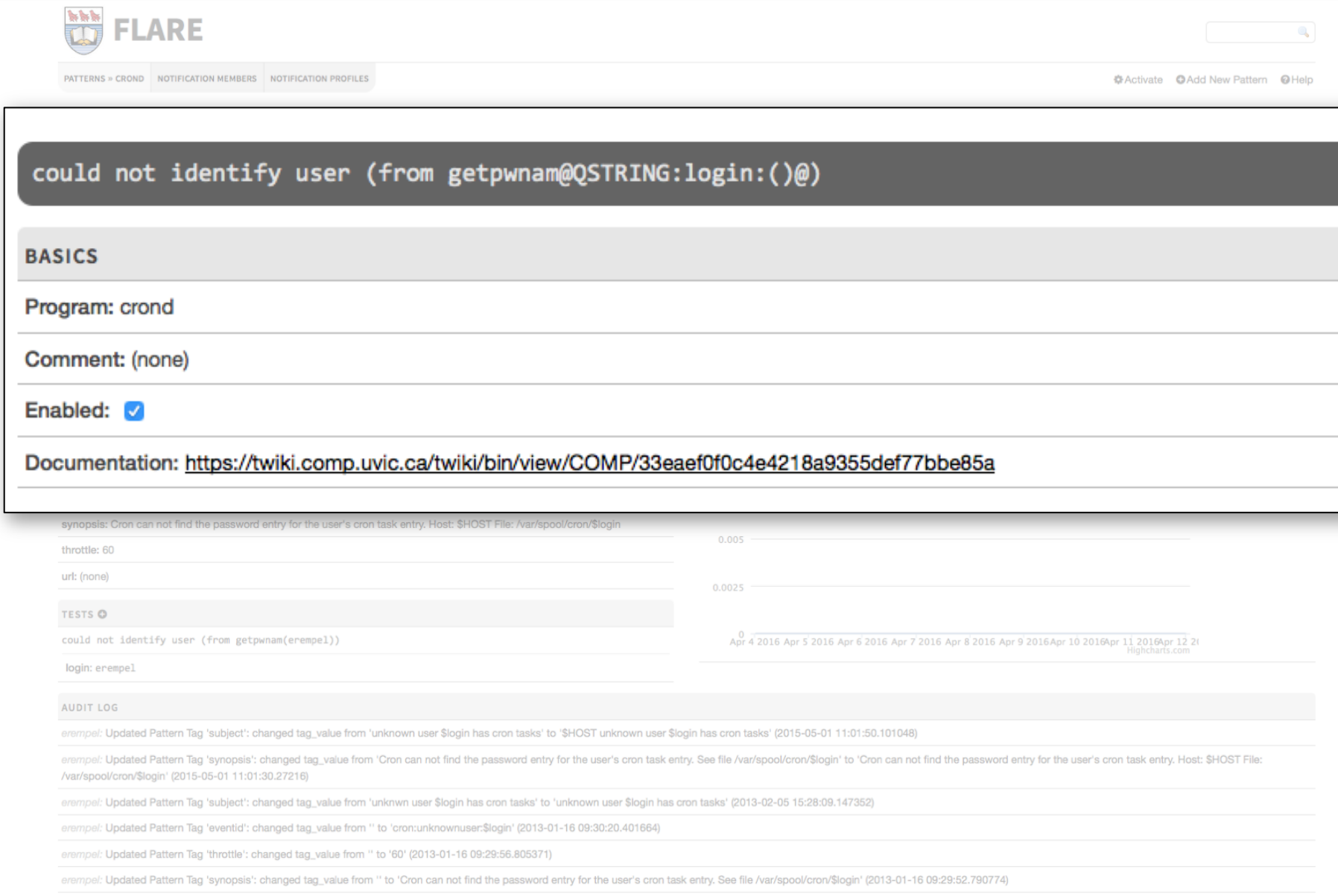
erempel: Updated Pattern Tag 'subject': changed tag_value from 'unknwn user $login has cron tasks' to 'unknown user $login has cron tasks' (2013-02-05 15:28:09.147352)

erempel: Updated Pattern Tag 'eventid': changed tag_value from '' to 'cron:unknownuser:$login' (2013-01-16 09:30:20.401664)

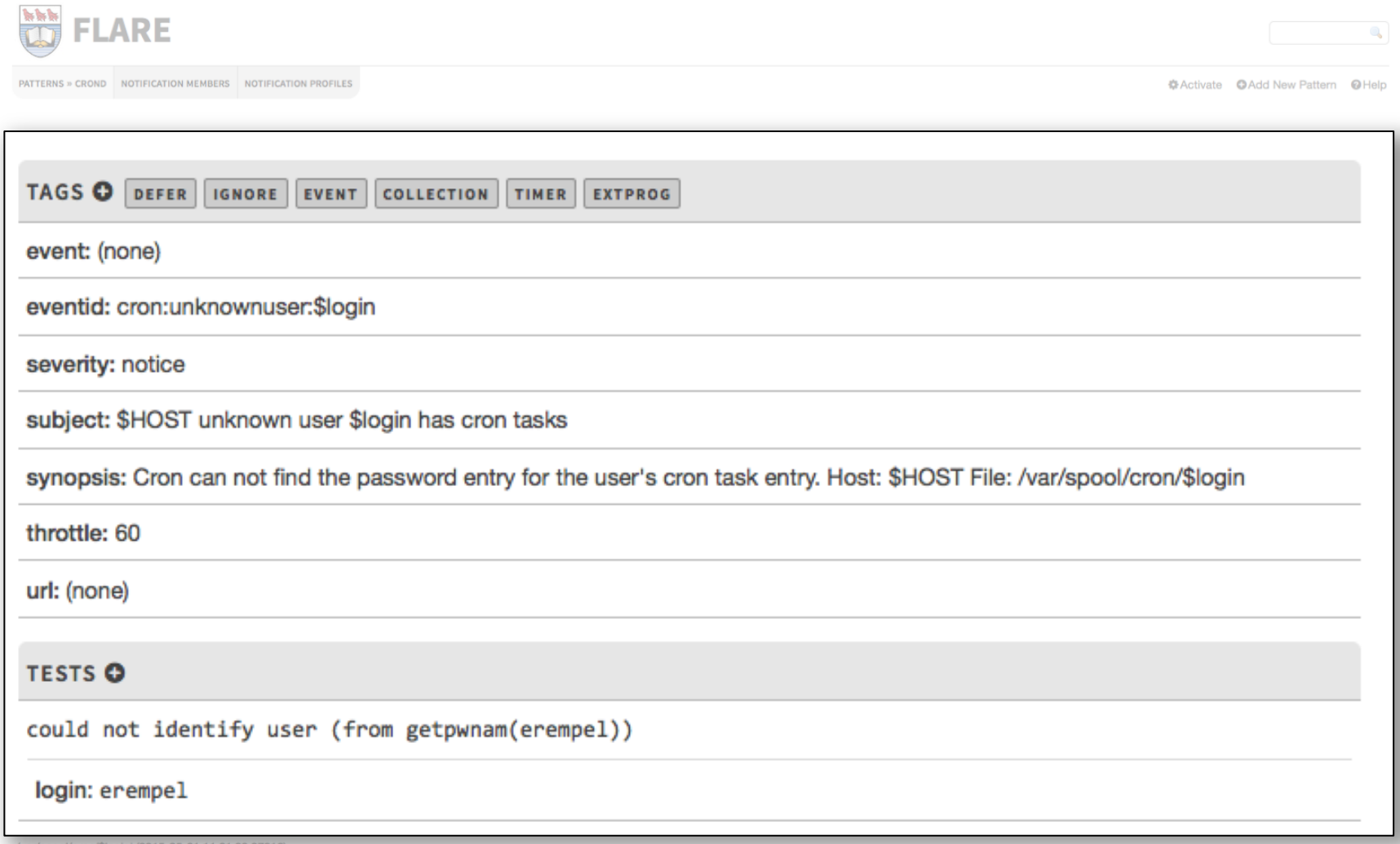
erempel: Updated Pattern Tag 'throttle': changed tag_value from '' to '60' (2013-01-16 09:29:56.805371)

erempel: Updated Pattern Tag 'synopsis': changed tag_value from '' to 'Cron can not find the password entry for the user's cron task entry. See file /var/spool/cron/$login' (2013-01-16 09:29:52.790774)

Events


FLARE
PATTERNS » CROND
NOTIFICATION MEMBERS
NOTIFICATION PROFILES
Activate
Add New Pattern
Help
could not identify user (from getpwnam@QSTRING:login:()@)
BASICS
Program: crond
Comment: (none)
Enabled:
Documentation: https://twiki.comp.uvic.ca/twiki/bin/view/COMP/33eaef0f0c4e4218a9355def77bbe85a
synopsis: Cron can not find the password entry for the user's cron task entry. Host: $HOST File: /var/spool/cron/$login
throttle: 60
url: (none)
TESTS
could not identify user (from getpwnam(erempel))
login: erempel
0.005
0.0025
0
Apr 4 2016 Apr 5 2016 Apr 6 2016 Apr 7 2016 Apr 8 2016 Apr 9 2016 Apr 10 2016 Apr 11 2016 Apr 12 2(
Highcharts.com
AUDIT LOG
erempel: Updated Pattern Tag 'subject': changed tag_value from 'unknown user $login has cron tasks' to '$HOST unknown user $login has cron tasks' (2015-05-01 11:01:50.101048)
erempel: Updated Pattern Tag 'synopsis': changed tag_value from 'Cron can not find the password entry for the user's cron task entry. See file /var/spool/cron/$login' to 'Cron can not find the password entry for the user's cron task entry. Host: $HOST File: /var/spool/cron/$login' (2015-05-01 11:01:30.27216)
erempel: Updated Pattern Tag 'subject': changed tag_value from 'unknwn user $login has cron tasks' to 'unknown user $login has cron tasks' (2013-02-05 15:28:09.147352)
erempel: Updated Pattern Tag 'eventid': changed tag_value from '' to 'cron:unknownuser:$login' (2013-01-16 09:30:20.401664)
erempel: Updated Pattern Tag 'throttle': changed tag_value from '' to '60' (2013-01-16 09:29:56.805371)
erempel: Updated Pattern Tag 'synopsis': changed tag_value from '' to 'Cron can not find the password entry for the user's cron task entry. See file /var/spool/cron/$login' (2013-01-16 09:29:52.790774)

Events


FLARE
PATTERNS » CROND
NOTIFICATION MEMBERS
NOTIFICATION PROFILES
Activate
Add New Pattern
Help
TAGS
DEFER
IGNORE
EVENT
COLLECTION
TIMER
EXTPROG
event: (none)
eventid: cron:unknownuser:$login
severity: notice
subject: $HOST unknown user $login has cron tasks
synopsis: Cron can not find the password entry for the user's cron task entry. Host: $HOST File: /var/spool/cron/$login
throttle: 60
url: (none)
TESTS
could not identify user (from getpwnam(erempel))
login: erempel
/var/spool/cron/$login' (2015-05-01 11:01:30.27216)
erempel: Updated Pattern Tag 'subject': changed tag_value from 'unknwn user $login has cron tasks' to 'unknown user $login has cron tasks' (2013-02-05 15:28:09.147352)
erempel: Updated Pattern Tag 'eventid': changed tag_value from '' to 'cron:unknownuser:$login' (2013-01-16 09:30:20.401664)
erempel: Updated Pattern Tag 'throttle': changed tag_value from '' to '60' (2013-01-16 09:29:56.805371)
erempel: Updated Pattern Tag 'synopsis': changed tag_value from '' to 'Cron can not find the password entry for the user's cron task entry. See file /var/spool/cron/$login' (2013-01-16 09:29:52.790774)

Collections

FLARE

PATTERNS » CROND | NOTIFICATION MEMBERS | NOTIFICATION PROFILES

Activate | Add New Pattern | Help

Permission denied

Permission denied

BASICS

Program: crond

Comment: (none)

Enabled: ☑

Documentation: https://twiki.comp.uvic.ca/twiki/bin/view/COMP/a0dd3a3af5c2491abd701f33783e294e

TAGS DEFER | IGNORE | EVENT | COLLECTION | TIMER | EXTPROG

collection: (none)

collection.duration: 60

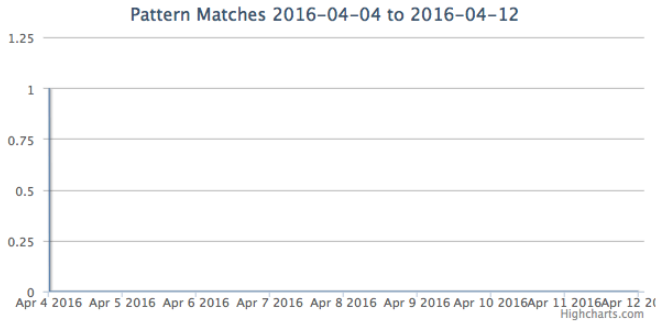
collection.id: $HOST:crond:$PID

collection.message: $S_HOUR:$S_MIN:$S_SEC $FACILITY.$LEVEL $MESSAGE

TESTS

Permission denied

STATS DAY | WEEK | MONTH | YEAR



AUDIT LOG

erempel: Deleted Pattern Tag 'collection.endall' (2013-06-20 21:26:45.127749)

erempel: Updated Pattern Tag 'collection.id': changed tag_value from '' to '$HOST:crond:$PID' (2013-06-20 21:26:44.165004)

erempel: Deleted Pattern Tag 'collection.end' (2013-06-20 21:26:30.721333)

erempel: Deleted Pattern Tag 'collection.required' (2013-06-20 21:26:29.653186)

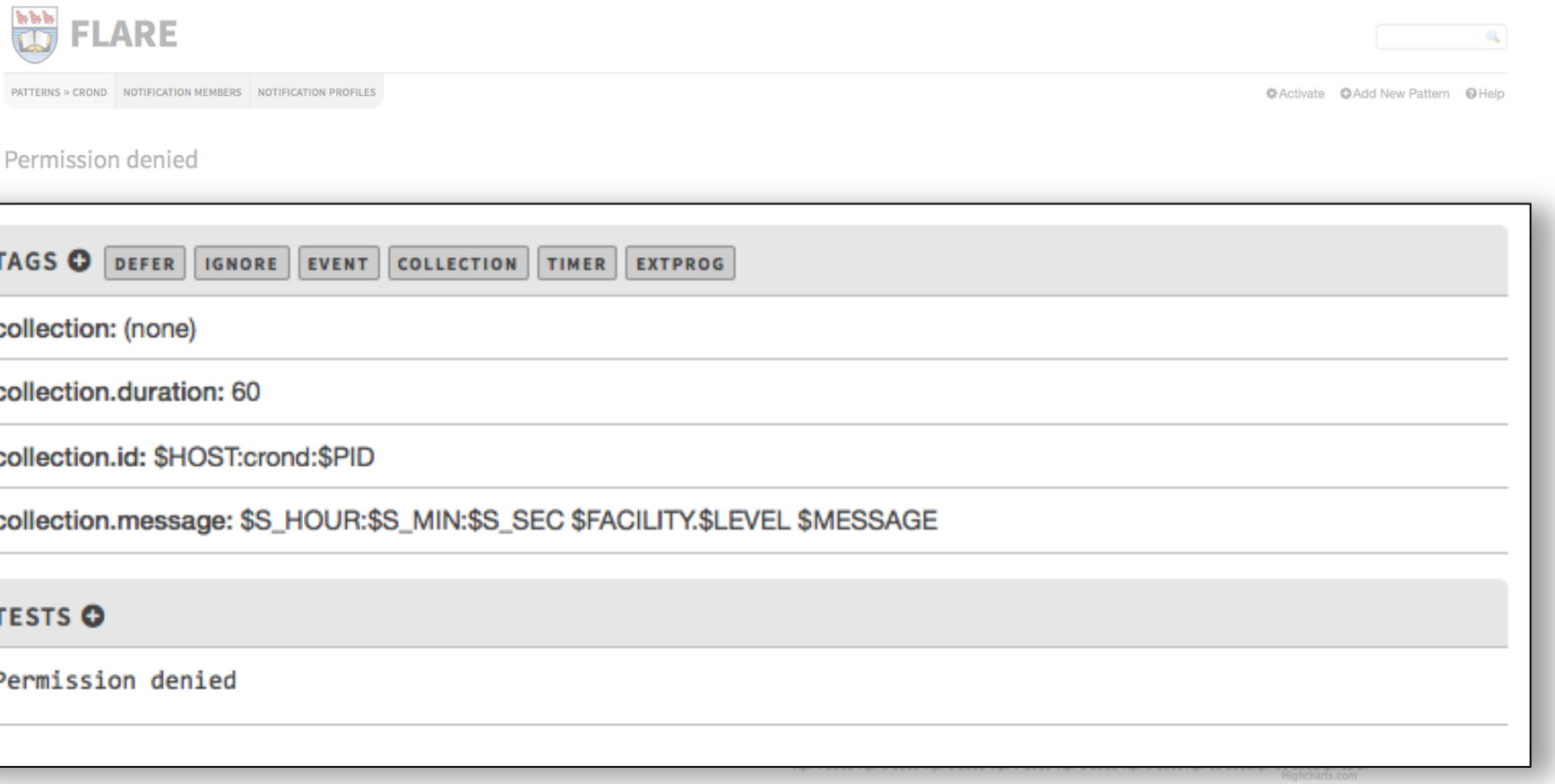
erempel: Updated Pattern Tag 'collection.message': changed tag_value from '' to '$S_HOUR:$S_MIN:$S_SEC $FACILITY.$LEVEL $MESSAGE' (2013-06-20 21:26:28.259279)

erempel: Deleted Pattern Tag 'collection.size' (2013-06-20 21:26:08.412944)

erempel: Deleted Pattern Tag 'collection.drop' (2013-06-20 21:26:07.712501)

erempel: Created Pattern Tag 'collection.endall' (2013-06-20 21:26:06.106518)

Collections



Collections

FLARE

PATTERNS » CROND | NOTIFICATION MEMBERS | NOTIFICATION PROFILES

Activate | Add New Pattern | Help

pam_access(crond:account): access denied for user `ahillair' from `cron'

```
pam_access(crond:account): access denied for user `@ESTRING:login:'@ from `cron'
```

BASICS

Program: crond

Comment: Deprecated for general pattern (https://flare.comp.uvic.ca/pattern/349)

Enabled: ☑

Documentation: https://twiki.comp.uvic.ca/twiki/bin/view/COMP/07902905787f4b779db736f120715fc2

TAGS DEFER | IGNORE | EVENT | COLLECTION | TIMER | EXTPROG

collection: (none)

collection.duration: 60

collection.id: $HOST:crond:$PID

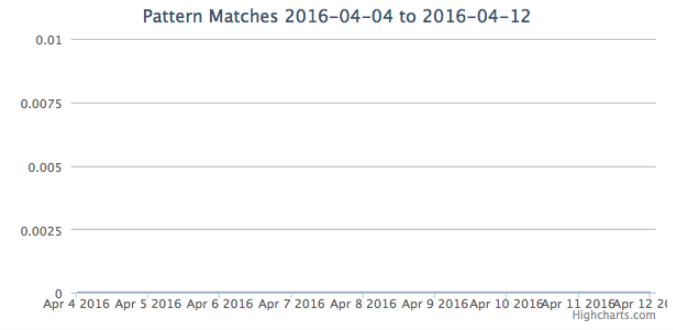
collection.message: $S_HOUR:$S_MIN:$S_SEC $FACILITY.$LEVEL $MESSAGE

TESTS

`pam_access(crond:account): access denied for user `ahillair' from `cron'`

login: `ahillair`

STATS DAY | WEEK | MONTH | YEAR



AUDIT LOG

erempel: Updated Pattern '07902905-787f-4b77-9db7-36f120715fc2': changed enabled from '0' to '1' (2013-06-20 21:32:57.315448)

erempel: Updated Pattern Tag 'collection.id': changed tag_value from '' to '$HOST:crond:$PID' (2013-06-20 21:32:54.764633)

erempel: Updated Pattern Tag 'collection.message': changed tag_value from '' to '$S_HOUR:$S_MIN:$S_SEC $FACILITY.$LEVEL $MESSAGE' (2013-06-20 21:32:51.808115)

erempel: Deleted Pattern Tag 'collection.required' (2013-06-20 21:32:38.058732)

erempel: Deleted Pattern Tag 'collection.size' (2013-06-20 21:32:36.924803)

erempel: Deleted Pattern Tag 'collection.endall' (2013-06-20 21:32:35.905033)

erempel: Deleted Pattern Tag 'collection.end' (2013-06-20 21:32:34.84484)

erempel: Deleted Pattern Tag 'collection.drop' (2013-06-20 21:32:34.04958)

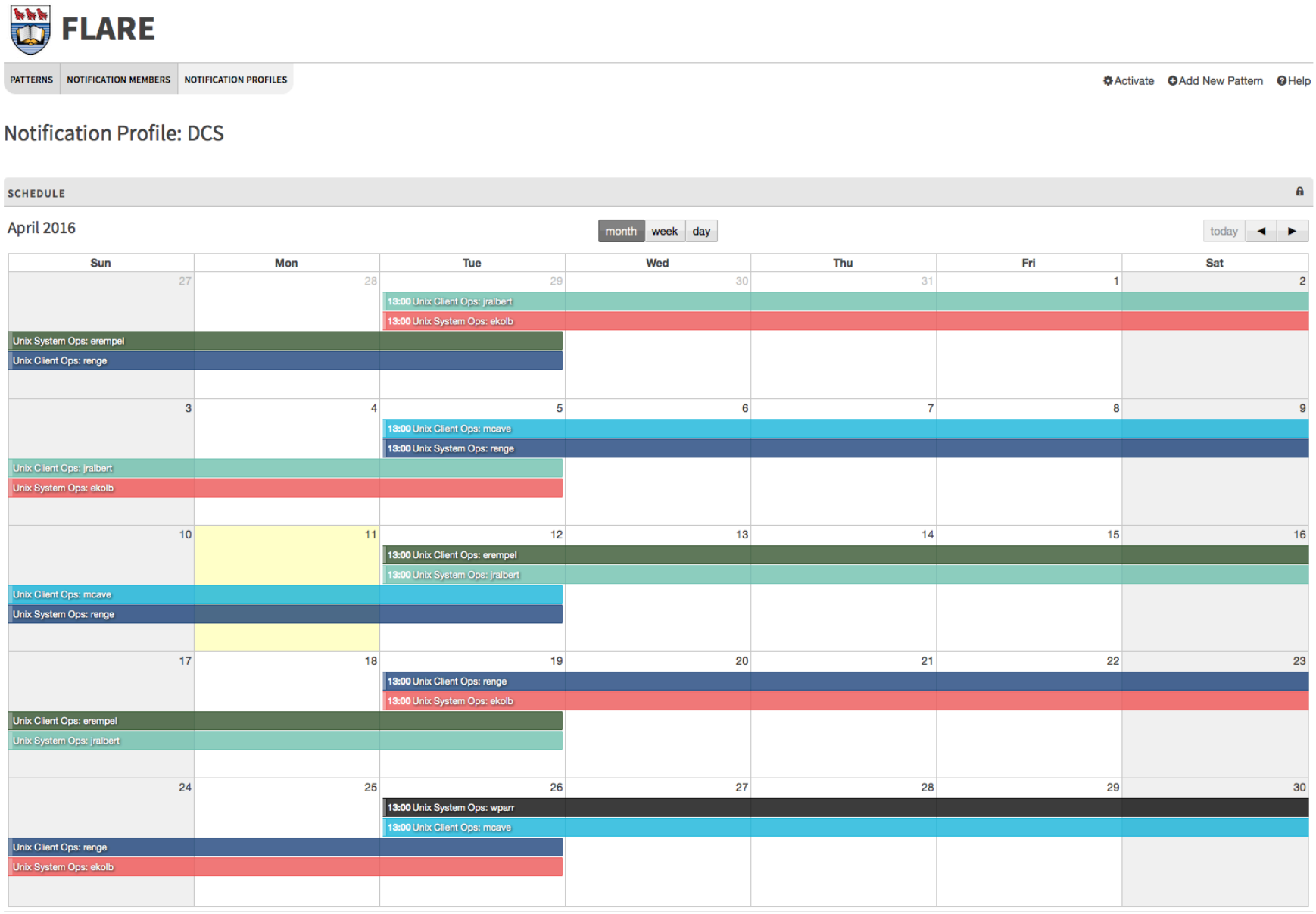
...and more!

- **Timer**
  Hold on to an event for a specified amount of time before notifying, and use *timer.id*-related patterns to cancel the event if a mitigating event occurs during the hold period.

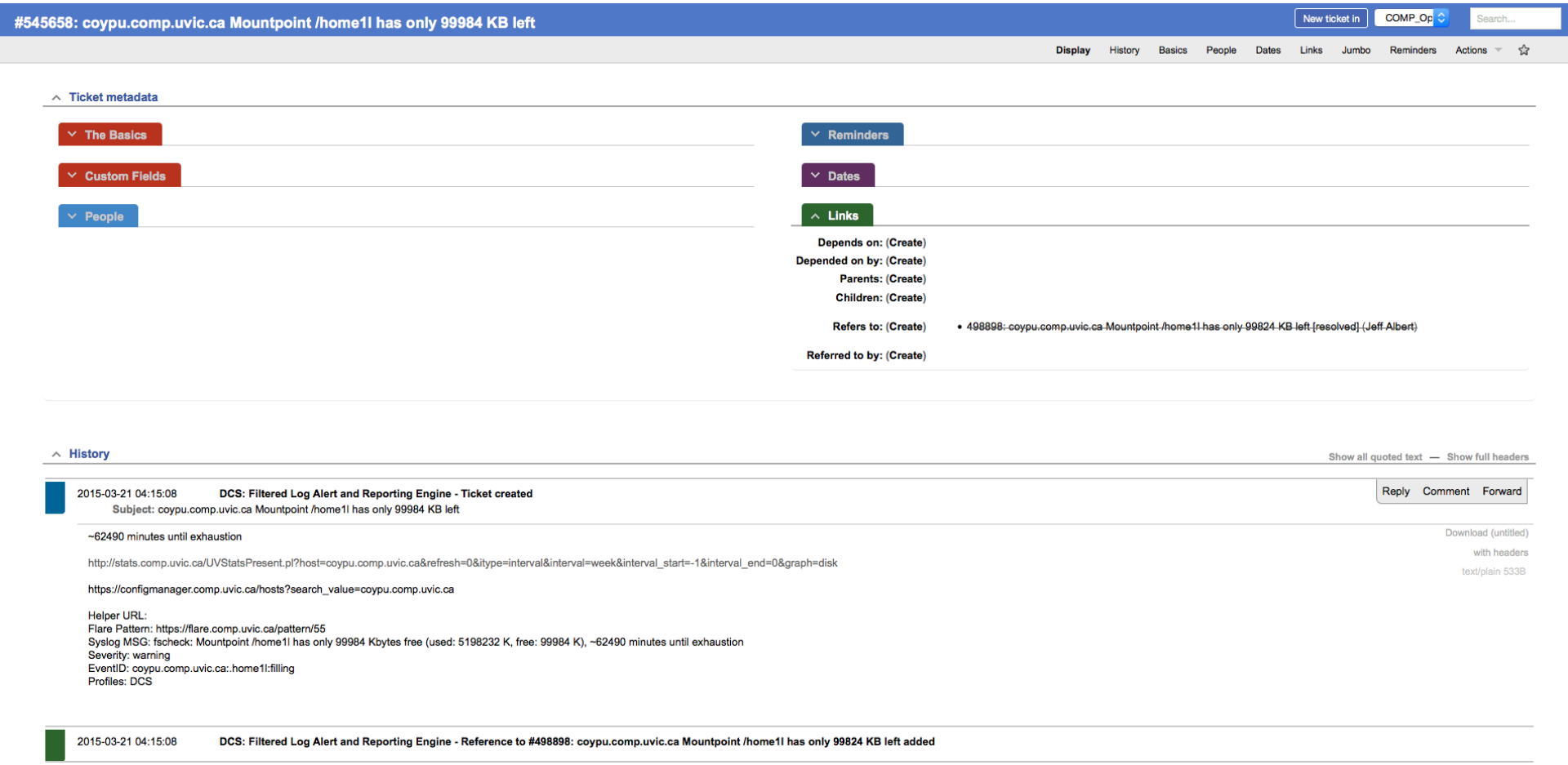
- **Extprog**
  Execute a command in a format specified by the pattern's tags, populated by pattern metadata – automated response!

- **...and more!**
  These are all plugins we wrote for the notification engine as the need arose, and more are on the way.

Notification Profiles



Notification Destinations: RT



Metadata Convergence

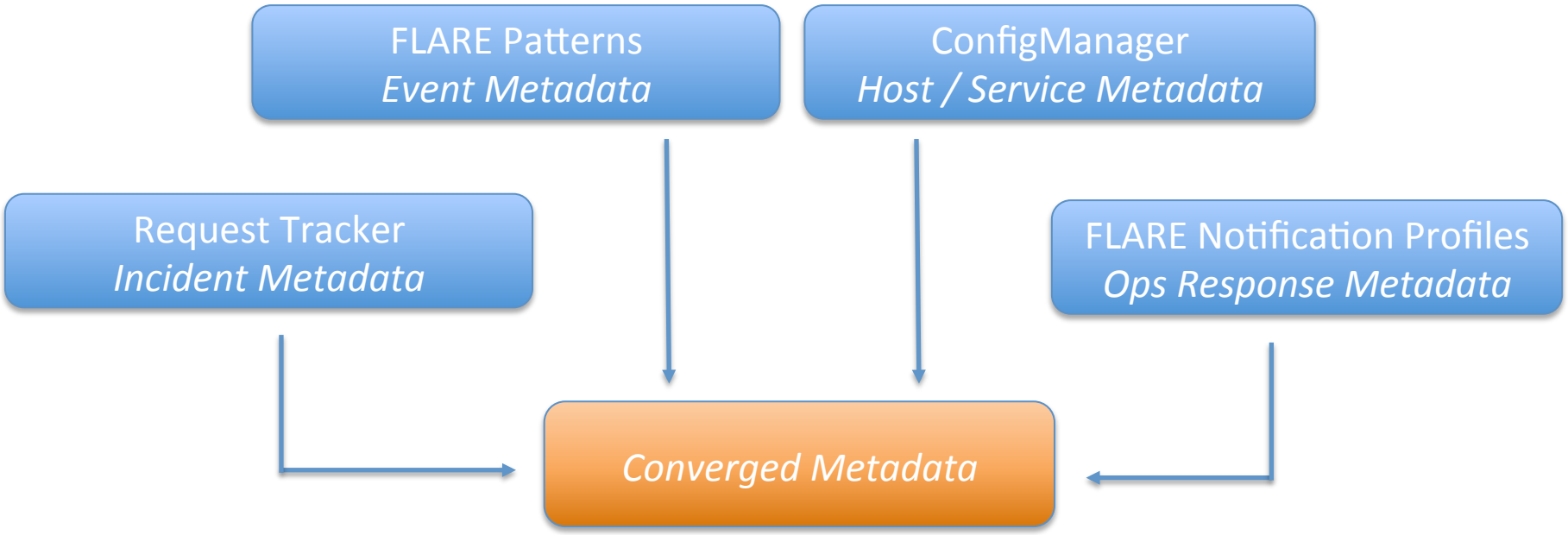
FLARE Patterns
Event Metadata

ConfigManager
Host / Service Metadata

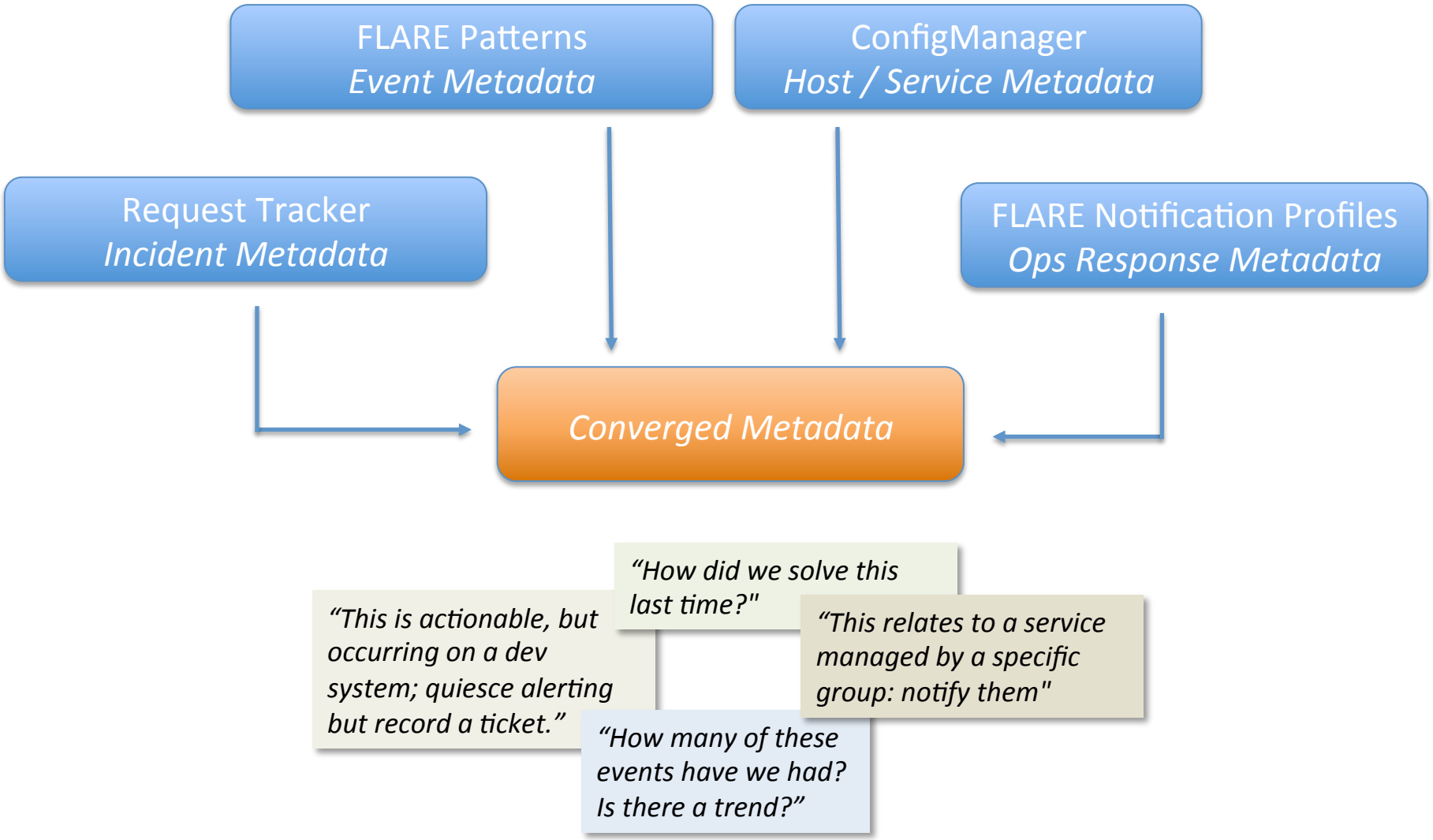
Request Tracker
Incident Metadata

FLARE Notification Profiles
Ops Response Metadata

Metadata Convergence



Metadata Convergence



THANKS!

Any Questions?

BCNET
Conference 2016