Consortium GARR
THE ITALIAN EDUCATION & RESEARCH NETWORK

Logging eduroam

Pasquale Mandato

Roma, 29/05/2018
Workshop GARR 2018

“

Definizione: *eduroam (education roaming) is the secure, world-wide roaming access service developed for the international research and education community.*

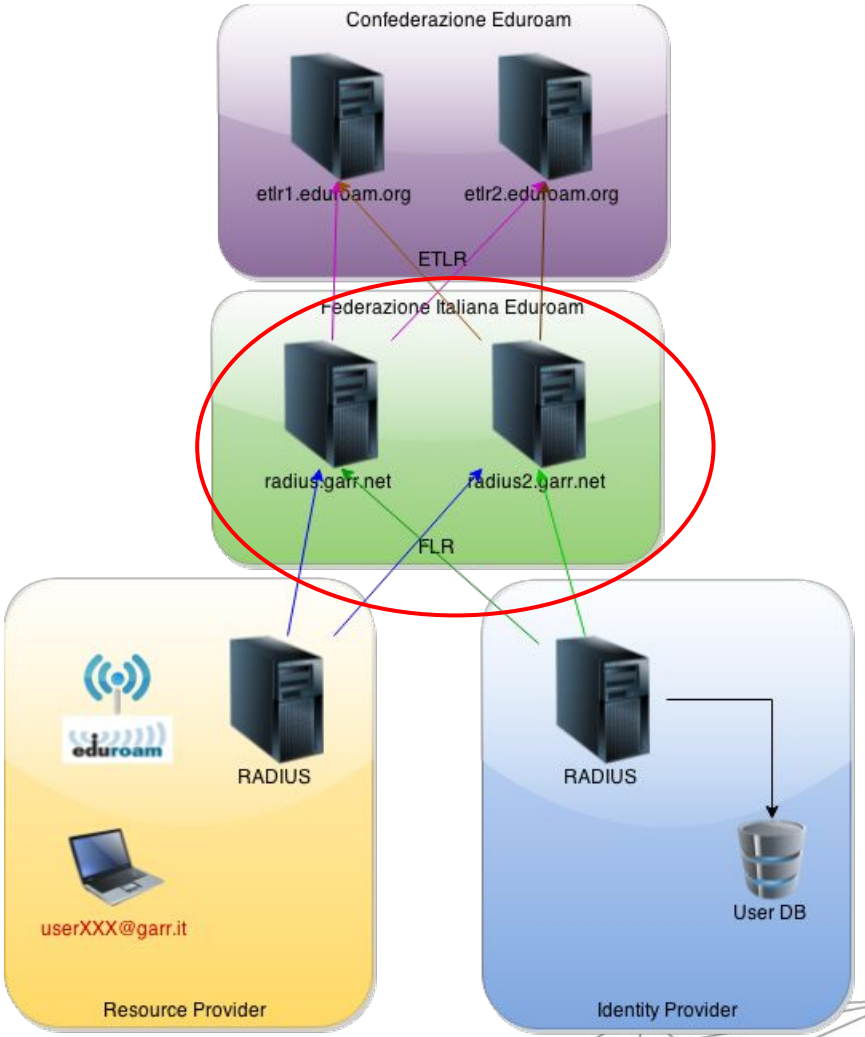
eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop.

”

Contesto di riferimento

Infrastruttura:

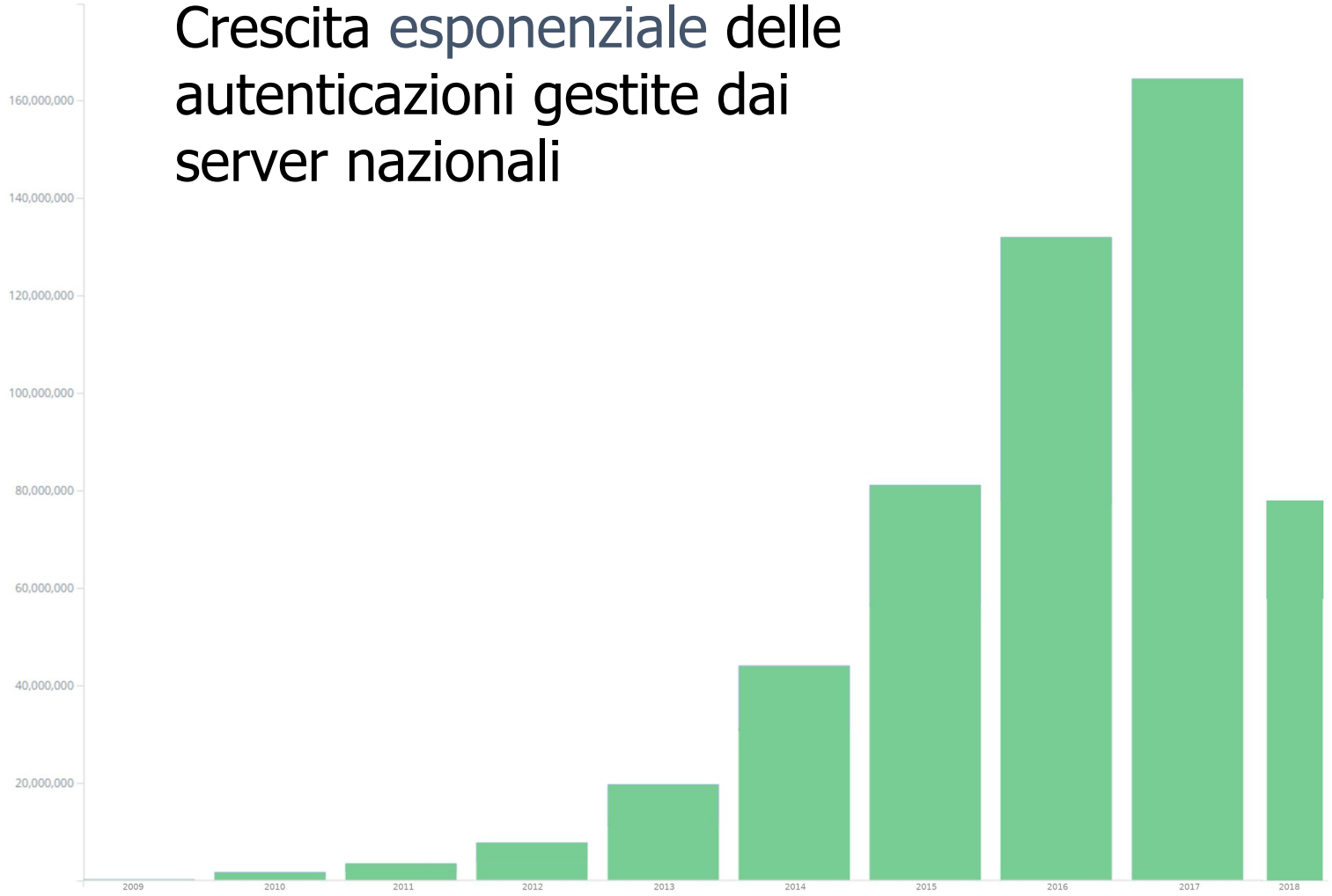
- **RO** (NREN): operatore del servizio nazionale o regionale -> Italia = *Consortium GARR*
- **IdP**: entità che crea e manutiene gli account per gli utenti -> *home institution*
- **RP**: entità che offre un accesso eduroam -> *visited institution*
- **Confederazione**



Contesto di riferimento

Definizione
Infrastruttura
Statistiche
Log

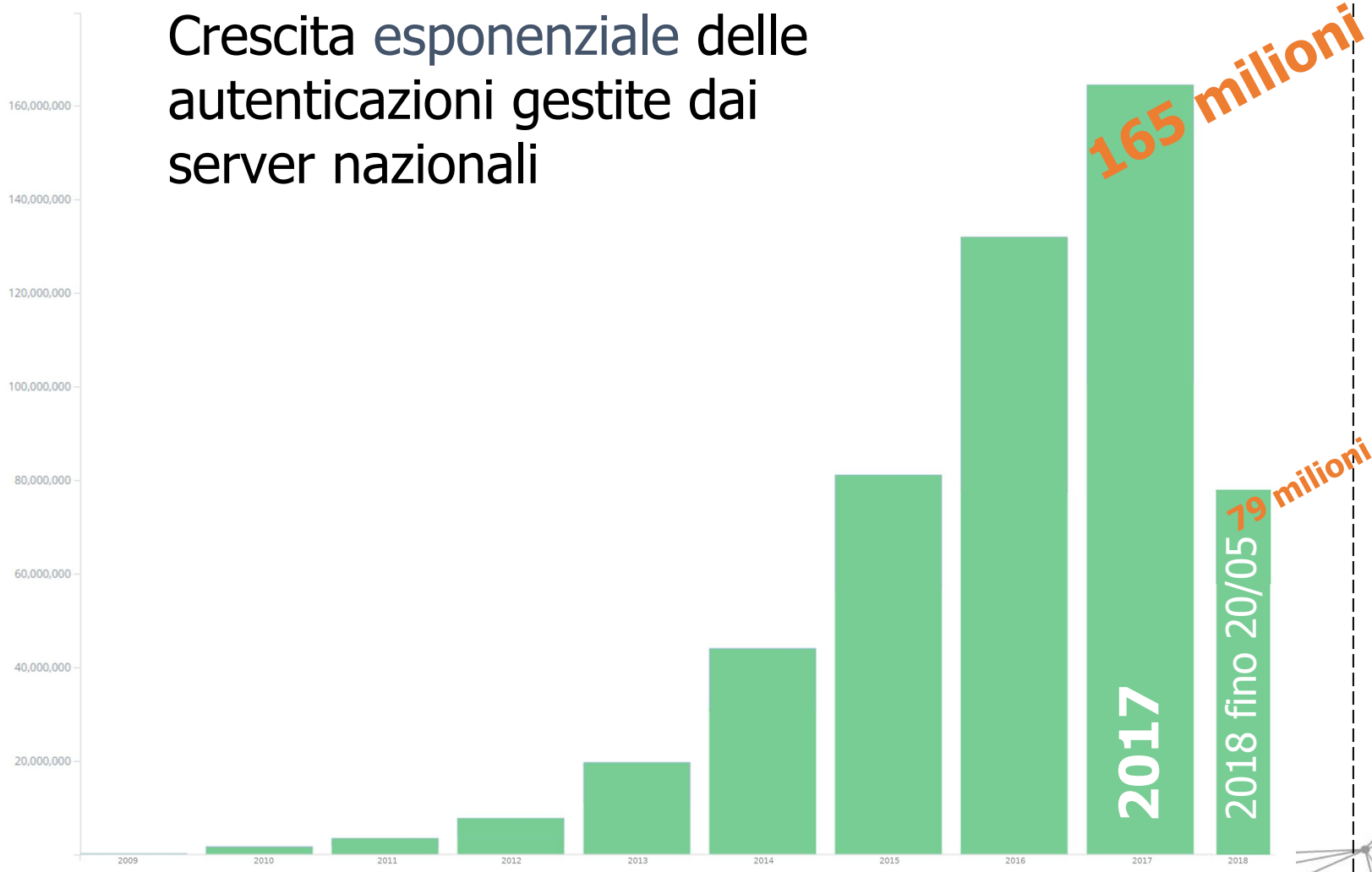
Crescita esponenziale delle autenticazioni gestite dai server nazionali



Contesto di riferimento

Definizione | Infrastruttura | **Statistiche** | Log

Crescita esponenziale delle autenticazioni gestite dai server nazionali



Consortium GARR | THE ITALIAN EDUCATION & RESEARCH NETWORK

Contesto di riferimento

Definizione | Infrastruttura | Statistiche | **Log**

Log:

Fri May 18 10:09:40 2018: **DEBUG**: Rewrote user name to *********@realm.tld
Fri May 18 10:09:40 2018: DEBUG: Packet dump:
*** Received from 160.97.*.* port 32904 ....
Code: **Access-Request**
Identifier: 72
Authentic: F&y<223><221><29><27>t<168><173>"<229><196><154><14><253>
Attributes:
User-Name = "*********@realm.tld"
NAS-IP-Address = 127.0.7.1
Called-Station-Id = "00:1f:45:**:**:**"
Calling-Station-Id = "04:db:56:**:**:**"
NAS-Identifier = "128-eduroam-S2"
EAP-Message = <2><0><0>&<1>*********@realm.tld
Message-Authenticator = .{<1><176><1><226><253><146>S**********
Operator-Name = "*********"
Proxy-State = 10

...

Fri May 18 10:09:40 2018: DEBUG: Received reply in AuthRADIUS for req 3 from 141.108.*.*:1812
Fri May 18 10:09:40 2018: DEBUG: Rewrote user name to *********@realm.tld
Fri May 18 10:09:40 2018: DEBUG: Packet dump:
*** Received from 141.108.*.* port 1812 ....
Code: **Access-Accept**
Identifier: 3
Authentic: <13><172>C<155><11><210><206>\3<202><13><26><206><159><137><211>
Attributes:
MS-MPPE-Recv-Key = <170><179>#B<30>@<171>dS8<194>R<31><237>M<17> <0><227><220>**********
MS-MPPE-Send-Key = <26>zR<235>:uB<19>R<15><29>t<191><167><214><1><9><2><170>**********
EAP-Message = <3><8><0><4>
Message-Authenticator = **********

Contesto di riferimento

Definizione
Infrastruttura
Statistiche
Log

Log:

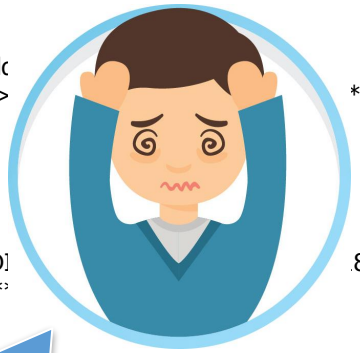
Fri May 18 10:0[illegible]e to *********@realm.tld
Fri May 18
*** Rec
Code:
Iden
Auth [illegible]196><154><14><253>
Attril
N
Call
Calling-
NAS-Identifier
EAP-Message = <2><0><0><1>********[illegible]m.tld
Message-Authenticator = .{<1><176><1><226><253>
Operator-Name = "*********"
Proxy-State = 10

...

Fri May 18 10:09:40 2018: DEBUG: Received reply in AuthRAD[illegible]812
Fri May 18 10:09:40 2018: DEBUG: Rewrote user name to ***
Fri May 18 10:09:40 2018: DEBUG: Packet dump:
*** Received from 141.108.*.* port 1812 ....
Code: **Access-Accept**
Identifier: 3
Authentic: <13><[illegible]><206><159><137><211>
Attributes:
[illegible]>M<17> <0><227><220>**********
[illegible]<1><9><2><170>**********

Dimensioni:
20GB/giorno

Verbose
Multiline
No correlation



Attesa decompressione
Attesa output ricerca
Semplice *grep* non sufficiente

Problemi

- Troubleshooting utente
  - nazionale
  - internazionale
- Troubleshooting ente/radius
- Compliance con *eduroam Service Definition*
  - attributi richiesti
- Monitoring

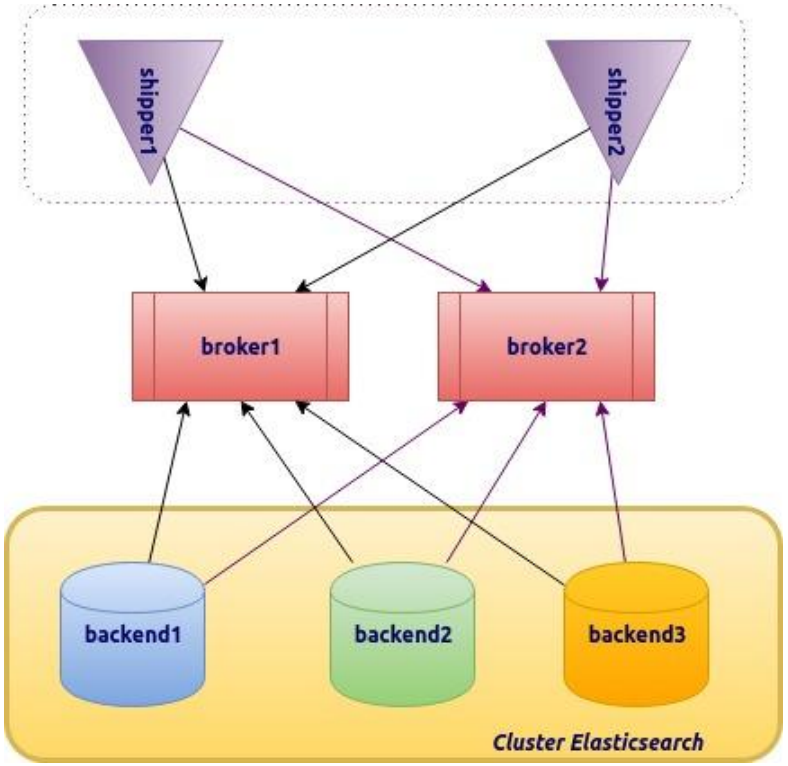
Problemi

- Troubleshooting utente
  - nazionale
  - internazionale
- Troubleshooting ente/radius
- Compliance con *eduroam Service Definition*
  - attributi richiesti
- Monitoring

Non più gestibile con i sistemi tradizionali

> *Misura ciò che è*
> ***misurabile***
> *e* ***rendi misurabile***
> *ciò che non lo è.*

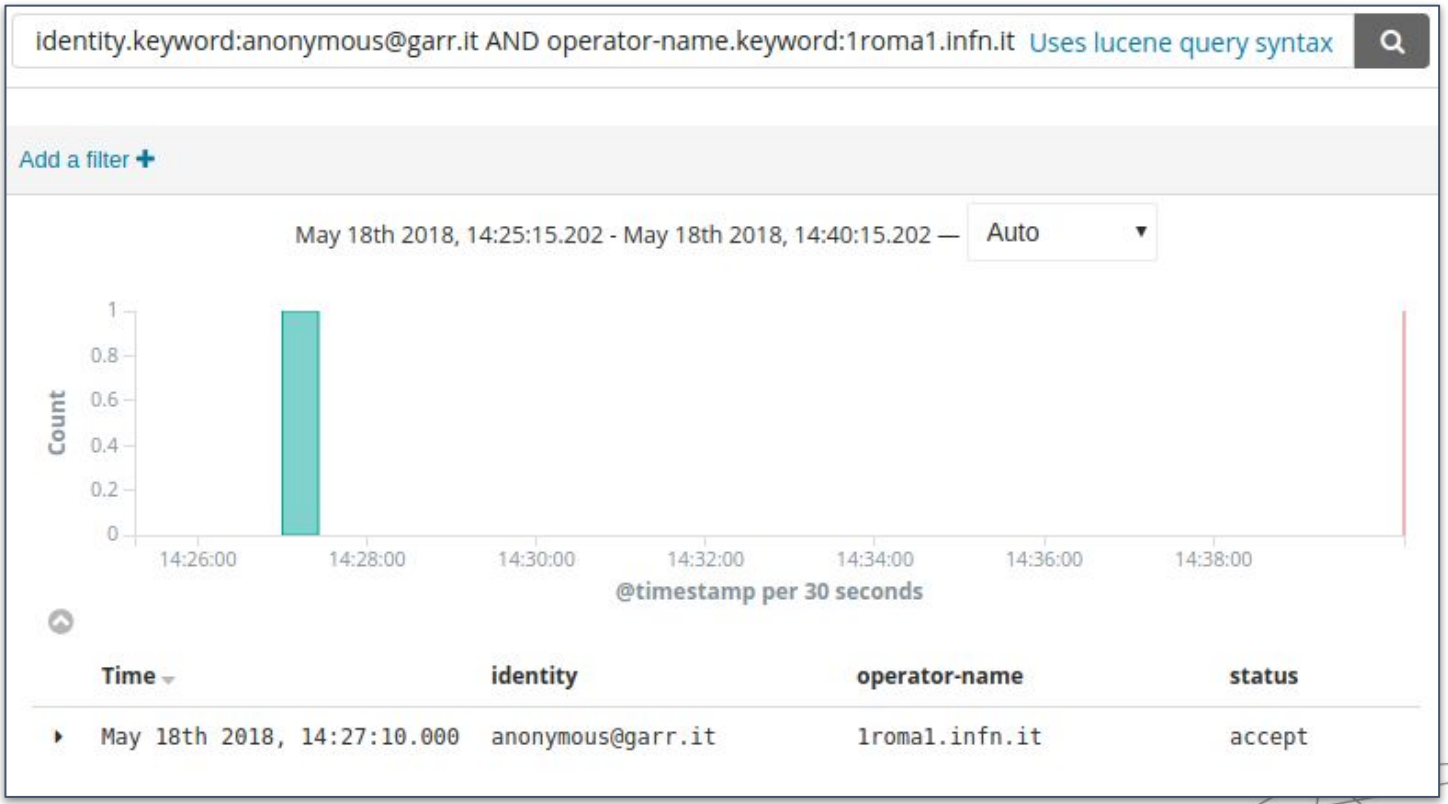
- Centralizzare i log dei radius nazionali
- ELK: Elasticsearch + Logstash + Kibana
  - 2 nodi frontend
  - 2 nodi queue
  - 3 nodi di backend:
    - elasticsearch
    - logstash
    - kibana



Totale: 18 vCPU/32 GB RAM

Troubleshooting (1/2)

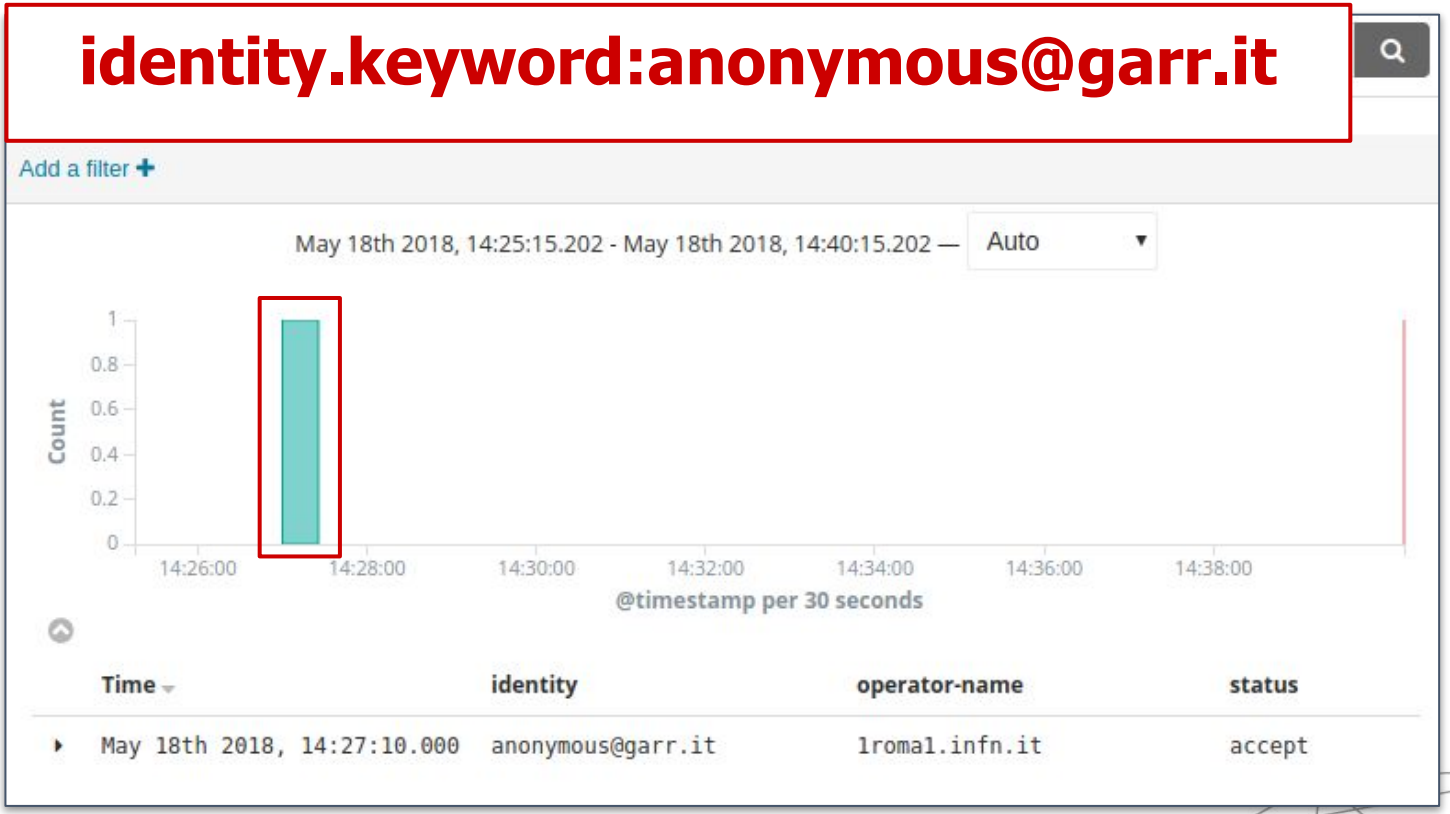
- Le richieste di autenticazione transitano correttamente sulla federazione?
- L'utente non si collega è un caso isolato?



Troubleshooting (1/2)

- Le richieste di autenticazione transitano correttamente sulla federazione?
- L'utente non si collega è un caso isolato?

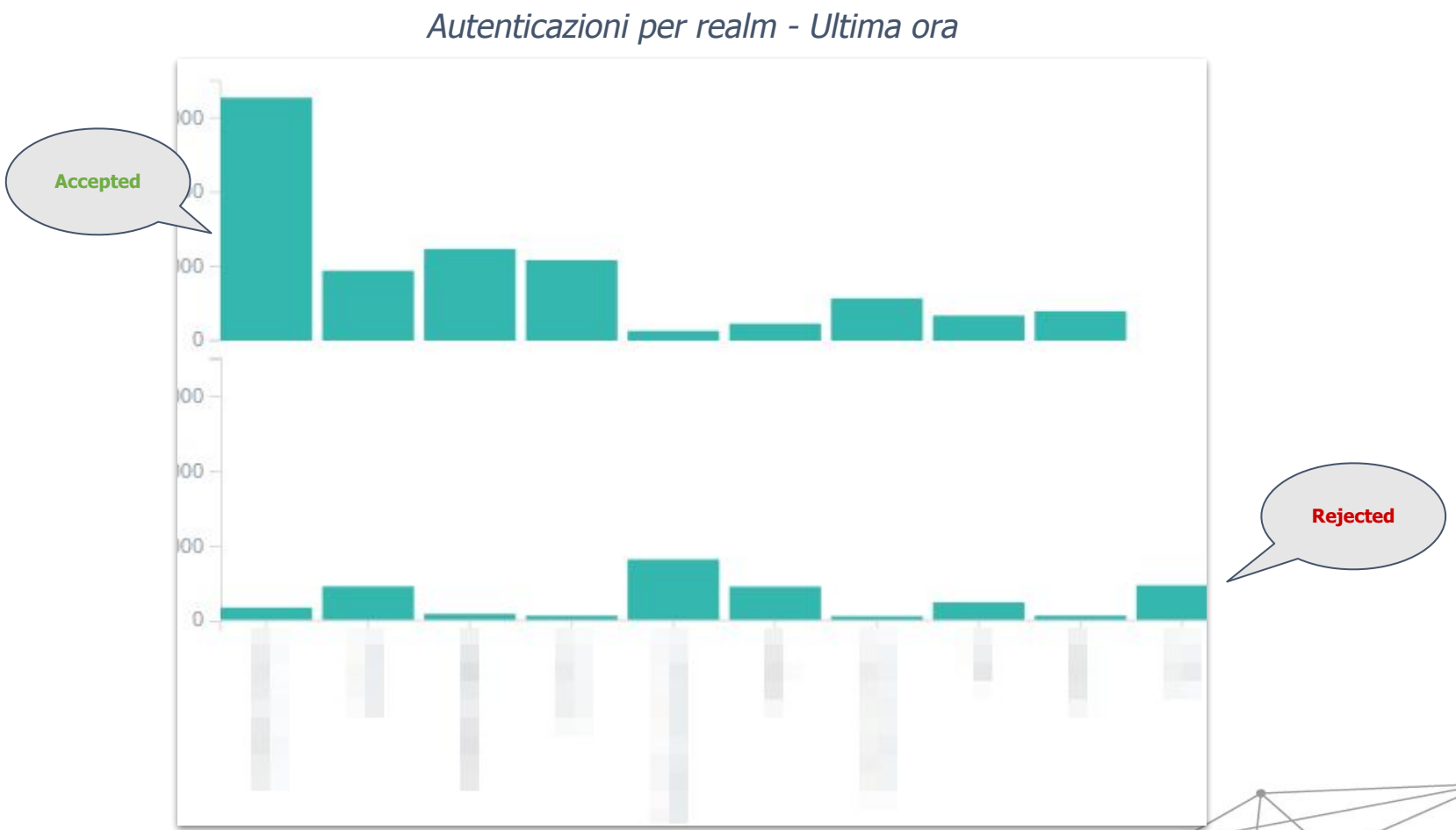
identity.keyword:anonymous@garr.it



Troubleshooting (2/2)

Troubleshooting | Compliance | Reject | Load Balancing | Statistiche

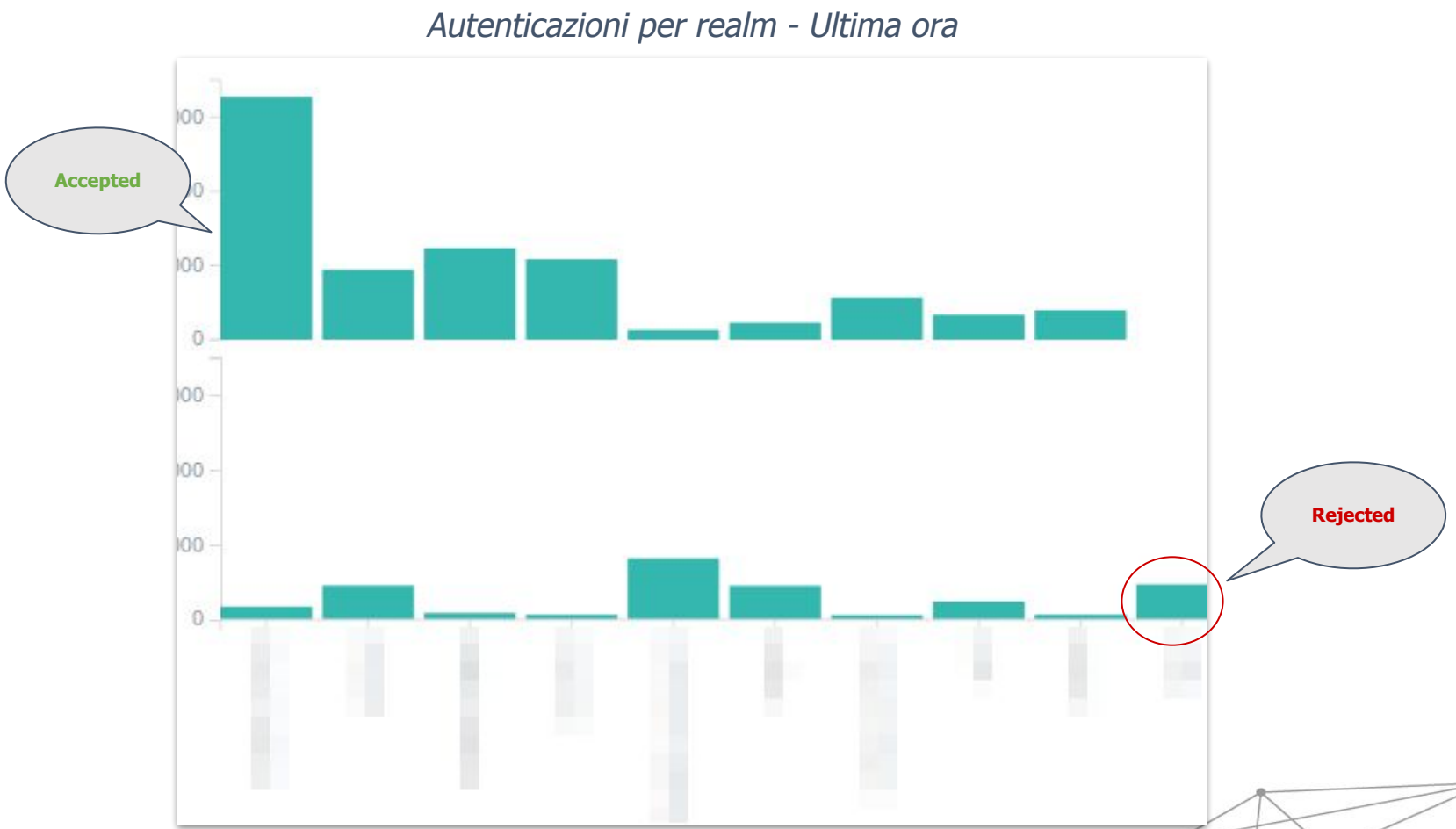
- Se 100% fail -> problema radius ente?



Troubleshooting (2/2)

Troubleshooting | Compliance | Reject | Load Balancing | Statistiche

- Se 100% fail -> problema radius ente?



Compliance

- Identificare immediatamente gli enti che non inviano le informazioni obbligatorie definite nell'eduroam Service Definition
  - Calling-Station-Id
  - NAS-IP-Address/NAS-Identifier
- Notifica ai contatti tecnici e correzione delle configurazioni

OperatorName	Realm	Status	Count
	cnr.it	accept	63
	biochem.mpg.de	accept	5
	unina.it	accept	5
	lngs.infn.it	accept	10
	inaf.it	accept	3
	pg.infn.it	accept	3
	univ-grenoble-alpes.fr	accept	1
	uva.es	accept	1
	uvigo.es	accept	1
	u-psud.fr	accept	2

Num. di autenticazioni con successo in cui manca il Calling-Station-Id

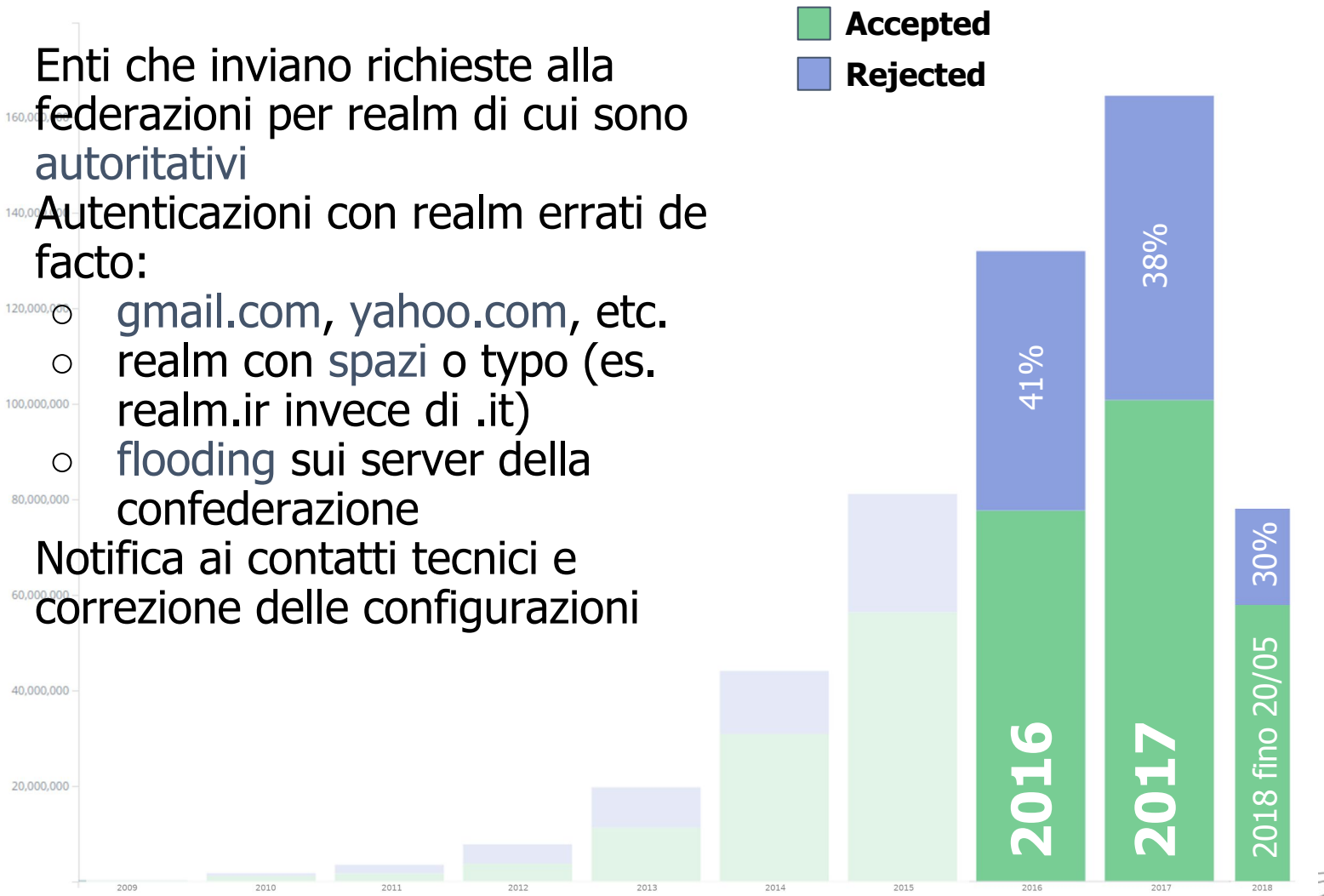
Num. di autenticazioni con successo in cui manca il NAS-Identifier o NAS-IP-Address

OperatorName	Realm	Status	Count
	studenti.unicampania.it	accept	14
	studenti.unior.it	accept	1

Autenticazioni rifiutate

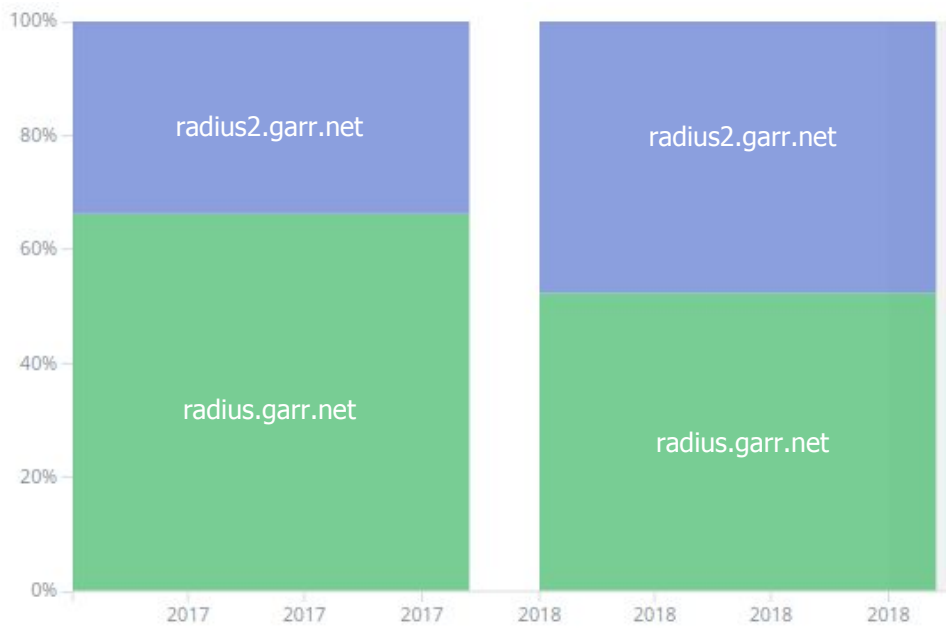
Troubleshooting
Compliance
Reject
Load Balancing
Statistiche

- Enti che inviano richieste alla federazioni per realm di cui sono autoritativi
- Autenticazioni con realm errati de facto:
  - gmail.com, yahoo.com, etc.
  - realm con spazi o typo (es. realm.ir invece di .it)
  - flooding sui server della confederazione
- Notifica ai contatti tecnici e correzione delle configurazioni



Load Balancing

- radius.garr.net utilizzato come primario
  - troppo carico
  - basse performance
  - timeout -> autenticazioni errate
- distribuzione del carico

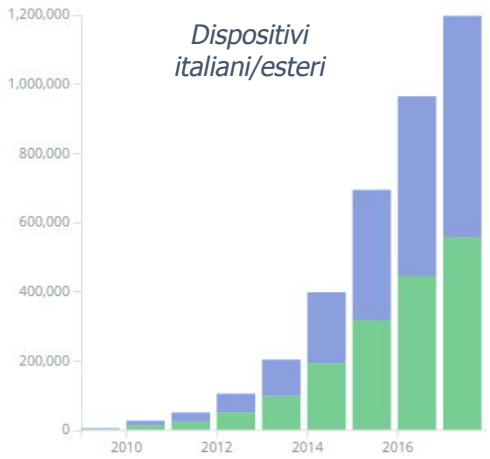


Statistiche

- prima:
  - script custom python
  - tempi di esecuzione lunghi
  - re-run se nuovo dato
- ora:
  - Visualization Kibana

Autenticazioni con successo

2017	Italiani	accept	79,382,797
2017	Esteri in Italia	accept	21,527,309



Top 10 realms

@timestamp per year	realm.keyword: Descending	Count
2017	studenti.unimi.it	9,180,165
2017	polimi.it	4,129,164
2017	ds.units.it	3,908,887
2017	studenti.unipd.it	2,158,154
2017	unipv.it	2,118,134
2017	campus.unimib.it	1,874,800
2017	unimi.it	1,838,046
2017	unipi.it	1,224,438
2017	aulecsit.uniud.it	1,153,707
2017	studenti.polito.it	946,281

Sviluppi futuri

- Alert automatizzati
- Estendere a:
  - log server
  - metriche
- Integrazione con altri servizi (Sessione *Automazione e Software* del 30 Maggio)

Conclusioni

- I log contengono molta informazione di cui a volte non si ha percezione
- L'analitica è fondamentale nel logging tradizionale di sistemi complessi
- **Indispensabile** e **necessario** per l'erogazione del servizio
- Il log diventa strumento di supporto alle decisioni