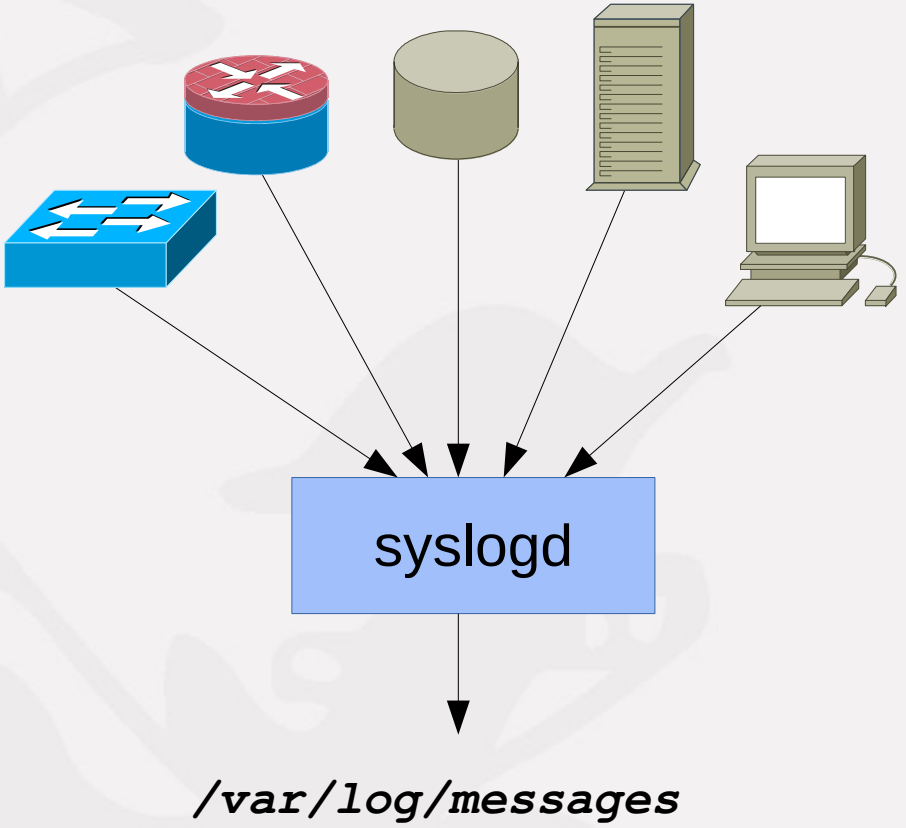
Monitoraggio alla SISSA

Davide Brunato
Scuola Internazionale Superiore di Studi Avanzati di Trieste

Workshop GARR 2018, Roma, 29/05/2018

Infrastruttura legacy (pre 2012)

- Server monitoraggio
  - Collettore syslog
  - Epylog (reports)
  - Nagios core
  - MRTG/Munin

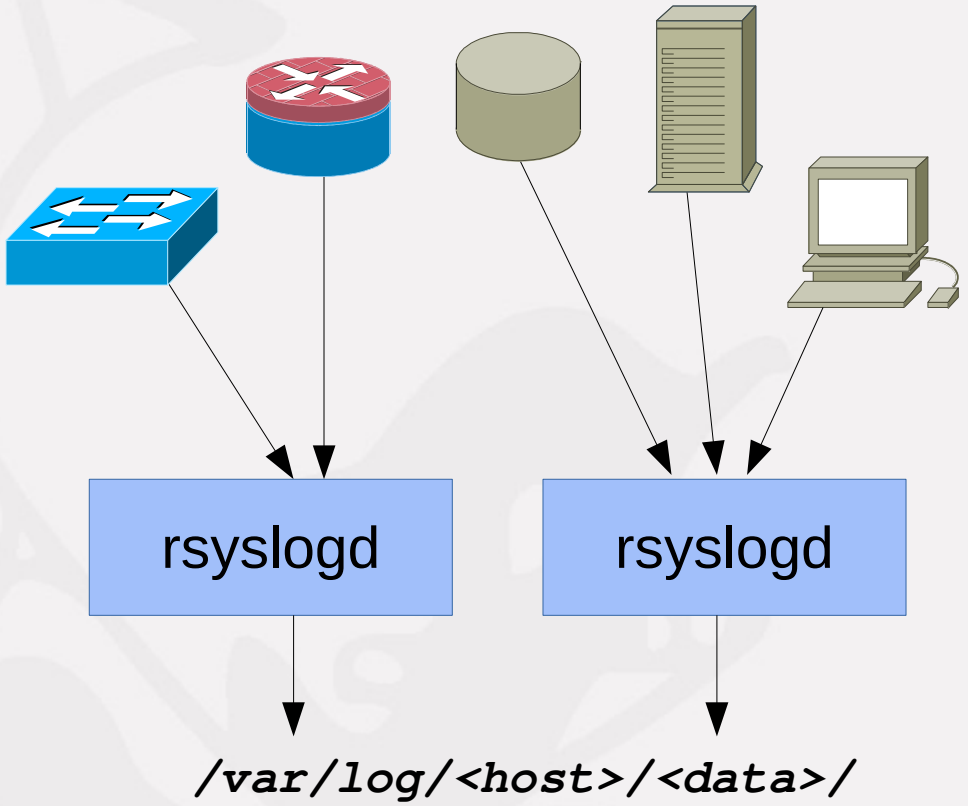


Limitazioni:

- Log collassati su file ampi
- Niente suddivisione rete/servizi
- Report epylog non adattabili
- Molto lavoro con ***grep***

Infrastruttura attuale

- 2 server monitoraggio
  - Apparecchiature rete
  - Servizi
- Tecnologie
  - rsyslog
  - Nagios core
  - Cacti
  - epylog → lograptor



Cos'è lograptor?

- Rielaborazione di epylog in modalità CLI grep-like
  - GPL2+ (ora LGPLv2.1+)
  - Python 2/3
  - BSD syslog format RFC 3164, IETF syslog protocol RFC 5424
  - Regexp based (GROK?)
  - Configurabile per match di nuove linee di log
  - Pubblicato su https://github.com/brunato/lograptor e PyPI
- Cosa ci permette di fare
  - Velocizzare le ricerche con più parametri
  - Match di host o protocollo
  - Produrre report dai dati
  - Analizzare nel dettaglio i formati di log (anonimizzazione)
  - Fare esperienza con l'uso effettivo di Python

Formati di Log

- **RFC 3164**
  - ***<pri> <month> <day> <ltime> <host> <apptag> <message>***

```
Jan 31 09:50:08 raptor postfix/smtpd[15802]: connect from
stegosaurus.dinos.test[192.168.4.150]
Jan 31 09:50:08 raptor postfix/smtpd[15802]: setting up TLS connection from
stegosaurus.dinos.test[192.168.4.150]
Jan 31 09:50:08 raptor postfix/smtpd[15802]: TLS connection established from
stegosaurus.dinos.test[192.168.4.150]: TLSv1 with cipher DHE-RSA-AES256-SHA
(256/256
```

- **RFC 5424**
  - ***<pri> <ver> <year> <month> <day> <ltime> <secfrac> (Z|<offset>) <host> <apptag> <procid> <msgid> <message>***

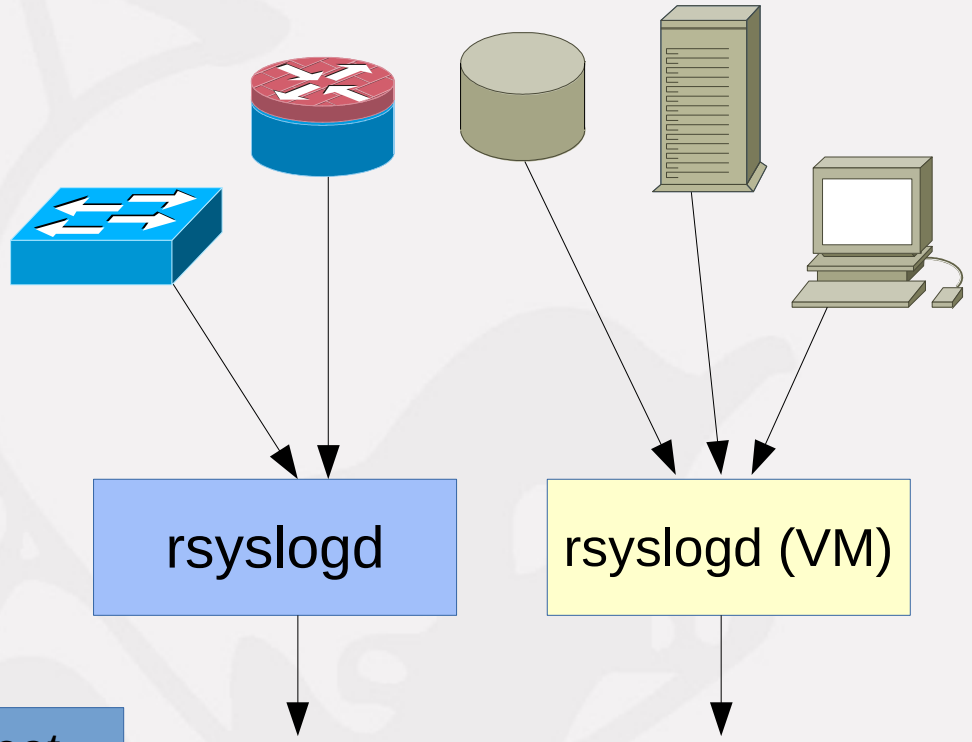
```
<34>1 2003-10-11T22:14:15.003Z mymachine.example.com su - ID47 - BOM'su root'
failed for lonvick on /dev/pts/8
<165>1 2003-10-11T22:14:15.003Z frodo.example.com postfix - ID47 -
[exampleSDID@17660 iut="3" eventID="1011" eventSource="Application"] - BOM Une
entré du journal des événements
```

Un esempio di utilizzo di lograptor

```
# lograptor --apps postfix --hosts=velociraptor --last=1h -e 'brunato'

*** Filename: /var/log/logdir/velociraptor/2018/05/maillog-20180522.log ***
May 22 13:59:49 velociraptor postfix-mta/smtps/smtpd[22497]: 7E1572612:
client=mrwolf.sissa.it[192.168.0.10], sasl_method=PLAIN, sasl_username=brunato

May 22 13:59:49 velociraptor postfix-mta/qmgr[2163]: 7E1572612: from=<brunato@sissa.it>, size=1437,
nrcpt=1 (queue active)

May 22 14:08:37 velociraptor postfix-mta/lmtp[612]: E6FF125B8: to=<brunato@sissa.it>,
orig_to=<apm@sissa.it>, relay=mda.sissa.it[192.168.0.11]:24, delay=0.27, delays=0.21/0.01/0/0.05,
dsn=2.0.0, status=sent (250 2.0.0 <brunato@sissa.it> cLd0BEUIBFuiGgAASpDaHg Saved)

May 22 14:18:15 velociraptor postfix-mta/smtpd[5278]: NOQUEUE: reject: RCPT from
mx.sissa.it[192.168.0.12]: 550 5.1.1 <brunatonn@sissa.it>: Recipient address rejected: User unknown in
virtual mailbox table; from=<double-bounce@mx.sissa.it> to=<brunato@sissa.it> proto=ESMTP
helo=<mx.sissa.it>

May 22 14:22:49 velociraptor postfix-mta/lmtp[10067]: 57B2B18A9: to=<brunato@sissa.it>,
orig_to=<lograptor@sissa.it>, relay=mda.sissa.it[192.168.0.11]:24, delay=0.22, delays=0.14/0/0/0.07,
dsn=2.0.0, status=sent (250 2.0.0 <brunato@sissa.it> GH0QGZkLBFueIwAASpDaHg Saved)

May 22 14:46:08 t-rex postfix-mta/lmtp[22799]: AA8F22612: to=<brunato@sissa.it>,
relay=mda.sissa.it[192.168.0.11]:24, delay=0.31, delays=0.23/0.01/0/0.07, dsn=2.0.0, status=sent (250
2.0.0 <brunato@sissa.it> UN+CLxARBFt5NQAASpDaHg Saved)

--- Lograptor run summary ---
Number of processed files: 1
Total lines read: 90789
Total log events matched: 6
Total log events for apps: postfix(15121)
```

Ipotesi per nuovo sistema

- Nagios core
- Elasticsearch + Kibana
- Collettore rsyslogd dei servizi su VM



Librerie Python per Elasticsearch

- **elasticsearch-py**
  - Libreria di basso livello
  - Low-level client come classe *Elasticsearch*
  - Accesso mediante metodi API REST like
- **elasticsearch-dsl**
  - Libreria di alto livello
  - Costruita sopra elasticsearch-py
  - Fornisce una classe *Search* che genera oggetti *Query*
  - Ricerche con query JSON DSL di Elastic
  - API simile ad altri pacchetti Python (SQLAlchemy, Django queryset)