# Industry made:
# NetEye per il settore finanziario

## Il Gruppo IBT punta su NetEye come asset strategico di controllo

**NetEye & Erizone User Group 2016**

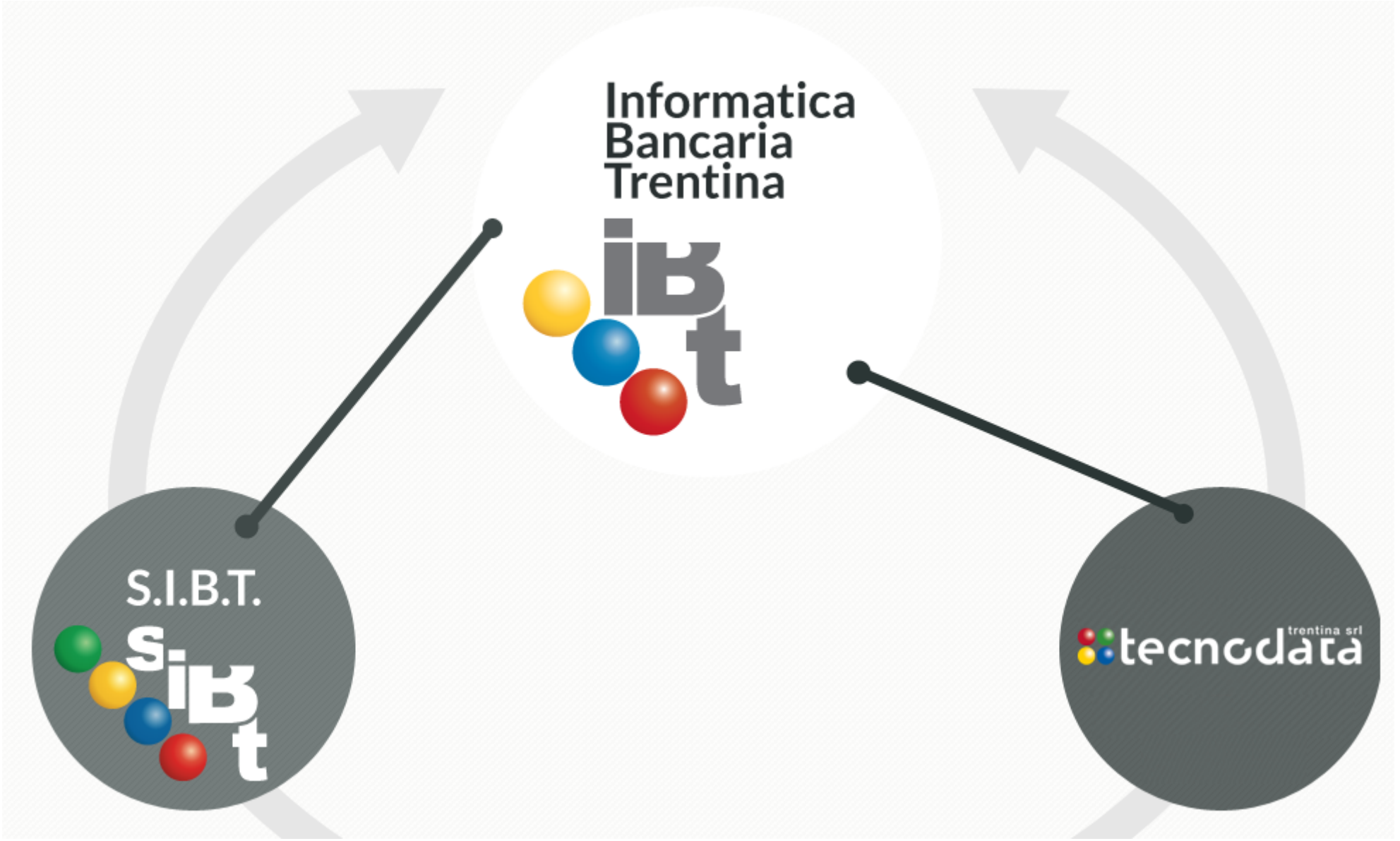
WÜRTHPHOENIX
NetEye

ibt L'Informatica Bancaria

sibt

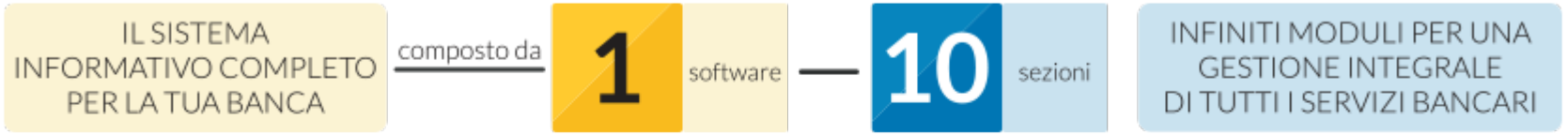
tecnodata trentina srl

# Un salto dentro il Gruppo IBT



# Cosa facciamo?

**IBT:**
sviluppo del sistema informativo bancario
Gesbank Evolution




Gesbank
evolution

# Cosa facciamo?

**SIBT:**

- outsourcing di Gesbank Evolution
- backoffice finanza, contabilità, estero, contrattualistica, incassi e pagamenti
- business intelligence
- sviluppo di un proprio sistema di gestione documentale
- accertamenti bancari telematici
- nodo rete SID (Agenzia delle Entrate)
- tutti i servizi accessibili anche da remoto (vpn)

# Cosa facciamo?

**Tecnodata:**

- outsourcing desktop ed applicazioni (Citrix)
- fornitura hardware
- connettività (provider di servizi internet)

# Alcuni numeri del Gruppo IBT

Fatturato 2015: **14 mln/€**
Dipendenti 2015: **116**
Banche totali servite: **~90**

# Storia del “nostro” monitoraggio

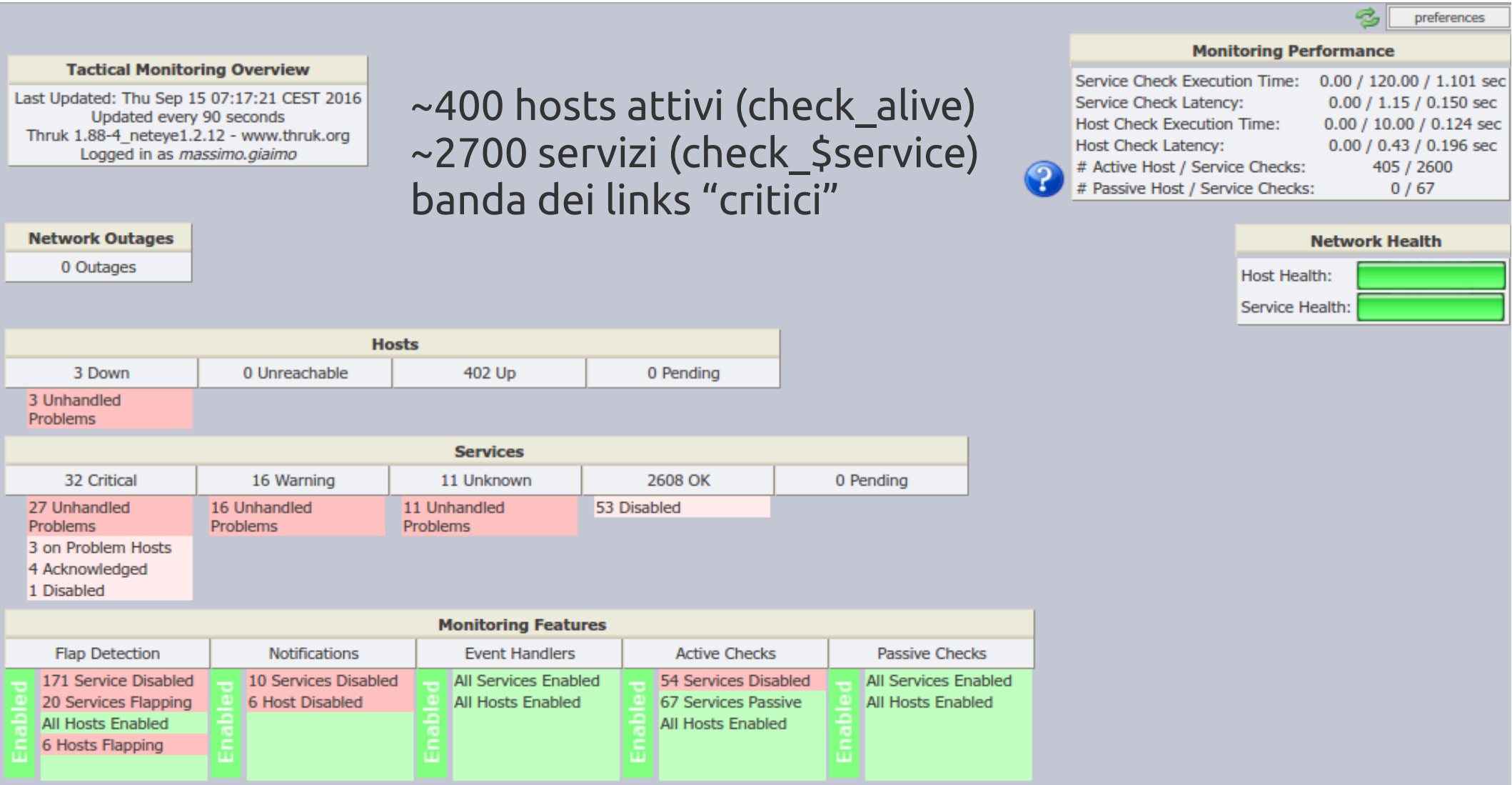
**1998-2004** Whatsup Gold e tanto Excel!
**> 2005** Nagios
**> 2009** Manage Engine Application Manager
**> 2009** PRTG
**> 2010** GLPI
**> 2011** OCS
e poi Cacti, MRTG, ntop, ...

Documentazione: confusa quando andava bene

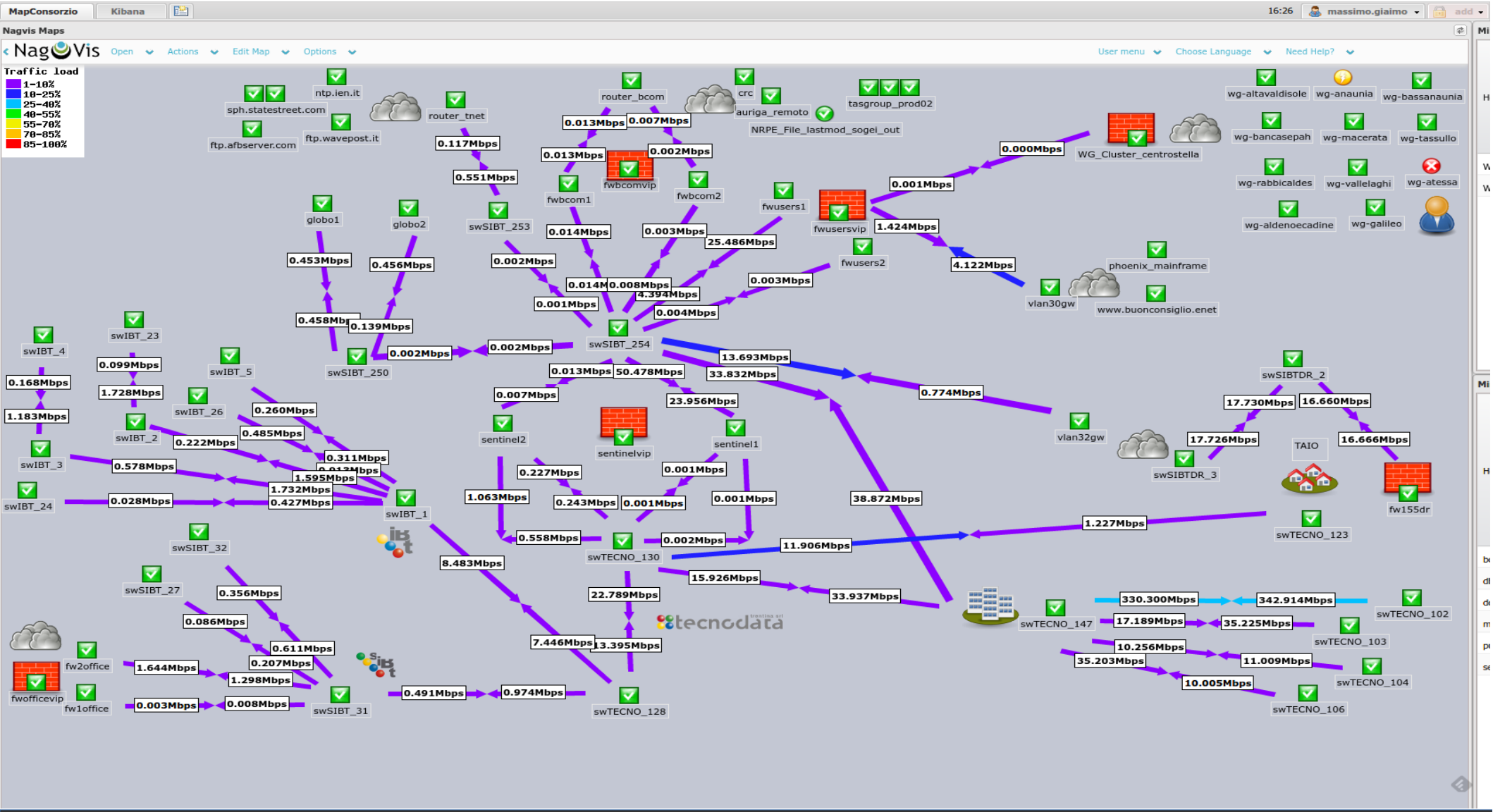
# 2015: NetEye… perché?

- Non avevamo (abbiamo) tempo di stare dietro a tutti gli aggiornamenti!
- Avevamo bisogno di qualcosa di più!
- Avevamo la necessità di fare check anche sul gestionale, non solo sui sistemi
- Infrastruttura sempre più complessa

# Cosa dobbiamo monitorare?



# Prima di tutto: vediamoci chiaro!



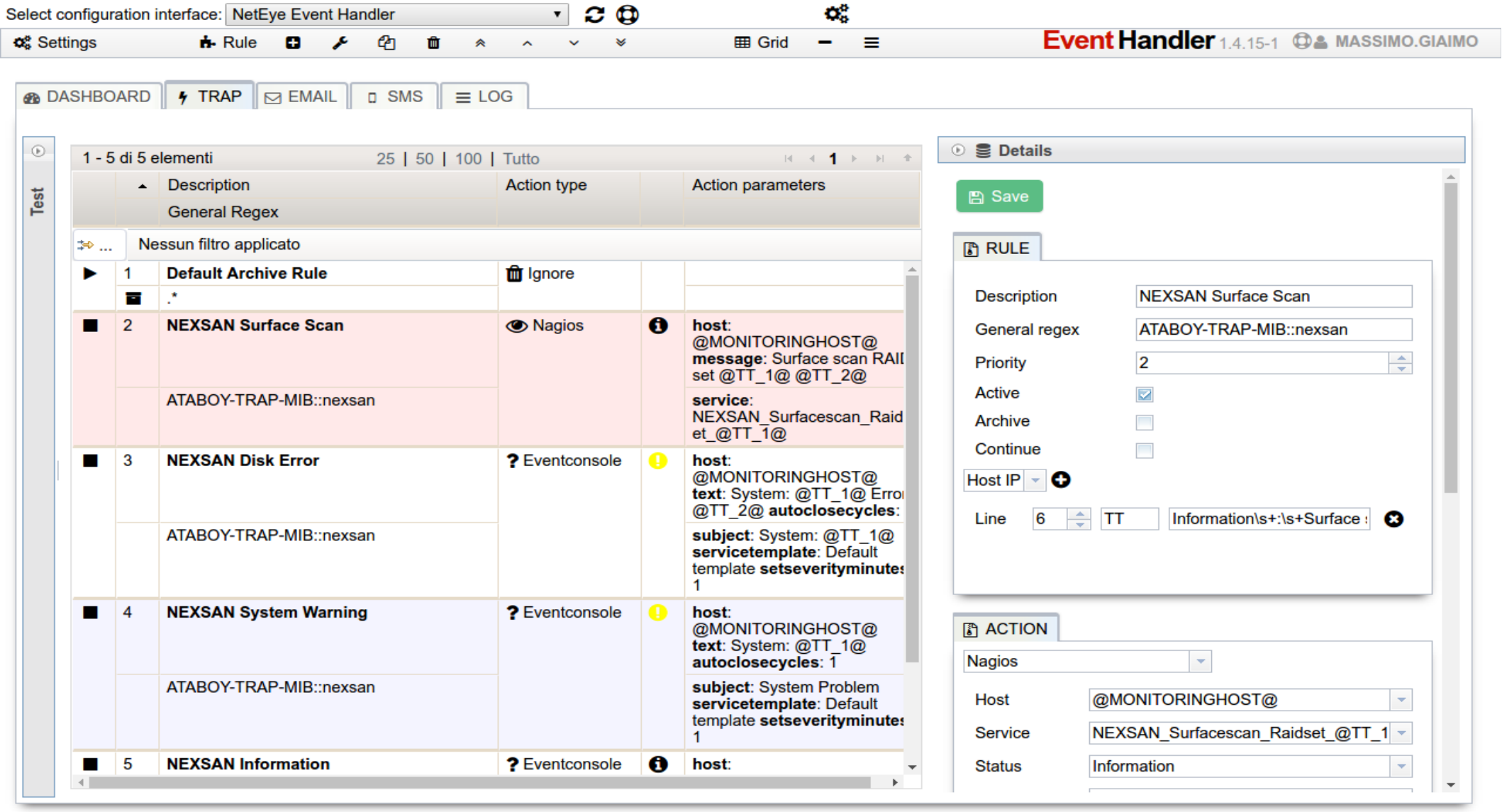
# Necessità 1

## SAN Monitoring

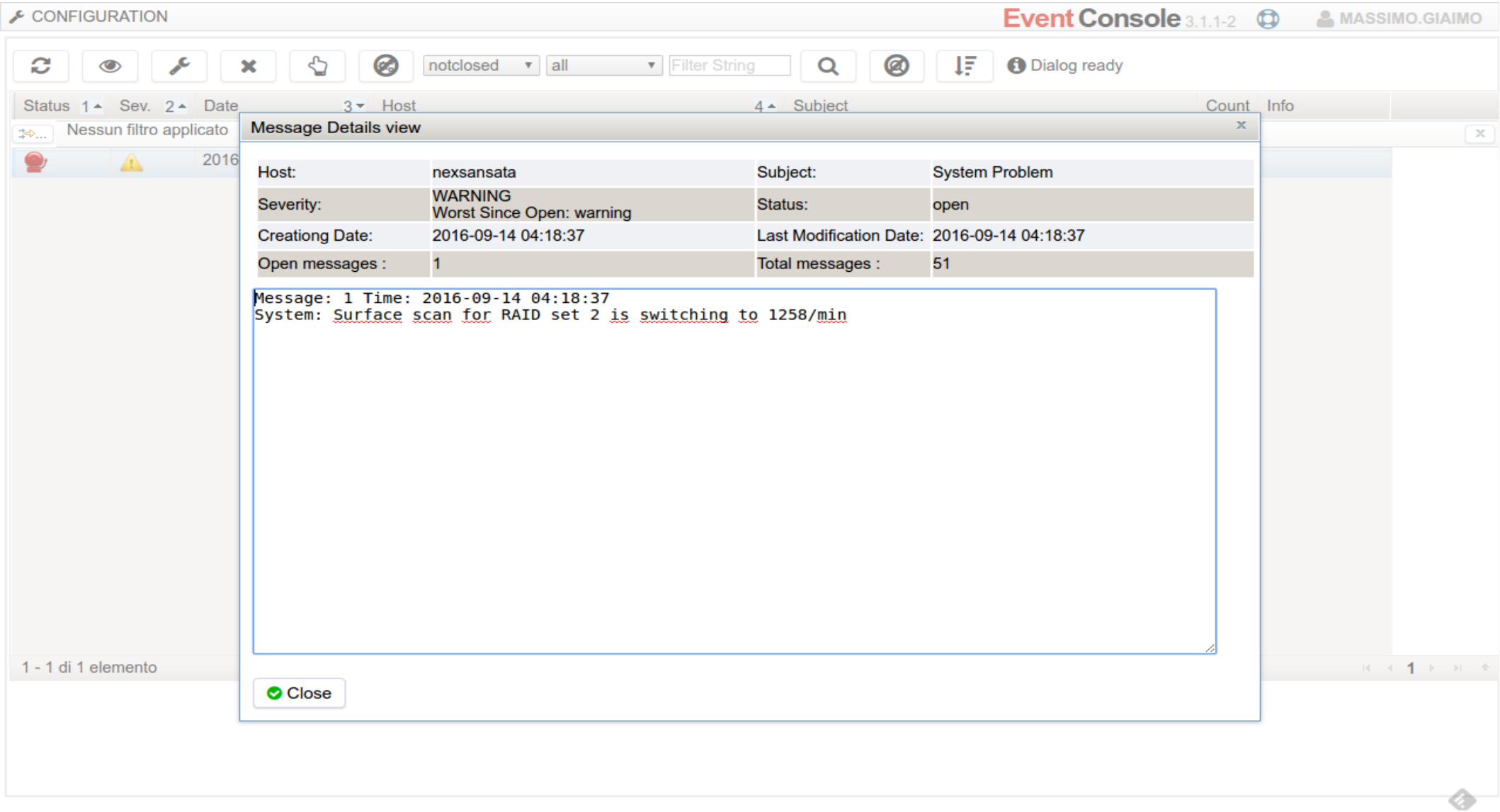
| SYSLOG Configuration | |
|---|---|
| **SYSLOG server IP address** | 10.133.0.141 |
| **SYSLOG server UDP Port** | 514 |
| **SYSLOG facility** | LOCAL0 ▼ |
| **When to send SYSLOG messages** | Send SYSLOG messages for all events ▼ |

non interrogabile via SNMP, può solo inviare i suoi log ad un syslog server

# Soluzione!


Select configuration interface: NetEye Event Handler
Settings
Rule
Grid
Event Handler 1.4.15-1
MASSIMO.GIAIMO
DASHBOARD
TRAP
EMAIL
SMS
LOG
Test
1 - 5 di 5 elementi
25 | 50 | 100 | Tutto
Description
General Regex
Action type
Action parameters
Nessun filtro applicato
1 Default Archive Rule
Ignore
.*
2 NEXSAN Surface Scan
Nagios
host: @MONITORINGHOST@ message: Surface scan RAI set @TT_1@ @TT_2@
ATABOY-TRAP-MIB::nexsan
service: NEXSAN_Surfacescan_Raid et_@TT_1@
3 NEXSAN Disk Error
Eventconsole
host: @MONITORINGHOST@ text: System: @TT_1@ Erro @TT_2@ autoclosecycles:
ATABOY-TRAP-MIB::nexsan
subject: System: @TT_1@ servicetemplate: Default template setseverityminute 1
4 NEXSAN System Warning
Eventconsole
host: @MONITORINGHOST@ text: System: @TT_1@ autoclosecycles: 1
ATABOY-TRAP-MIB::nexsan
subject: System Problem servicetemplate: Default template setseverityminute 1
5 NEXSAN Information
Eventconsole
host:
Details
Save
RULE
Description
NEXSAN Surface Scan
General regex
ATABOY-TRAP-MIB::nexsan
Priority
2
Active
Archive
Continue
Host IP
Line
6
TT
Information\s+:\s+Surface
ACTION
Nagios
Host
@MONITORINGHOST@
Service
NEXSAN_Surfacescan_Raidset_@TT_1
Status
Information

# Soluzione!


CONFIGURATION
Event Console 3.1.1-2
MASSIMO.GIAIMO
notclosed
all
Filter String
Dialog ready
Status 1
Sev. 2
Date 3
Host 4
Subject
Count
Info
Nessun filtro applicato
Message Details view
Host: nexsansata
Subject: System Problem
Severity: WARNING
Worst Since Open: warning
Status: open
Creationg Date: 2016-09-14 04:18:37
Last Modification Date: 2016-09-14 04:18:37
Open messages : 1
Total messages : 51
Message: 1 Time: 2016-09-14 04:18:37
System: Surface scan for RAID set 2 is switching to 1258/min
Close
1 - 1 di 1 elemento

# Soluzione!

| Host | Service | Status | Last Check | Duration | Attempt | Status Information |
|---|---|---|---|---|---|---|
| nexsansata | Eventconsole_Open_Problems | OK | 12:01:12 | 1d 2h 32m 57s | 1/1 | OK - no open problems for host: nexsansata subject: .* |
| | NEXSAN_Surfacescan_Raidset_1 | OK | 2016-09-13 00:26:26 | 280d 20h 15m 59s | 1/1 | Surface scan RAID set 1 has finished |
| | NEXSAN_Surfacescan_Raidset_2 | OK | 2016-09-13 04:14:43 | 280d 20h 15m 59s | 1/1 | Surface scan RAID set 2 has started |
| | NEXSAN_Surfacescan_Raidset_3 | OK | 2016-09-03 23:25:09 | 280d 20h 15m 59s | 1/1 | Surface scan RAID set 3 has finished |
| | NEXSAN_Surfacescan_Raidset_4 | OK | 2016-09-09 00:45:31 | 280d 20h 15m 59s | 1/1 | Surface scan RAID set 4 has finished |
| | PING | OK | 11:59:29 | 304d 1h 19m 51s | 1/3 | PING OK - Packet loss = 0%, RTA = 0.14 ms |

# Necessità 2

Automazione del processo invio e ricezione flussi tramite SID (Sistema di Interscambio flussi Dati) – Agenzia delle Entrate

# Soluzione!

Abbiamo scritto gli script di invio/ricezione con la finalità di avvisare NetEye di ogni step importante

**OK**

```
/usr/local/bin/postie -host:neteye -from:sibt-
noreply@sibtonline.eu -to:eventgw@neteye.sibtonline
-s:"NAGIOS - bcc${1} - EC_SID_AnagR
app_send - Information" -msg:"Nessun file da
elaborare"
```

# Soluzione!

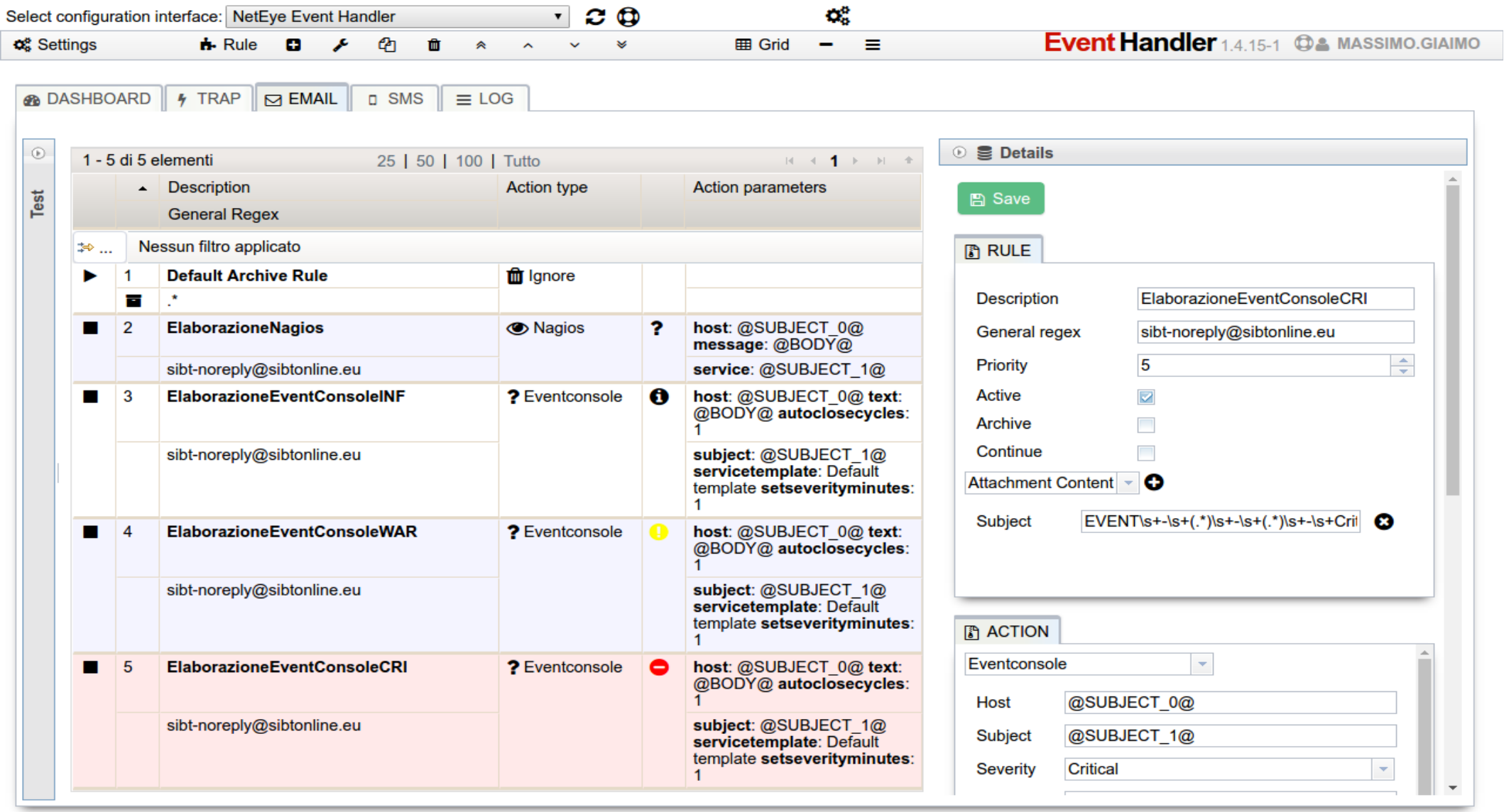
## WARNING

```
/usr/local/bin/postie -host:neteye -from:sibt-
noreply@sibtonline.eu -to:eventgw@neteye.sibtonline
-s:"NAGIOS - bcc${1} - EC_SID_AnagR
app_send - Warning" -msg:"Flussi elaborati: 0"
```

## CRITICAL

```
/usr/local/bin/postie -host:neteye -from:sibt-
noreply@sibtonline.eu -to:eventgw@neteye.sibtonline
-s:"NAGIOS - bcc${1} - EC_SID_AnagR
app_send - Critical" -msg:"$giornomese Flussi
scartati: $errore su $numero"
```

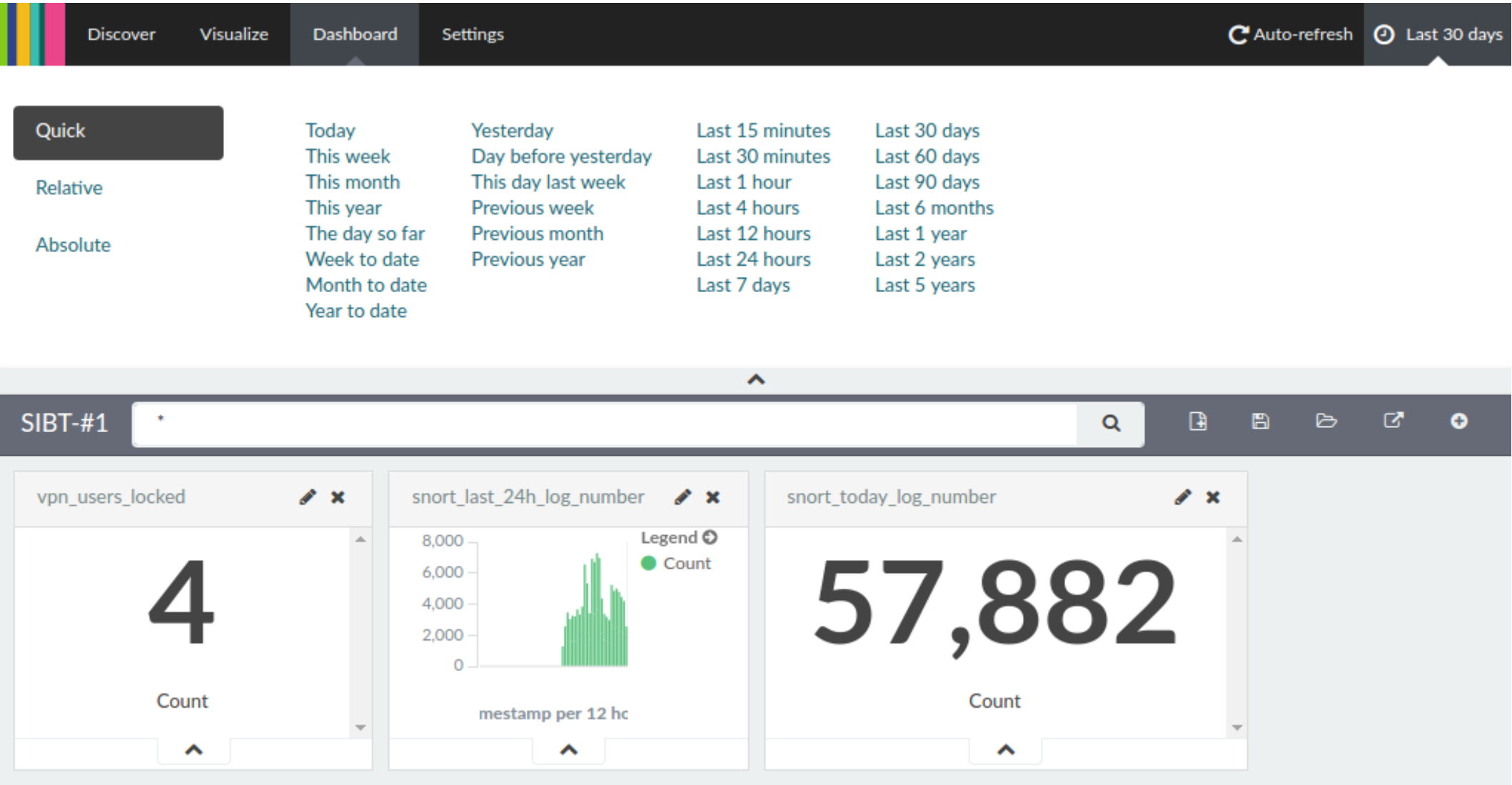
# Soluzione!


Select configuration interface: NetEye Event Handler
Settings
Rule
Grid
Event Handler 1.4.15-1
MASSIMO.GIAIMO
DASHBOARD
TRAP
EMAIL
SMS
LOG
Test
1 - 5 di 5 elementi
25 | 50 | 100 | Tutto
Description
General Regex
Action type
Action parameters
Nessun filtro applicato
1 Default Archive Rule
Ignore
.*
2 ElaborazioneNagios
Nagios
host: @SUBJECT_0@ message: @BODY@
sibt-noreply@sibtonline.eu
service: @SUBJECT_1@
3 ElaborazioneEventConsoleINF
Eventconsole
host: @SUBJECT_0@ text: @BODY@ autoclosecycles: 1
sibt-noreply@sibtonline.eu
subject: @SUBJECT_1@ servicetemplate: Default template setseverityminutes: 1
4 ElaborazioneEventConsoleWAR
Eventconsole
host: @SUBJECT_0@ text: @BODY@ autoclosecycles: 1
sibt-noreply@sibtonline.eu
subject: @SUBJECT_1@ servicetemplate: Default template setseverityminutes: 1
5 ElaborazioneEventConsoleCRI
Eventconsole
host: @SUBJECT_0@ text: @BODY@ autoclosecycles: 1
sibt-noreply@sibtonline.eu
subject: @SUBJECT_1@ servicetemplate: Default template setseverityminutes: 1
Details
Save
RULE
Description ElaborazioneEventConsoleCRI
General regex sibt-noreply@sibtonline.eu
Priority 5
Active
Archive
Continue
Attachment Content
Subject EVENT\s+-\s+(.*)\s+-\s+(.*)\s+-\s+Cri
ACTION
Eventconsole
Host @SUBJECT_0@
Subject @SUBJECT_1@
Severity Critical

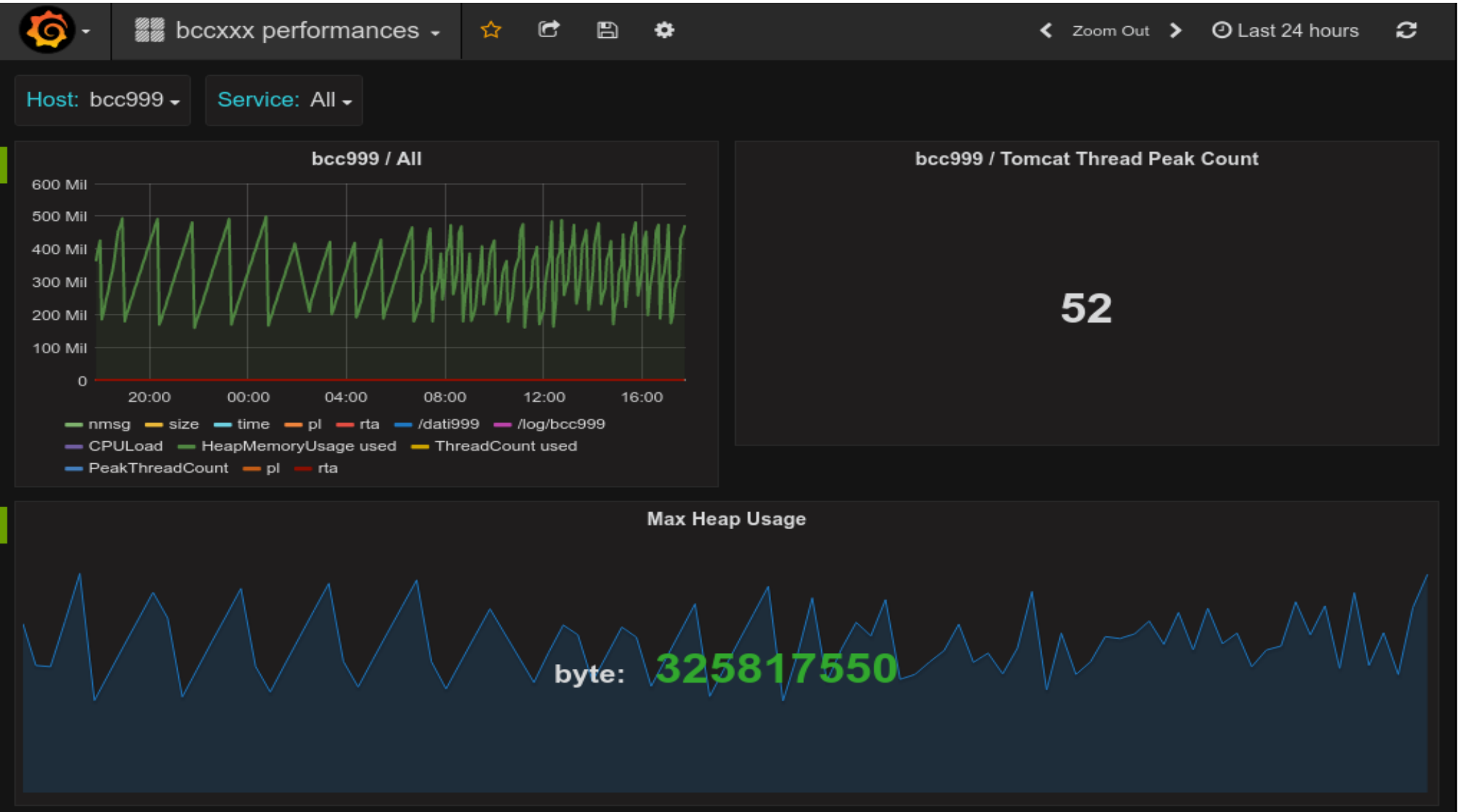
# Soluzione!

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| bcc002 | EC_SID_AnagRapp_receive | | OK | 2016-09-14 23:00:05 | 106d 20h 44m 32s | 1/1 | Nessuna ricevuta da elaborare |
| | EC_SID_AnagRapp_send | | OK | 2016-09-14 21:00:04 | 62d 20h 30m 19s | 1/1 | Nessun file da elaborare |
| | EC_SID_FATCA_receive | | OK | 2016-06-22 10:53:52 | 140d 2h 55m 57s | 1/1 | OK: forzato |
| | EC_SID_FATCA_send | | OK | 2016-06-22 10:53:52 | 140d 2h 55m 57s | 1/1 | OK: forzato |
| | EC_SID_MonFisc_receive | | OK | 2016-08-22 09:12:38 | 127d 19h 30m 0s | 1/1 | OK: forzato |
| | EC_SID_MonFisc_send | | OK | 2016-08-22 09:12:38 | 63d 0h 6m 28s | 1/1 | OK: forzato |

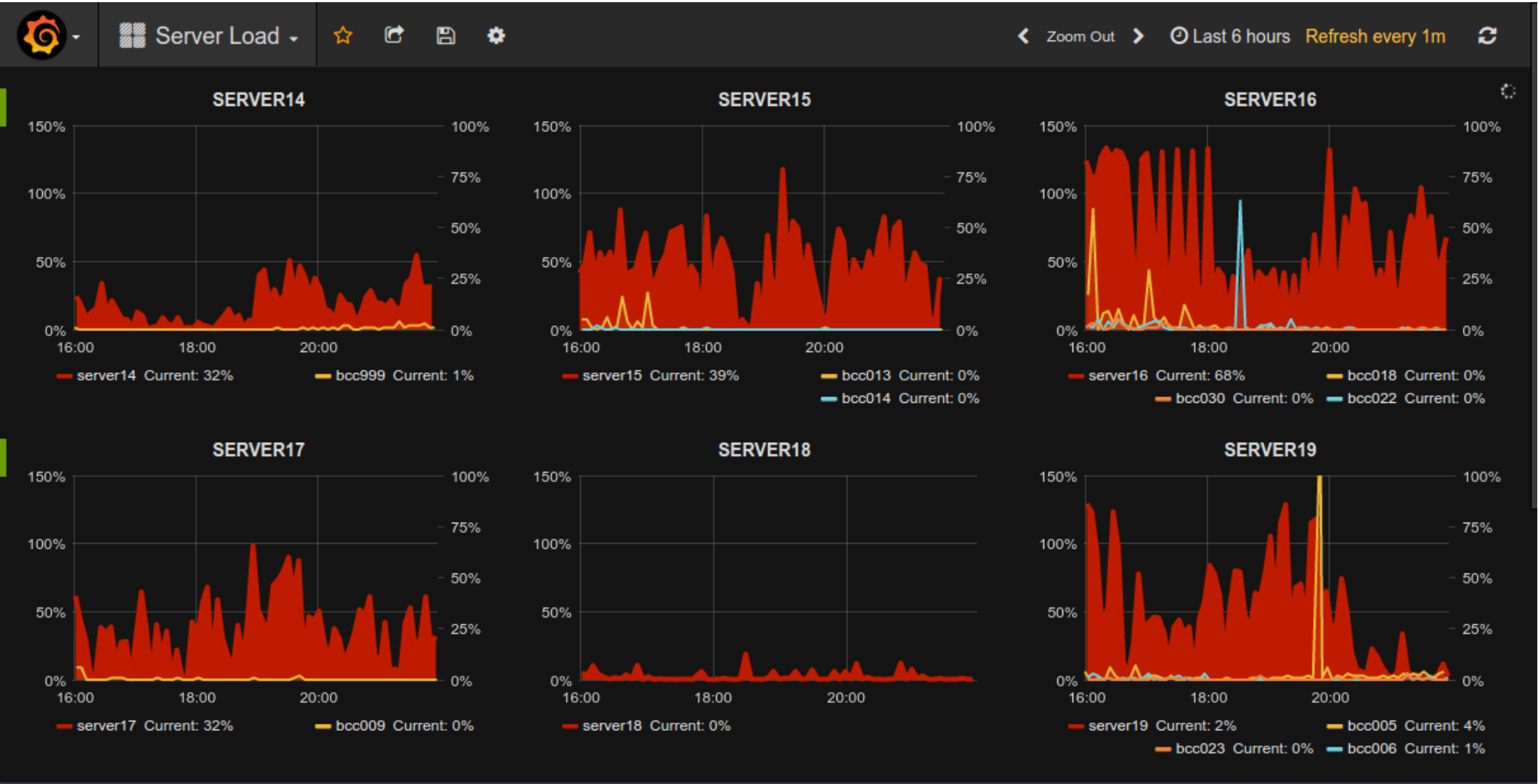
# L’appetito vien mangiando...



# L’appetito vien mangiando...

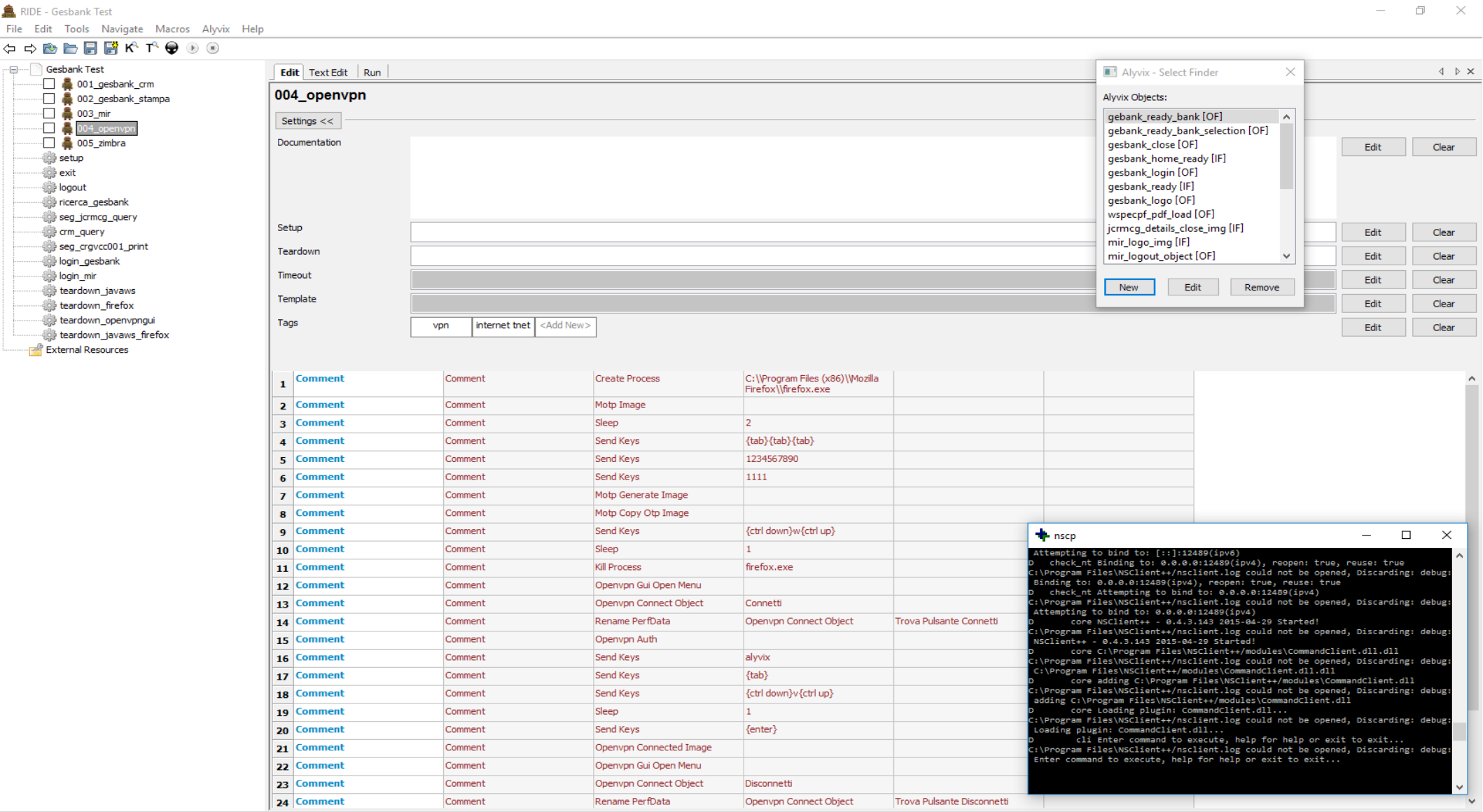


# L’appetito vien mangiando...



# L’appetito vien mangiando...

# L’appetito vien mangiando…



# Metodologia di lavoro

Per qualsiasi cosa acquistiamo, sviluppiamo, pensiamo ci chiediamo…

*“possiamo controllare questo aspetto con NetEye?”*

# Metodologia di lavoro

Questo ci consente di:

- creare uno standard da seguire
- essere certi che qualsiasi fase delle nostre procedure sia compliance allo standard
- provare la piacevole sensazione di avere sotto controllo il nostro lavoro!

Da ottobre 2015 ogni script scritto da noi non può fare a meno di avere queste variabili:

```
$STATE_OK=0;
$STATE_WA=1;
$STATE_CR=2;
$STATE_UN=3;
```

# Grazie!

**Massimo Giaimo (@fastfire)**
**Simone Cagol (@CagolSimone)**
**it@sibtonline.eu**