



**WORKSHOP
GARR 2020**



L'esperimento "Social" della Community: (il Bar del) GarrLab

Damiano Verzulli
damiano@verzulli.it



APM GARR
Università "G. d'Annunzio"
di Chieti-Pescara
<http://www.unich.it>

APM GARR
ICRANET Research Center
Pescara
<http://www.icranet.org>



“...da dove venite?”

- ...tutto parte dal “grido di dolore” lanciato al WS17...

Possiamo “reggere”?

Tecnologie sempre più pervasive => coperture IP sempre più ampie

Contesto normativo sempre in (pericolosa) evoluzione

“Storm” quotidiano di nuovi paradigmi (SDN, SDS, IaaS, cloud...)

Utenti sempre più esigenti e affamati di servizi

**IMHO,
non potendo scalare,
il destino
[verso la sconfitta]
è segnato!**

Banda IP sempre maggiormente disponibile!

Packet-Loss “significativo” (ed in aumento) fra MNGMT e OPER

Disponibilità di tecnologie SW impensabili solo pochi anni fa!

“Tentazioni” pro-Cloud sempre più “forti” ed efficaci!

Evoluzione delle tecnologie HW estremamente rilevante

Il “futuro” (...ed il “presente”) visto da un (piccolo) ufficio “Reti e Sistemi”

Dr. Damiano Verzulli - GARR WS 17 - Roma - 05/04/2017

Slide 9/14 

GARR WorkShop
2017

Intervento del
05/04/2017
dal titolo:

Il “futuro”
(...ed il “presente”) visto da un (piccolo) ufficio
“Reti e Sistemi”

Slide 9

“...da dove venite?”

- ...e dal relativo “desiderata”

Mi piacerebbe.... *(...solo esempi)*

- ...leggere di un Ateneo che ha un “backup” di cui è soddisfatto... e ci racconta come è fatto;
- ...poter evitare di spendere un giorno a mettere in piedi un accrocchio di ElasticSearch per sparargli dentro un po' di LOG e... esercitarmi nella log-analysis
- ...poter inviare a “qualcosa” i miei 400 log/sec ed averne indietro una dashboard di Kibana da poter personalizzare
- ...poter spegnere i miei blade e non preoccuparmi di VMware o XenServer, o, peggio della SAN, avendo calcolo e storage equivalenti, altrove... ma in contesti NREN;
- Che qualcuno, ogni tanto, mi venga a trovare e... in 20 minuti capisce “chi siamo” e ci dice: *“Ehi! Questo potrebbe servire a Y! Z, invece, ha fatto esattamente quello di cui hai bisogno!!”*
- Discutere, con gente competente, del rapporto fra “Controllo” e “Cloud”, fra “privacy” e “gestione infrastrutturale”, etc.;

...e mi piacerebbe NON sentirmi un visionario

GARR WorkShop
2017

Intervento del
05/04/2017
dal titolo:

Il “futuro”
(...ed il “presente”)
visto da un (piccolo)
ufficio
“Reti e Sistemi”

Ultima slide

“...eravamo quattro amici al Bar...”

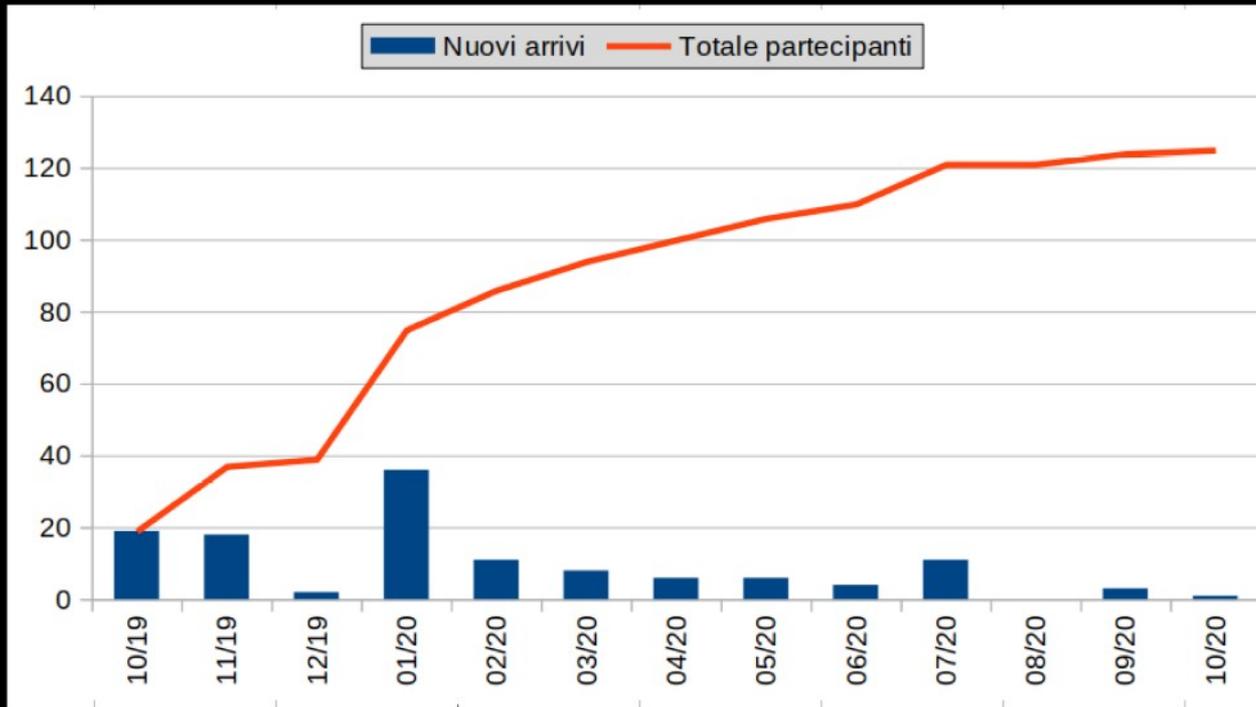
- Durante un coffee-break del **WS19**, scocca la scintilla: l'esigenza viene palesata anche da altri che condividono l'idea di “fare qualcosa”:
 - ✓ Giuseppe De Marco - UniCalabria
 - ✓ Francesco Izzi - CNR
 - ✓ Ermann Ripepi – CNR
- Due giorni più tardi, l'**11/10/2019**, nasce il gruppo Telegram dei

“GARRisti Operativi (*al Bar*)”

“Chi siete?”

- Con un moderato filtro all'ingresso ed una attenzione a non trasformarlo nel luogo di incontro degli alcolisti anonimi, il Bar è andato via via crescendo (come frequentatori e come volume di discussioni)
- Una costante è stata (ed è) quella di non snaturarne l'origine: **il Bar è dei “GARRISTI OPERATIVI”**, ossia di tutti coloro che vedono in GARR il “Grande Padre della Connettività” (*Principalmente Atenei, ma anche CNR, INFN, ed altri Enti [...oltre a GARR stesso ed a qualche “intruso”]*)

“Si, ma quanti siete?”



69 @ ~ 37 Atenei
19 @ Altri enti
28 @ GARR
3 @ (altro)

119 umani presenti
(+ 1 bot)

6 ci hanno salutato
(5 deleted account)

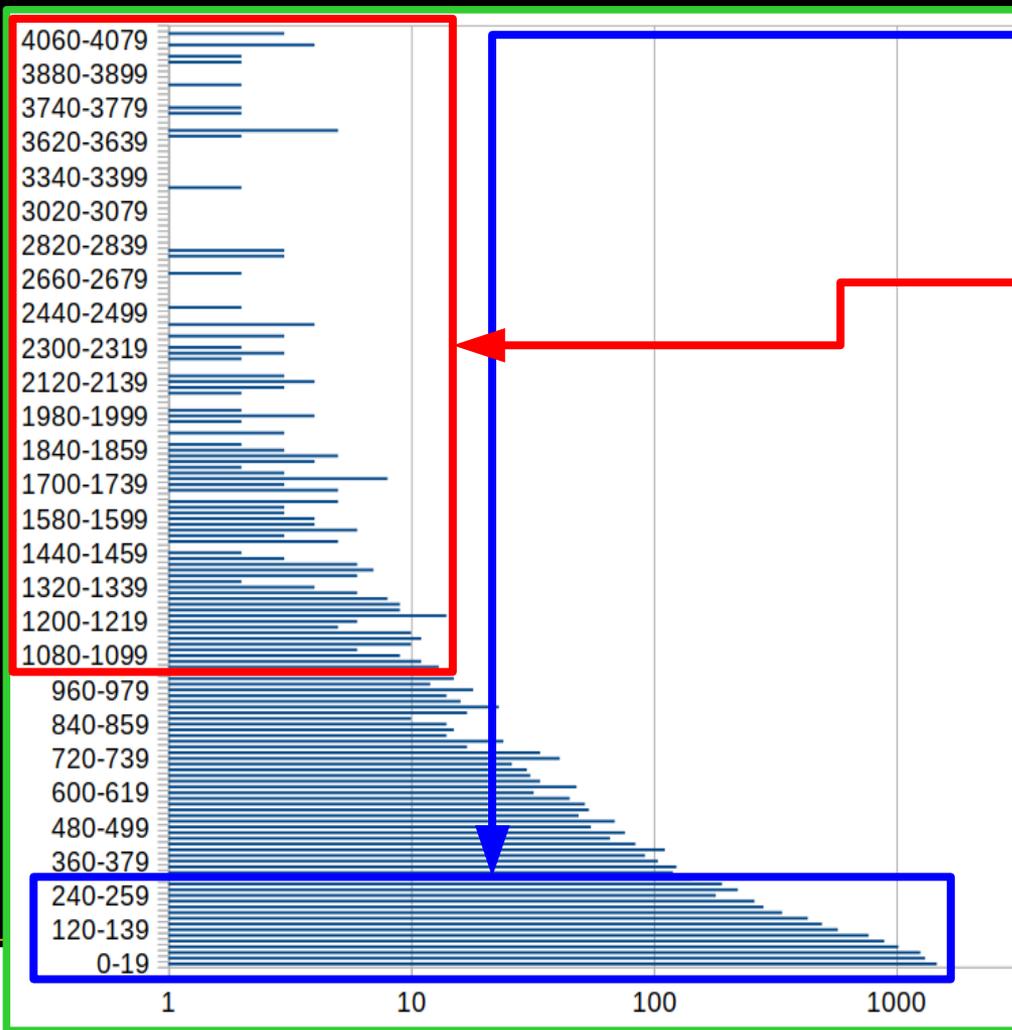
Pochi? Molti? ...Non so dirvelo :-)

**Quello che so, però, è che il rapporto
“segnale/rumore” è *MOLTO* elevato!**



...e cosa dite?

- Distribuzione dei messaggi, per numero dei caratteri (**SCALA LOGARITMICA!**)



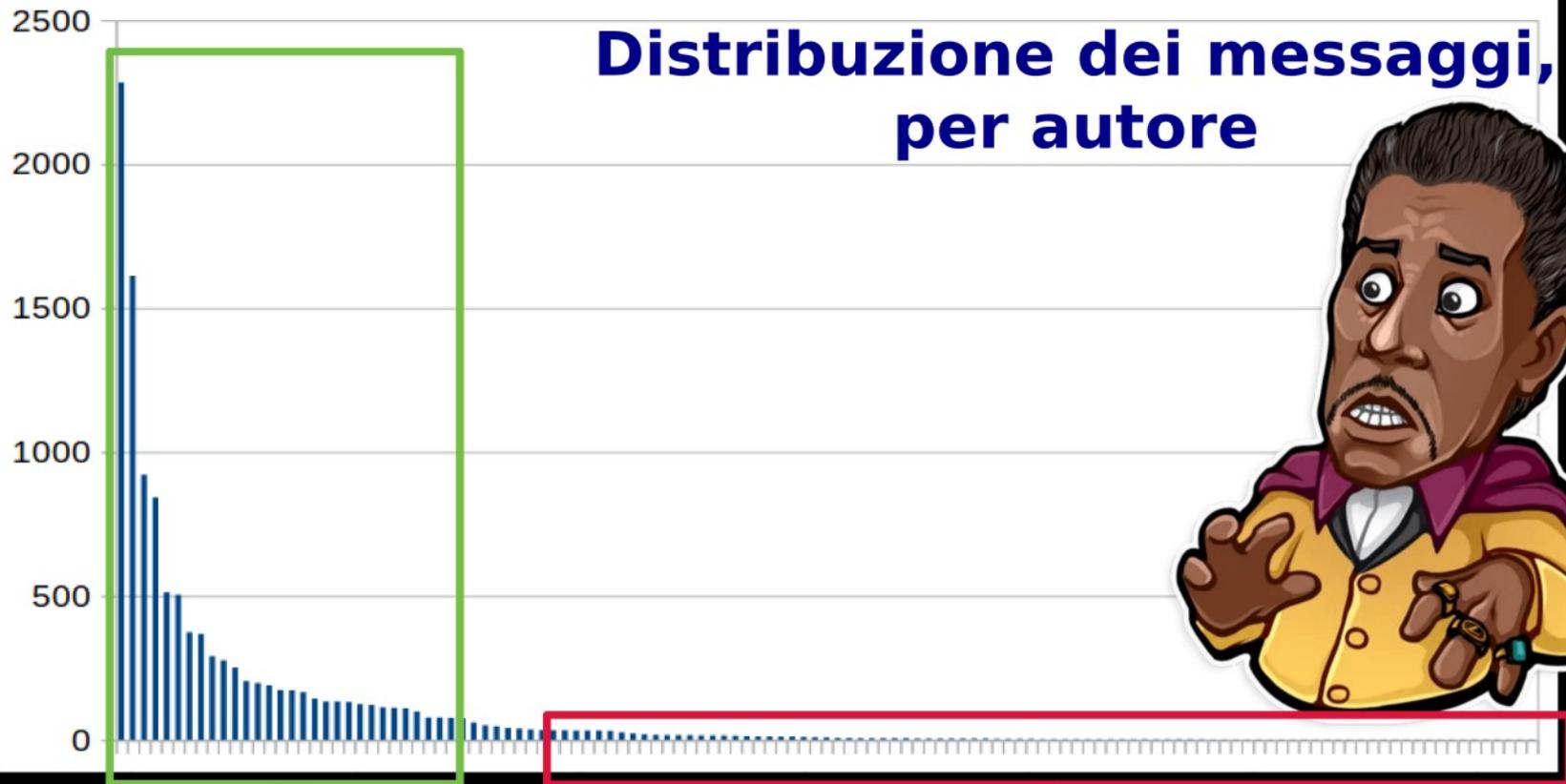
Molti messaggi sono particolarmente brevi (< ~250 char).

Ma i messaggi particolarmente densi di contenuto sono un numero rilevante!

IMHO, è sufficiente anche solo un singolo messaggio "giusto", per dare un senso a questo esperimento

Rose e fiori?

Distribuzione dei messaggi, per autore



**Il gruppo vive grazie
al 20/30% degli iscritti**

**Più del 50% degli iscritti,
di fatto,
NON HA MAI POSTATO!**

Qualche “Perla”!

- In un anno di attività, il Bar ha prodotto delle vere e proprie “perle” di conoscenza (ordine delle decine). Messaggi per i quali –IMHO– è valsa la pena di esserci... e (almeno) “leggere”
- Ne ho estratte **TRE**:
 - **Chiedo scusa in anticipo a tutti quelli che non citerò**: Non sarebbe possibile;
 - D'altronde ritengo necessario far capire cosa intendo per “perla”



Qualche “Perla”!



- Un paio di “trattati” sul SIEM di **Simone Bonetti** (CERT-UniBo)

“....Vi sento parlare di SIEM e da quel che recepisco ho la sensazione che non abbiate capito molto della cosa

[...]

- Non avete del tempo per addestrare un SIEM? Allora non avete bisogno di un SIEM...

- Wazuh è troppo difficile/ostico? Un SIEM commerciale non lo sarà di meno

- Wazuh non mi risolve il problema! => Un SIEM è un oggetto che segnala problemi. La reazione al problema va capita è ingegnerizzata.

[...]

il SIEM (open/closed non fa differenza) è una enorme lente d'ingrandimento: come ogni sistema di analisi vi fa vedere cose che voi umani non volete vedere :-D....”

Qualche “Perla”!



- Considerazioni “dal campo” sul complesso mondo del CLOUD

di Federico Zani - INFN

“[Damiano] Lato GARRLab, ad esempio, un vincolo irrinunciabile era che “noi” (gestori) fossimo autonomi (sul firewalling) al 100%. Chiaramente questo ha un costo: non abbiamo utilizzato affatto i security groups di OpenStack e... abbiamo allestito due VM “dedicate” a questo scopo (una a PA, l'altra a CT). Il tutto era possibile grazie allo IAAS messoci a disposizione (OpenStack)

[Federico] Qui secondo me vi siete tagliati da soli fuori dal bello di avere sistemi cloud sotto al sedere: senza funzionalità come i sec group, load balancer as a service, automazione, etc, OpenStack diventa un “semplice” sistema per fare spawn di vm.

[...e tutta un'altra lunga serie di considerazioni interessanti...]

Qualche “Perla”!



- Router di backbone (GARR; 10G) implementato con una VM Linux

di Fabio Pedretti - UniBS

“ la VM "router" ha due interfacce: eth0 untagged su cui arriva solo il link GARR. Ed eth1 su cui ci stanno tutte le VLAN interne [...]

Routing: solo statico

Firewall: iptables + varie blacklist caricate con il tool di FireHOL (che usa ipset e ottimizza le regole consolidando le reti [...])

I server sono 3 Dell PowerEdge con 2 socket Xeon, complessivamente le CPU sono utilizzate circa al 25%.

La VM del firewall attualmente ha 6 core e sono usati durante il traffico di punta circa al 70%...”

Realizzato internamente a costo zero, ha consentito risparmi significativi in termini di TCO

...anche tanto vino buono!

Oltre alle “perle”, ci sono stati anche numerosi (~ cinquantina) spunti di discussione che non sarebbero esistiti... senza il Bar. Qualche esempio:

- ✓ Troubleshooting di un problema con Facebook @ UniBS + UniCH + UniParthenope (192.167.0.0/20)
- ✓ Analisi e troubleshooting del DDOS/Reflection “Lottomatica” (con annesso SYN-Flood outbound)
- ✓ Spunti e discussioni su temi importanti (Privacy; Supporto alla Didattica; Aspetti normativi; Bandi/opportunità; lo stesso GARR ed il ruolo di APM)

Che tutto questo sia accaduto esclusivamente “pro-bono” lo considero un SUCCESSO!



Le “sale fumatori”

Qualche volta gli ospiti del Bar hanno chiesto le chiavi di una “sala fumatori”. Sulla porta c’era (c’è) scritto:

- ELK
- Infrastruttura AD
- Infrastruttura GarrCloud
- SIEM - Wazuh
- Altre volte gli stessi ospiti hanno scovato qualche altro piccolo bancone:
 - “GARRisti Tech...nicisti (al Bar)” (36 banconisti)
 - “GARRisti Makeristi” (12 banconisti)

Ho la sensazione (mia; personale) che il Bar sia diventato un posto dove, “finalmente”, si possono condividere “gioie e dolori” del proprio lavoro (...e del proprio DNA “tecnico”)

L'officina di fianco al Bar

Poco dopo l'apertura del Bar, abbiamo chiesto al.... proprietario dell'Immobile (ndr: GARR) di darci una "officina", dove divertirci a fare "tuning" delle nostre auto.

Un "GRAZIE, GARR" a nome di tutta la community: senza di voi, tutto questo NON sarebbe stato possibile.

*Un grazie "particolare" a **Massimo Carboni** (per il tempo e le risorse dedicate ai banconisti) ed a **Claudia Battista** (per la fiducia mostrata nei nostri confronti)*



L'officina di fianco al Bar

l'officina è un posto... strano:

- È ampia e ricca di strumenti al punto tale da rendere possibile... qualunque attività;
- È piena di carrelli con dentro attrezzi mai visti. Di alcuni si è sentito parlare; di altri si ignorava l'esistenza... e non si sa come utilizzarli;
- Alcuni attrezzi suscitano sensazioni di "amore/odio": li vorresti prendere ed usare... ma sai che –quasi certamente– ti farai male.



*L'intera sessione pomeridiana
del Workshop
sarà dedicata all'officina!*



L'officina... fa miracoli :-)

In officina ci sono diversi che lavorano (~ decina) e diversi che hanno dato un'occhiata (~ ventina).

Alcuni hanno creato dei veri e propri "tesori":



➤ Progetto "ecs-logstash"

di Michele Albrigo - UniVerona

Fra APR e GIU 2020, Michele ha pubblicato – in "31 commit":

- il template degli indici di Elasticsearch utilizzati per la raccolta dei suoi LOG in formato ECS
- le sue 13 pipelines utilizzate per filtrare, analizzare ed arricchire i log di DHCP, DNS, NGFW, Radius, Switch, VPN, Wifi, Load Balancer...

**...ovviamente è tutto in officina,
a disposizione di tutti!**

conclusioni

- Più che “concludere” qualcosa, questa presentazione vuole essere un pit-stop, dal quale ripartire (più e meglio di prima)
- E quindi apriamo le porte del Bar è... invitiamo tutti (...*gli “operativi” amici del GPC*) a fare un salto:



GARRisti Operativi (al BAR)

 <https://url.garrlab.it/zfz9b>

N.B.: la porta resterà aperta tutt'oggi. Se entrate, cortesemente, presentatevi (nome, cognome, Ente di appartenenza). Se la trovate chiusa, bussatemi: @Damiano_Vorzulli (Telegram ; la mia porta è SEMPRE aperta!).

Quei brutti e cattivi banconisti...



Andrea Barontini.jpg



Daniele Albrizio.jpg



Enrico Ardizzoni.jpg



Ermann Ripepi.jpg



Fabio Pedretti.jpg



Federico Zani.jpg



Francesco Izzi.jpg



Gabriele Brandolini.jpg



Giancarlo Galluzzi.jpg



Giorgio Giorgetti.jpg



Giuseppe De Marco.jpg



Leonardo Lanzi.jpg



Luca Vanni.jpg



Marco Marletta.jpg



Marco Pirovano.jpg



Michele Albrigo.jpg



Nunzio Napolitano.jpg



Roberto Passuello.jpg



Salvatore Todaro.jpg



Simone Bonetti.jpg

Grazie!

L'esperimento "Social" della community: (il Bar del) GarrLab

Damiano Verzulli - GARR WS 20

on-air @ 02/11/2020