UNIVERSITÀ
DI PARMA

PANEL Monitoring, logging, log retention

Update (sys)logging UNIPR a Elastic Stack

Andrea Barontini

UO Erogazione Servizi
Università degli Studi di Parma

andrea.barontini@unipr.it

- 29 Maggio 2018 -

legacy

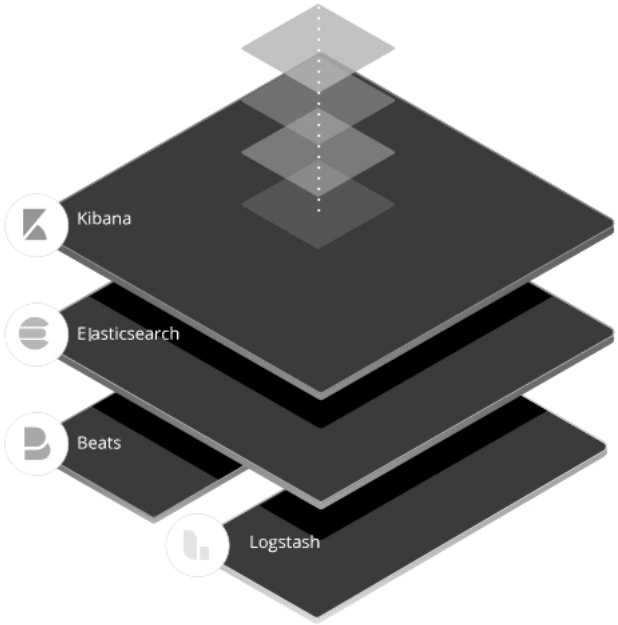
- Syslogd
  - Nodo fisico RHEL5 (8 GB, 500 GB, 8 core)
  - Network, wifi radacct, AD windows
  - 30-35 EPS ≃ 2,5-3 Mevents/d ≃ 20 Mevents/w
- Necessità
  - Consolidamento su ESX
  - Intanto che ci siamo svecchiamo?
  - Upgrade consapevolezza e fruibilità dati

looking around

- Novembre: discussione@garr.it
  - Raccolta ok, magari un po' di analytics
  - Lnx / Win? Supporto?
  - Graylog / ELK / LogAnalyze / …
- Dicembre di innamoramento, ma…
  - Tempo tiranno
  - Priorità mutevoli
  - Workaround (transizione non banale)
- Nuova linfa da questo Panel

stretching

- Intro su logz.io
  - Occhio, ES è NoSQL!
- Pacchetti Bitnami
  - VM e installer
    - MacBook Pro → Win10Pro → Win Srv 2012R2
- elastic.co doc & Beat
- NXLog Community Ed.



elastic datasources

- (Syslogd →) NXLog Syslog → ES
  - firewall, switch, VoIP
  - REST API via *om_http* (vs *om_elasticsearch* EE)
- Aruba Clearpass → Logstash → ES
  - *https://github.com/njohnsn/ClearPassAndELK*
- AD DC Events → Winlogbeat → ES
- Metriche ELK Server → Metricbeat → ES

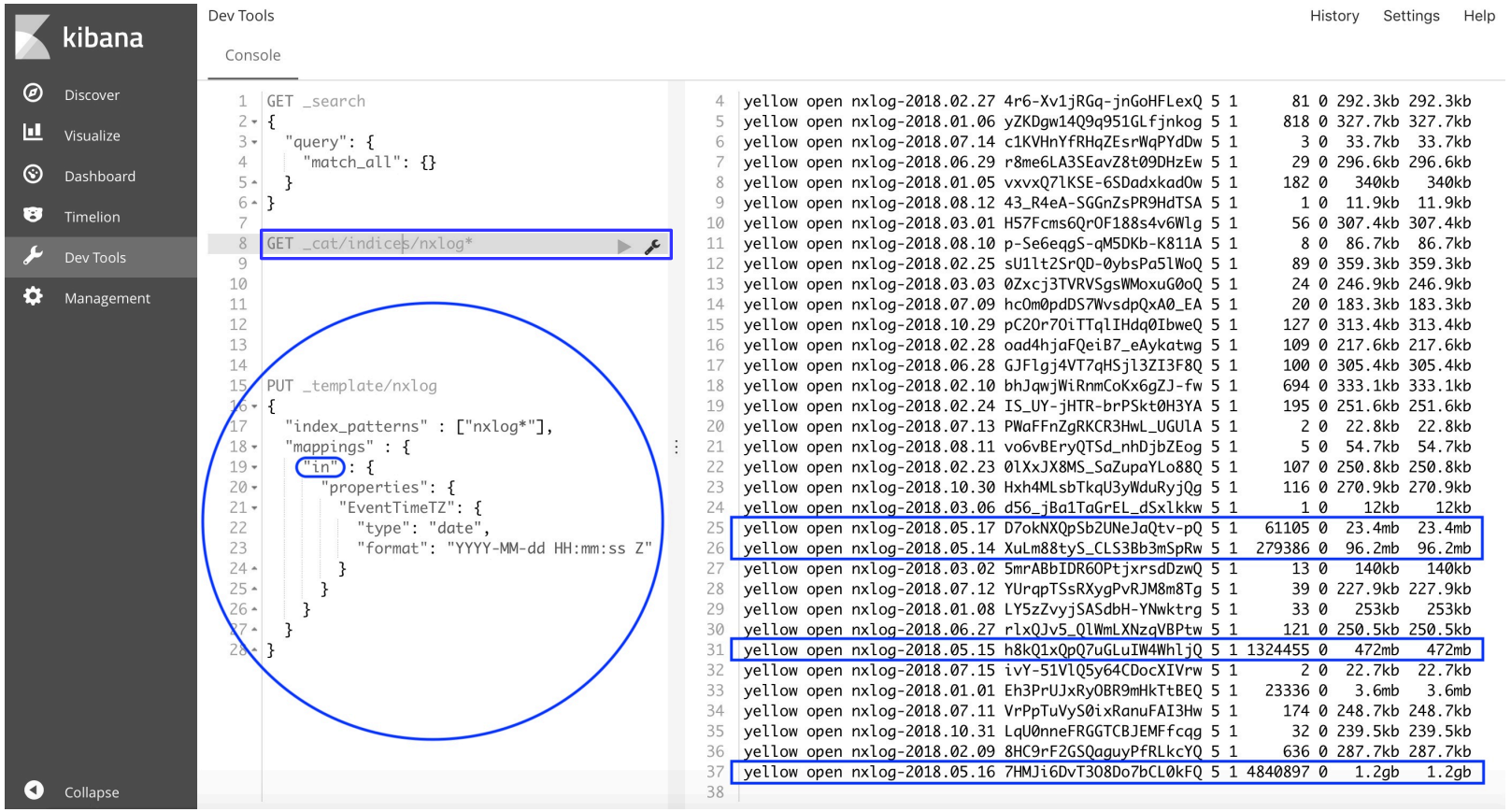
nxlog

```
<Extension _charconv>
    Module      xm_charconv
    AutodetectCharsets iso8859-2, utf-8, utf-16, utf-32
</Extension>

<Input in>
    Module  im_udp
    Port  514
    Host  160.78.48.60
    Exec  parse_syslog(); convert_fields("auto", "utf-8");
</Input>
```

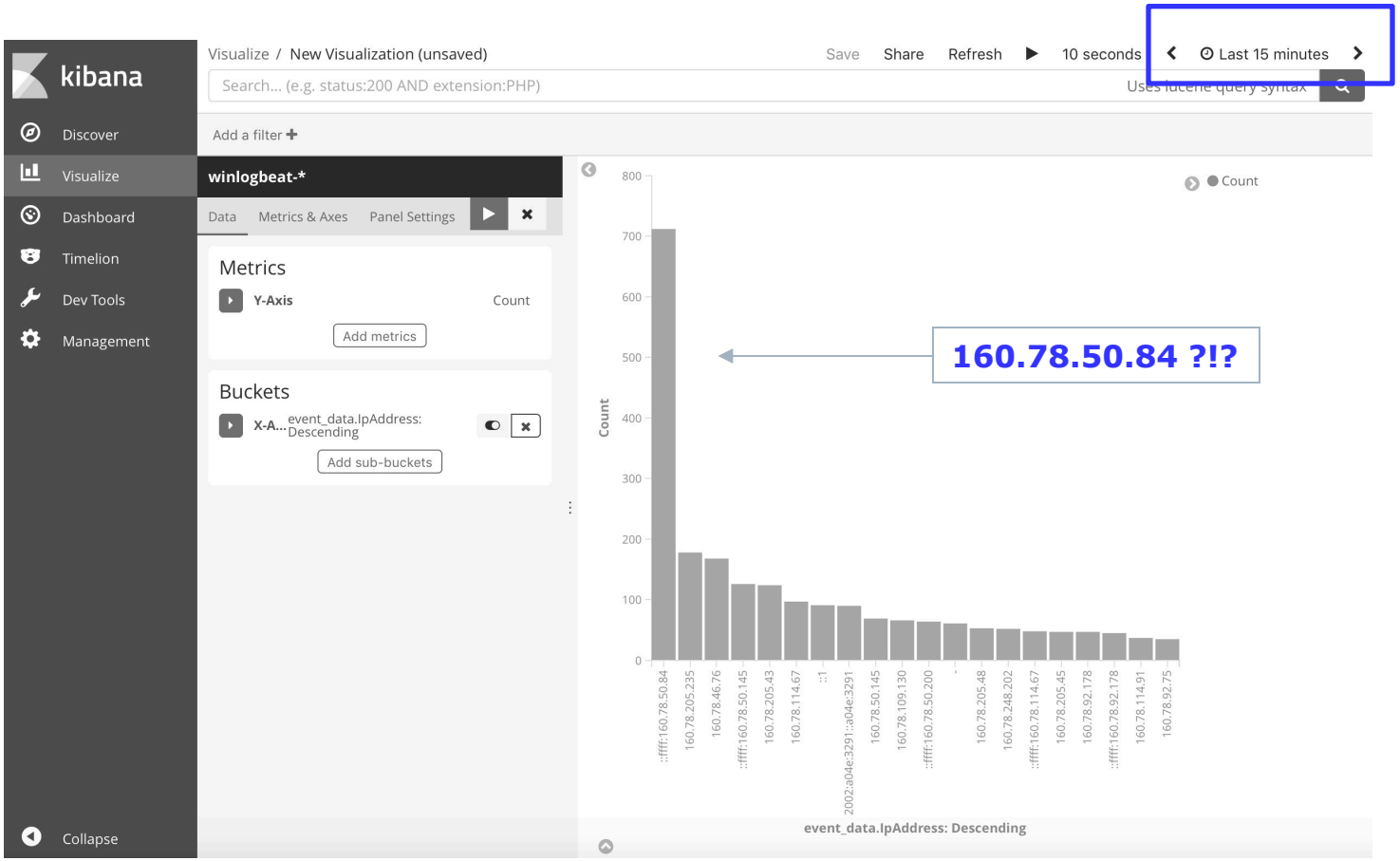
nxlog

```
<Output outELK>
    Module       om_http
    URL          http://127.0.0.1:9200
    ContentType  application/json
    <Exec>
        set_http_request_path(strftime($EventTime, "/nxlog-%Y.%m.%d/in"));

        if strftime($EventTime, "%Z") == "W. Europe Daylight Time"
                  set_var('fuso', '+0200'); else set_var('fuso', '+0100');
        $EventTimeTZ=strftime($EventTime, "%Y-%m-%d %H:%M:%S "
                                              + get_var('fuso'));
        to_json();
    </Exec>
</Output>
```

server ntp :-/


kibana
Discover
Visualize
Dashboard
Timelion
Dev Tools
Management
Collapse
Dev Tools
History
Settings
Help
Console
GET _search
{
"query": {
"match_all": {}
}
}
GET _cat/indices/nxlog*
PUT _template/nxlog
{
"index_patterns" : ["nxlog*"],
"mappings" : {
"in" : {
"properties": {
"EventTimeTZ": {
"type": "date",
"format": "YYYY-MM-dd HH:mm:ss Z"
}
}
}
}
}
yellow open nxlog-2018.02.27 4r6-Xv1jRGq-jnGoHFLexQ 5 1 81 0 292.3kb 292.3kb
yellow open nxlog-2018.01.06 yZKDgw14Q9q951GLfjnkog 5 1 818 0 327.7kb 327.7kb
yellow open nxlog-2018.07.14 c1KVHnYfRHqZEsrWqPYdDw 5 1 3 0 33.7kb 33.7kb
yellow open nxlog-2018.06.29 r8me6LA3SEavZ8t09DHzEw 5 1 29 0 296.6kb 296.6kb
yellow open nxlog-2018.01.05 vxvxQ7lKSE-6SDadxkadOw 5 1 182 0 340kb 340kb
yellow open nxlog-2018.08.12 43_R4eA-SGGnZsPR9HdTSA 5 1 1 0 11.9kb 11.9kb
yellow open nxlog-2018.03.01 H57Fcms6QrOF188s4v6Wlg 5 1 56 0 307.4kb 307.4kb
yellow open nxlog-2018.08.10 p-Se6eqgS-qM5DKb-K811A 5 1 8 0 86.7kb 86.7kb
yellow open nxlog-2018.02.25 sU1lt2SrQD-0ybsPa5lWoQ 5 1 89 0 359.3kb 359.3kb
yellow open nxlog-2018.03.03 0Zxcj3TVRVSgsWMoxuG0oQ 5 1 24 0 246.9kb 246.9kb
yellow open nxlog-2018.07.09 hcOm0pdDS7WvsdpQxA0_EA 5 1 20 0 183.3kb 183.3kb
yellow open nxlog-2018.10.29 pC2Or7OiTTqlIHdq0IbweQ 5 1 127 0 313.4kb 313.4kb
yellow open nxlog-2018.02.28 oad4hjaFQeiB7_eAykatwg 5 1 109 0 217.6kb 217.6kb
yellow open nxlog-2018.06.28 GJFlgj4VT7qHSjl3ZI3F8Q 5 1 100 0 305.4kb 305.4kb
yellow open nxlog-2018.02.10 bhJqwjWiRnmCoKx6gZJ-fw 5 1 694 0 333.1kb 333.1kb
yellow open nxlog-2018.02.24 IS_UY-jHTR-brPSkt0H3YA 5 1 195 0 251.6kb 251.6kb
yellow open nxlog-2018.07.13 PWaFFnZgRKCR3HwL_UGUlA 5 1 2 0 22.8kb 22.8kb
yellow open nxlog-2018.08.11 vo6vBEryQTSd_nhDjbZEog 5 1 5 0 54.7kb 54.7kb
yellow open nxlog-2018.02.23 0lXxJX8MS_SaZupaYLo88Q 5 1 107 0 250.8kb 250.8kb
yellow open nxlog-2018.10.30 Hxh4MLsbTkqU3yWduRyjQg 5 1 116 0 270.9kb 270.9kb
yellow open nxlog-2018.03.06 d56_jBa1TaGrEL_dSxlkkw 5 1 1 0 12kb 12kb
yellow open nxlog-2018.05.17 D7okNXQpSb2UNeJaQtv-pQ 5 1 61105 0 23.4mb 23.4mb
yellow open nxlog-2018.05.14 XuLm88tyS_CLS3Bb3mSpRw 5 1 279386 0 96.2mb 96.2mb
yellow open nxlog-2018.03.02 5mrABbIDR6OPtjxrsdDzwQ 5 1 13 0 140kb 140kb
yellow open nxlog-2018.07.12 YUrqpTSsRXygPvRJM8m8Tg 5 1 39 0 227.9kb 227.9kb
yellow open nxlog-2018.01.08 LY5zZvyjSASdbH-YNwktrg 5 1 33 0 253kb 253kb
yellow open nxlog-2018.06.27 rlxQJv5_QlWmLXNzqVBPtw 5 1 121 0 250.5kb 250.5kb
yellow open nxlog-2018.05.15 h8kQ1xQpQ7uGLuIW4WhljQ 5 1 1324455 0 472mb 472mb
yellow open nxlog-2018.07.15 ivY-51VlQ5y64CDocXIVrw 5 1 2 0 22.7kb 22.7kb
yellow open nxlog-2018.01.01 Eh3PrUJxRyOBR9mHkTtBEQ 5 1 23336 0 3.6mb 3.6mb
yellow open nxlog-2018.07.11 VrPpTuVyS0ixRanuFAI3Hw 5 1 174 0 248.7kb 248.7kb
yellow open nxlog-2018.10.31 LqU0nneFRGGTCBJEMFfcqg 5 1 32 0 239.5kb 239.5kb
yellow open nxlog-2018.02.09 8HC9rF2GSQaguyPfRLkcYQ 5 1 636 0 287.7kb 287.7kb
yellow open nxlog-2018.05.16 7HMJi6DvT3O8Do7bCL0kFQ 5 1 4840897 0 1.2gb 1.2gb

winlogbeat dei DC…

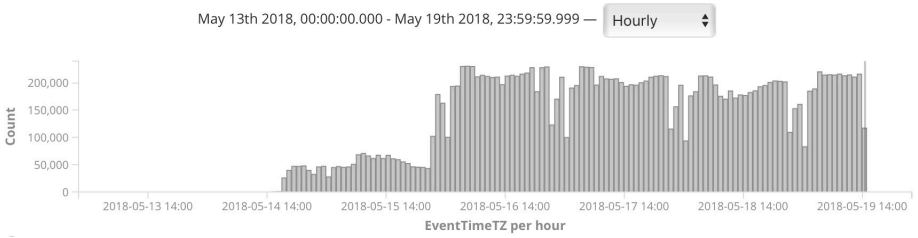


…e metricbeat

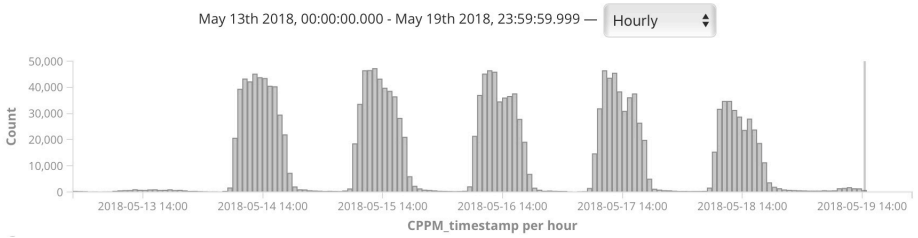
- *beat
  - Win/Linux/MacOS
    - Go
  - No deps
  - Light
  - Conf: *.yml ☹
- Filebeat
  - Back-pressure w/ Logstash
  - TMZ via ES ingest pipeline
  - RHEL5 no service, ma ok ☺

dove?

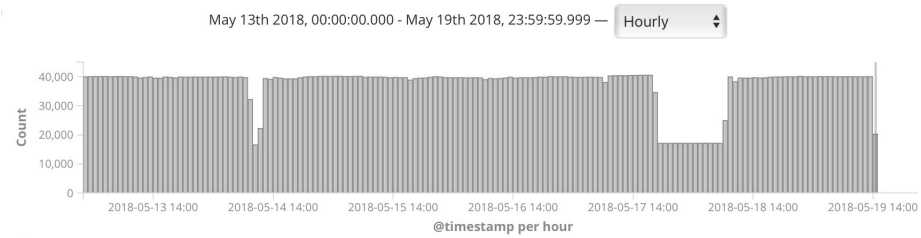
VM ESX WinSrv 2012R2 w/ 4 vCPU @2GHz, 16GB RAM, 500GB HD



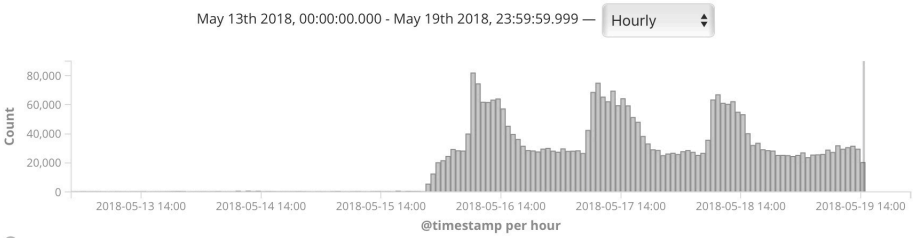
NXLog: 64 EPS (50 fw)



Clearpass: 13 EPS



Metricbeat: 11 EPS



Winlogbeat: 22 EPS

todo

- Dismissione Syslogd, ruolo NXLog?
- Ulteriori datasource (DHCP e CAS per es.)
- Dashboard (SFX per l'ego ☺)
- More ES, no X-Pack
  - Auth (*mod_auth**? NGINX?)
  - 'SQL' (*github.com/NLPchina/elasticsearch-sql*)
  - Trigger? ML?