

Industry made: NetEye per il settore finanziario

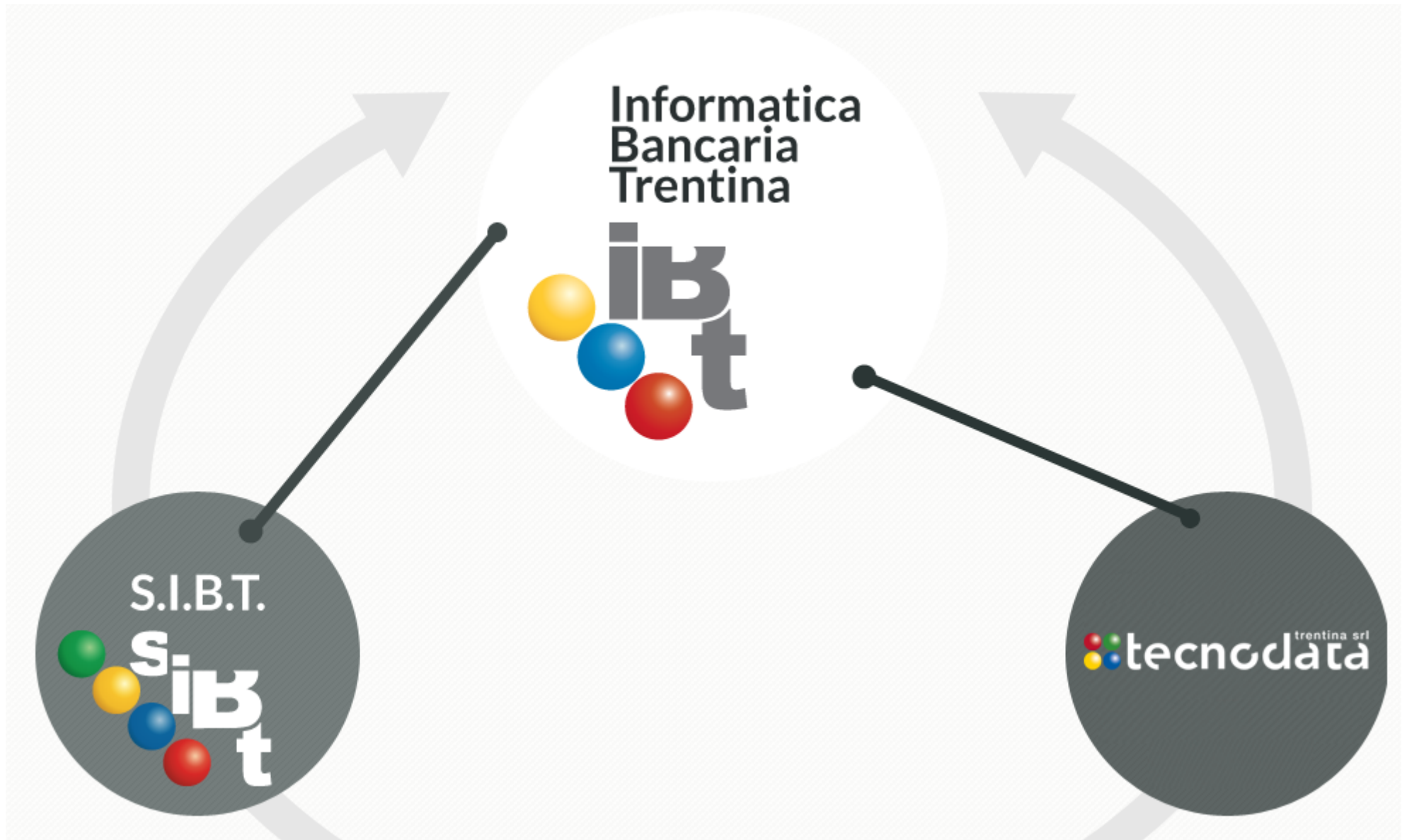
Il Gruppo IBT punta su NetEye
come asset strategico di controllo

NetEye & Erizone User Group 2016

WÜRTHPHOENIX
NetEye



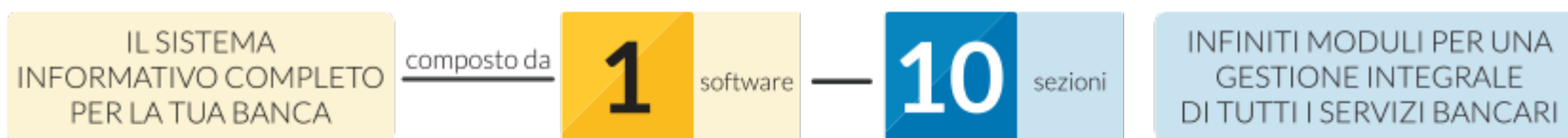
Un salto dentro il Gruppo IBT



Cosa facciamo?

IBT:

sviluppo del sistema informativo bancario
Gesbank Evolution



Gesbank
e v o l u t i o n

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?

Tactical Monitoring Overview

Last Updated: Thu Sep 15 07:17:21 CEST 2016
Updated every 90 seconds
Thruk 1.88-4_neteye1.2.12 - www.thruk.org
Logged in as *massimo.giaino*

~400 hosts attivi (check_alive)
~2700 servizi (check_\$service)
banda dei links "critici"

Network Outages

0 Outages

Hosts

3 Down 0 Unreachable 402 Up 0 Pending

3 Unhandled Problems

Services

32 Critical 16 Warning 11 Unknown 2608 OK 0 Pending

27 Unhandled Problems
3 on Problem Hosts
4 Acknowledged
1 Disabled

16 Unhandled Problems

11 Unhandled Problems

53 Disabled

Monitoring Features

Flap Detection

Notifications

Event Handlers

Active Checks

Passive Checks

Enabled
171 Service Disabled
20 Services Flapping
All Hosts Enabled
6 Hosts Flapping

Enabled
10 Services Disabled
6 Host Disabled

Enabled
All Services Enabled
All Hosts Enabled


Enabled
54 Services Disabled
67 Services Passive
All Hosts Enabled


Enabled
All Services Enabled
All Hosts Enabled

Monitoring Performance

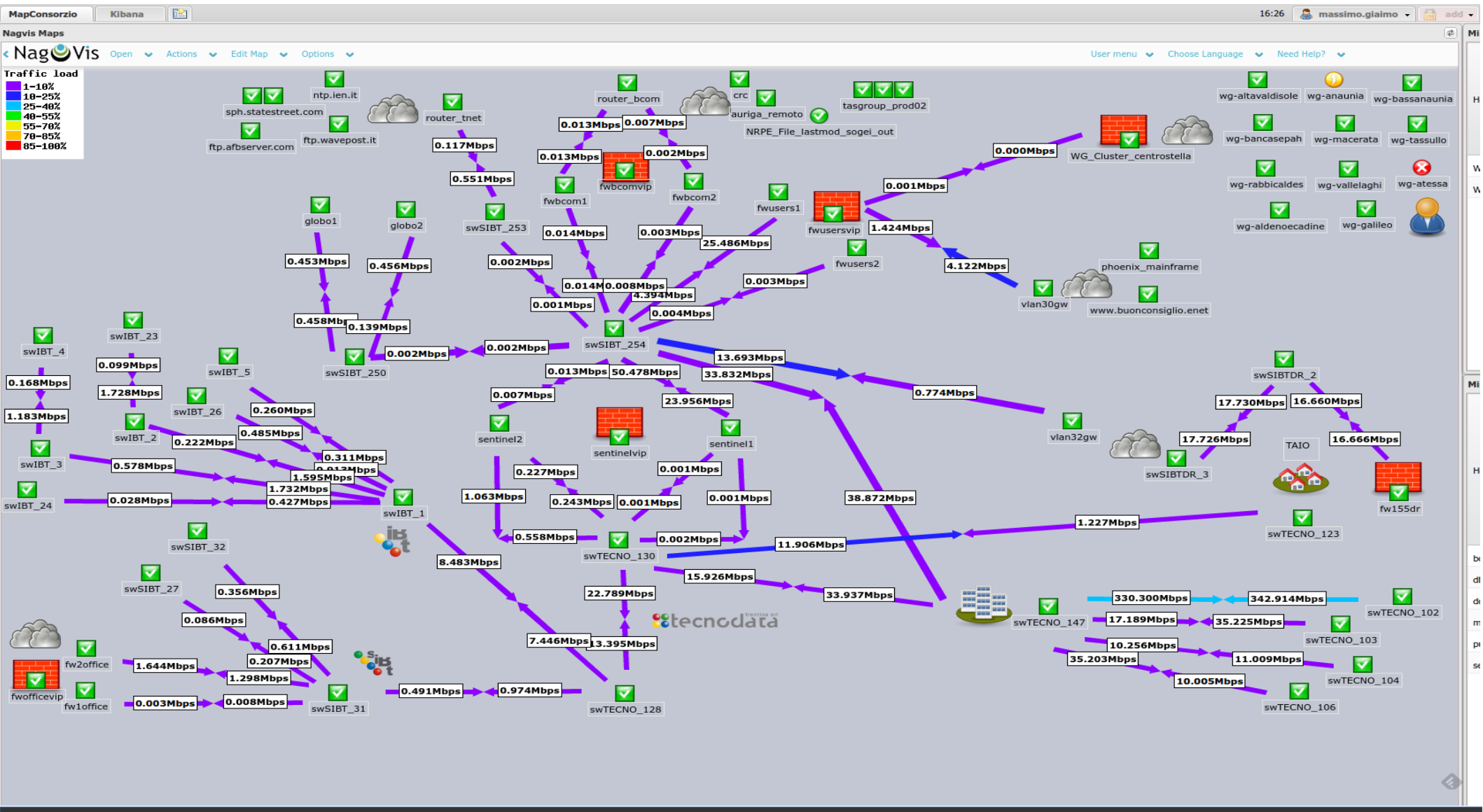
Service Check Execution Time: 0.00 / 120.00 / 1.101 sec
Service Check Latency: 0.00 / 1.15 / 0.150 sec
Host Check Execution Time: 0.00 / 10.00 / 0.124 sec
Host Check Latency: 0.00 / 0.43 / 0.196 sec
Active Host / Service Checks: 405 / 2600
Passive Host / Service Checks: 0 / 67

Network Health

Host Health: 

Service Health: 

Prima di tutto: vediamoci chiaro!



Necessità 1

SAN Monitoring

SYSLOG Configuration	
SYSLOG server IP address	<input type="text" value="10.133.0.141"/>
SYSLOG server UDP Port	<input type="text" value="514"/>
SYSLOG facility	<input type="text" value="LOCAL0 ▼"/>
When to send SYSLOG messages	<input type="text" value="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 Add Edit Delete Refresh Grid -

Event Handler 1.4.15-1 MASSIMO.GIAIMO

DASHBOARD TRAP EMAIL SMS LOG

1 - 5 di 5 elementi 25 | 50 | 100 | Tutto

Description	Action type	Action parameters
General Regex		
Nessun filtro applicato		
1 Default Archive Rule	Ignore	
2 NEXSAN Surface Scan	Nagios	host: @MONITORINGHOST@ message: Surface scan RAID set @TT_1@ @TT_2@ service: NEXSAN_Surfacescan_Raidet_@TT_1@
3 NEXSAN Disk Error	Eventconsole	host: @MONITORINGHOST@ text: System: @TT_1@ Error @TT_2@ autoclosecycles: subject: System: @TT_1@ servicetemplate: Default template setseverityminutes: 1
4 NEXSAN System Warning	Eventconsole	host: @MONITORINGHOST@ text: System: @TT_1@ autoclosecycles: 1 subject: System Problem servicetemplate: Default template setseverityminutes: 1
5 NEXSAN Information	Eventconsole	host:

Test

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

2016

Message Details view









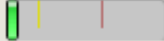
Host:	nexsansata	Subject:	System Problem
Severity:	WARNING Worst Since Open: warning	Status:	open
Creation Date:	2016-09-14 04:18:37	Last Modification Date:	2016-09-14 04:18:37
Open messages :	1	Total messages :	51

Message: 1 Time: 2016-09-14 04:18:37
System: Surface scan for RAID set 2 is switching to 1258/min

1 - 1 di 1 elemento

Close

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 [Icons] Grid - [Menu]

Event Handler 1.4.15-1 MASSIMO.GIAIMO

DASHBOARD TRAP EMAIL SMS LOG

Test

1 - 5 di 5 elementi 25 | 50 | 100 | Tutto

Description	Action type	Action parameters
General Regex		
Nessun filtro applicato		
1 Default Archive Rule	Ignore	
2 ElaborazioneNagios	Nagios	host: @SUBJECT_0@ message: @BODY@ service: @SUBJECT_1@
3 ElaborazioneEventConsoleINF	Eventconsole	host: @SUBJECT_0@ text: @BODY@ autoclosecycles: 1 subject: @SUBJECT_1@ servicetemplate: Default template setseverityminutes: 1
4 ElaborazioneEventConsoleWAR	Eventconsole	host: @SUBJECT_0@ text: @BODY@ autoclosecycles: 1 subject: @SUBJECT_1@ servicetemplate: Default template setseverityminutes: 1
5 ElaborazioneEventConsoleCRI	Eventconsole	host: @SUBJECT_0@ text: @BODY@ autoclosecycles: 1 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+Crii *

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

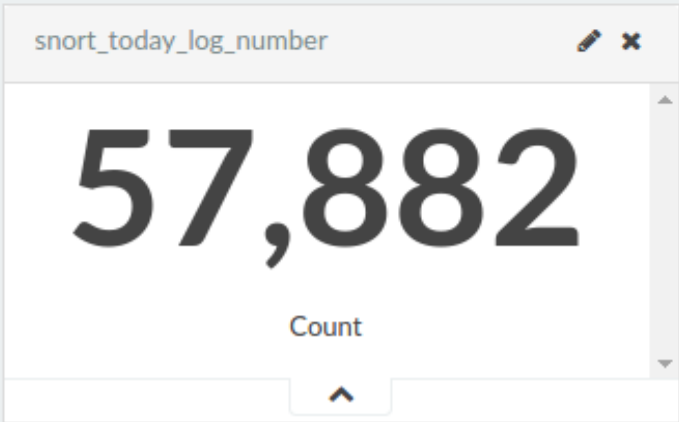
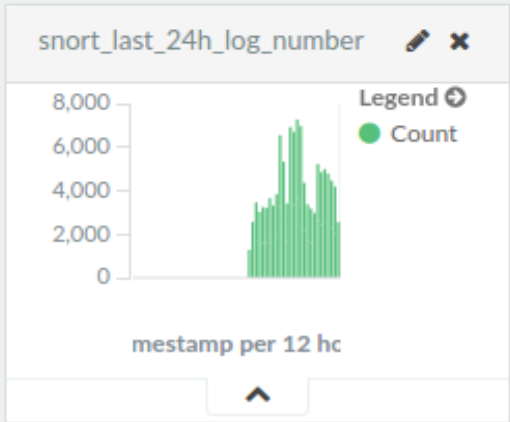
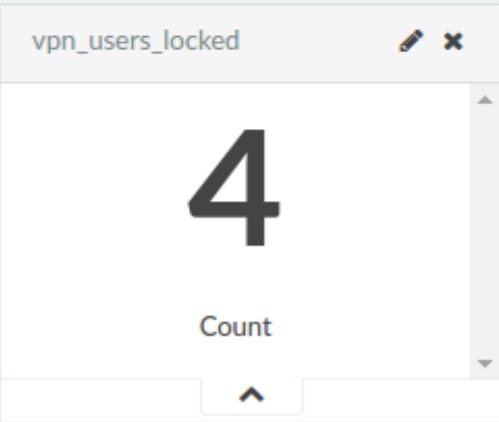
L'appetito vien mangiando...

Discover Visualize Dashboard Settings Auto-refresh Last 30 days

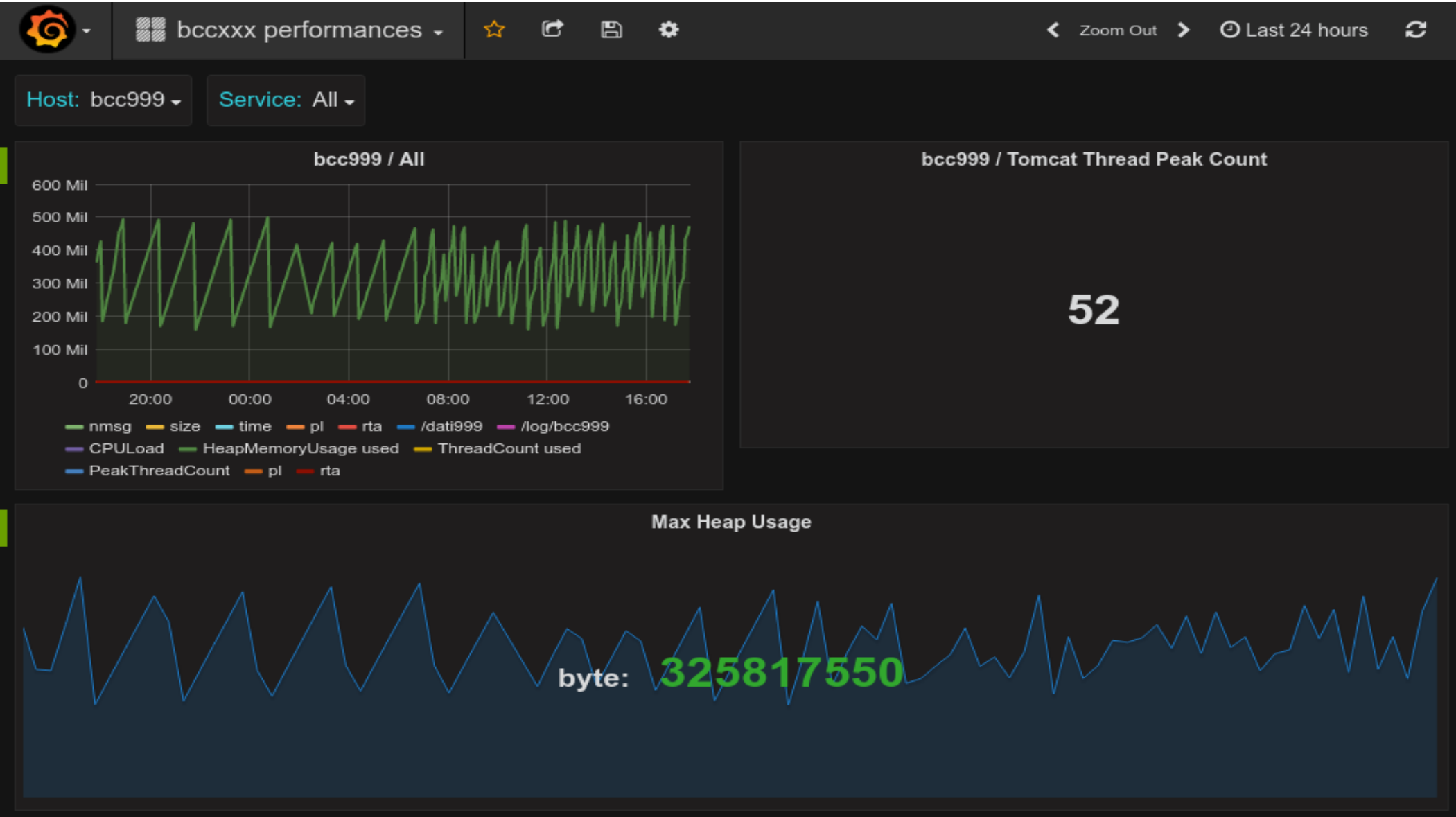
- Quick
- Relative
- Absolute

- Today
- This week
- This month
- This year
- The day so far
- Week to date
- Month to date
- Year to date
- Yesterday
- Day before yesterday
- This day last week
- Previous week
- Previous month
- Previous year
- Last 15 minutes
- Last 30 minutes
- Last 1 hour
- Last 4 hours
- Last 12 hours
- Last 24 hours
- Last 7 days
- Last 30 days
- Last 60 days
- Last 90 days
- Last 6 months
- Last 1 year
- Last 2 years
- Last 5 years

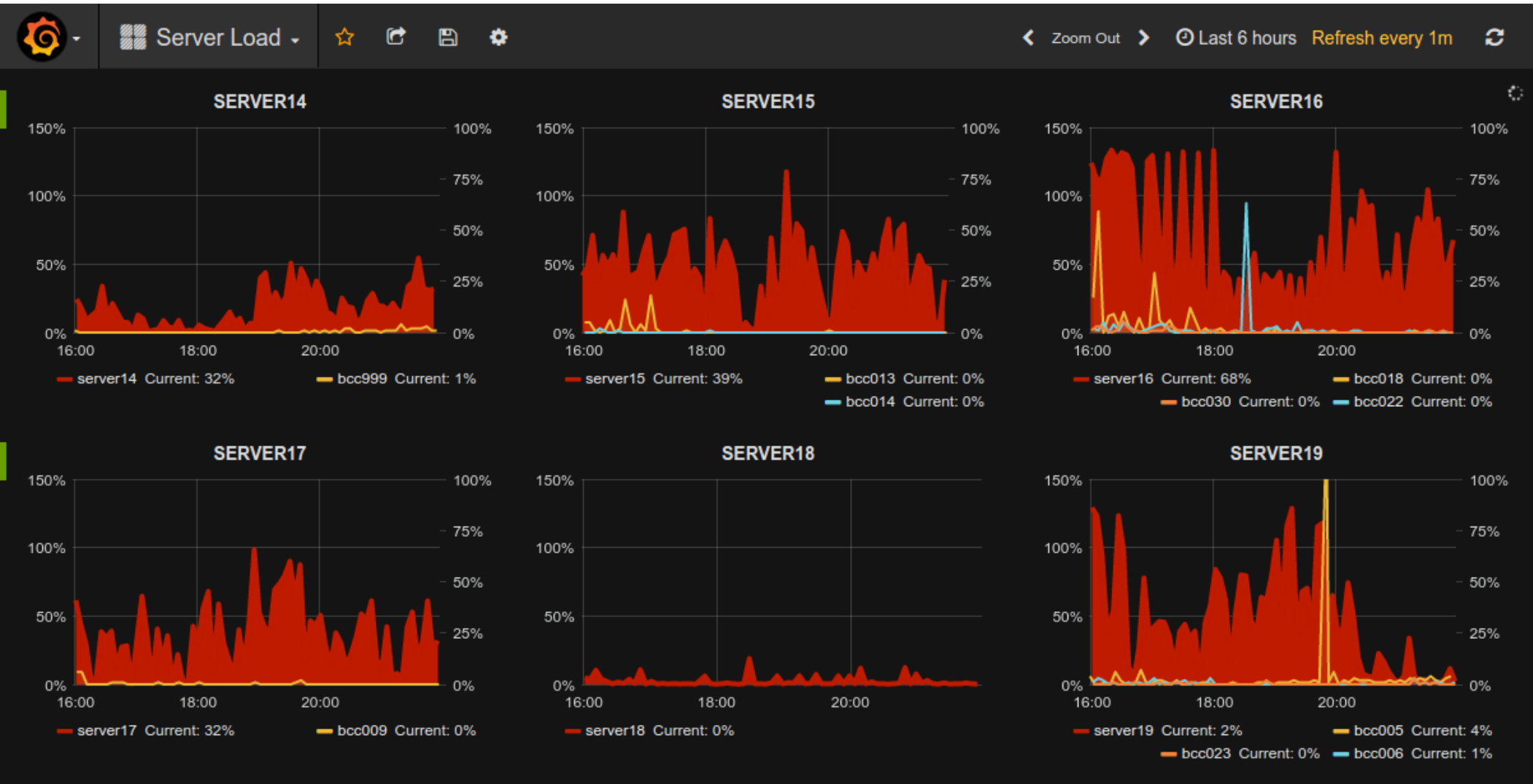
SIBT-#1 [Search] [Icons]



L'appetito vien mangiando...



L'appetito vien mangiando...



L'appetito vien mangiando...



L'appetito vien mangiando...

The screenshot displays the RIDE (Rational IDE) interface for a test suite named 'Gesbank Test'. The left sidebar shows a tree view of test cases, with '004_openvpn' selected. The main area shows the details for '004_openvpn', including a table of test steps.

Step	Comment	Action	Parameters	Expected Results
1	Comment	Create Process	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	
2	Comment	Motp Image		
3	Comment	Sleep	2	
4	Comment	Send Keys	{tab}{tab}{tab}	
5	Comment	Send Keys	1234567890	
6	Comment	Send Keys	1111	
7	Comment	Motp Generate Image		
8	Comment	Motp Copy Otp Image		
9	Comment	Send Keys	{ctrl down}w{ctrl up}	
10	Comment	Sleep	1	
11	Comment	Kill Process	firefox.exe	
12	Comment	Openvpn Gui Open Menu		
13	Comment	Openvpn Connect Object	Connetti	
14	Comment	Rename PerfData	Openvpn Connect Object	Trova Pulsante Connetti
15	Comment	Openvpn Auth		
16	Comment	Send Keys	alyvix	
17	Comment	Send Keys	{tab}	
18	Comment	Send Keys	{ctrl down}v{ctrl up}	
19	Comment	Sleep	1	
20	Comment	Send Keys	{enter}	
21	Comment	Openvpn Connected Image		
22	Comment	Openvpn Gui Open Menu		
23	Comment	Openvpn Connect Object	Disconnetti	
24	Comment	Rename PerfData	Openvpn Connect Object	Trova Pulsante Disconnetti

An 'Alyvix - Select Finder' dialog box is open, listing various Alyvix objects such as 'gebank_ready_bank [OF]', 'gesbank_close [OF]', and 'wspeccp_pdf_load [OF]'. A terminal window titled 'nscsp' is also visible, showing network-related logs and error messages.

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**