

Have you ever thought of...

Using Zabbix for...

- making pizza?
- maccheroni?
- cappuccino?



Neither did we, but...



Using Zabbix as Access Control engine

Gabriele Armao
Systematica Srl.

Who am I?



Gabriele Armao

System Administrator at Systematica Srl

Zabbix Certified Trainer since November 2012

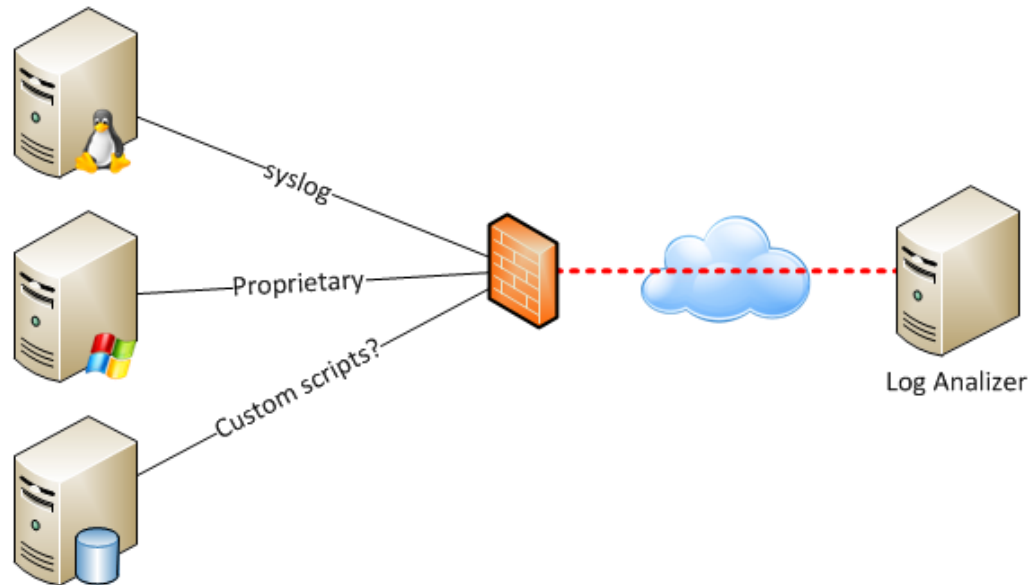
Email: g.armao@ads.it

Who is Systematica?

- Italian company, part of the “Gruppo Finmatica”
- 300 employee, 25mil € sales volume developing management software for public administrations
- Zabbix Certified Partner and Trainer
- Over 100 customers monitored through Zabbix, ~1000 hosts, ~25000 items, ~10000 triggers
- Zabbix is used for custom application, backup, access control monitoring
- Website: <http://www.ads.it>

The Problem

- Find a standard way to collect, filter at origin and transmit our customers' access logs through internet (VPN)

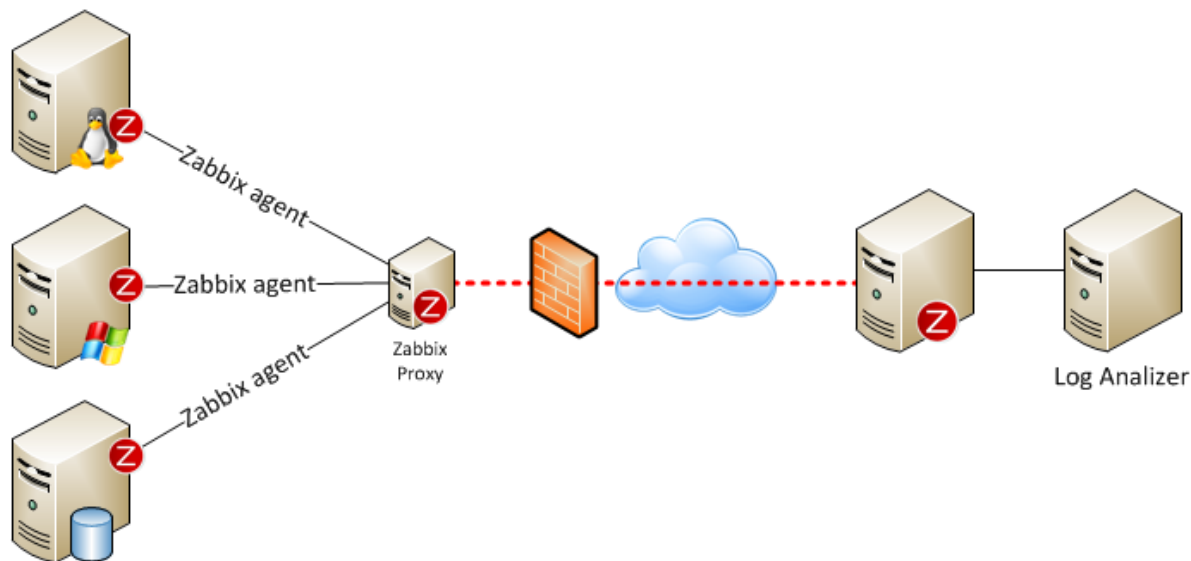


Hint: they already have zabbix agents installed for systems monitoring

The Solution (1)

Use Zabbix as underlying engine to collect servers' logs by using `log[]`, `eventlog[]` items and custom scripts:

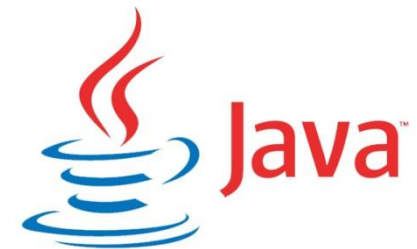
- Agent can filter any type of log via `log[]`, `eventlog[]` items and custom scripts
- Logs can be collected in a standard way (zabbix protocol) and cached by Zabbix Proxy



The Solution (2)

Java engine that periodically:

- Reads data from Zabbix database history and history_log table (will use API in the future)
- Parses and matches every log with custom built regexps to extract, correlate and format logins/logouts
- Feed an external database table with normalized entries





Solution (3)

- Tomcat webapp (company standard) that allows:
 - visualization
 - filtering
 - exporting of data in CSV format



Screenshot

MLog Access Control
MANAGEMENT LOG DI SISTEMA E SERVIZI REMOTI

FINMATIC : 20/10/2010  Accessi  Dizionari


Criteri di ricerca


Utente: --


Host: --

Log: Windows Login

Logon/Logoff | Connessione | Fascia oraria

dalle ore: 10:00:00 del: 19/10/2010 

fino alle ore: 11:59:59 del: 19/10/2010 

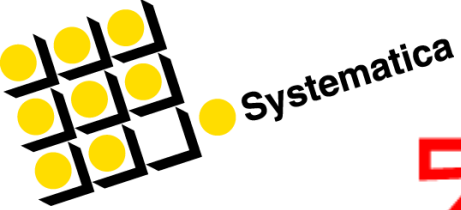
 Cerca

Utente	Host	Log	Ora Logon	Ora Logoff	Motivo Logoff	Tipo Logon	IP	Processo
PERSONALE\Administrator	Finmatica_personale	Windows Login	19/10/2010 08:53:44	19/10/2010 11:19:02	Chiusura per PID	10	10.97.200.130	User32
FINMATICA\ffantoni	Finmatica_ts01	Windows Login	19/10/2010 10:42:24	19/10/2010 10:42:40	Chiusura per PID	10	10.97.200.87	User32
FINMATICA\ffantoni	Finmatica_ts01	Windows Login	19/10/2010 10:42:24	19/10/2010 10:42:26	Chiusura per PID	10	10.97.200.87	User32
FINMATICA\glombardo	Finmatica_ts01	Windows Login	19/10/2010 11:08:29	19/10/2010 11:08:45	Chiusura per PID	10	10.98.30.38	User32
FINMATICA\backup	Finmatica_ts01	Windows Login	19/10/2010 10:18:28	19/10/2010 10:18:28	Chiusura per PID	2	:::1	seclogo
FINMATICA\backup	Finmatica_ts01	Windows Login	19/10/2010 10:18:28	19/10/2010 10:18:28	Chiusura per PID	2	:::1	seclogo
FINMATICA\backup	Finmatica_ts01	Windows Login	19/10/2010 11:40:11	19/10/2010 11:40:11	Chiusura per PID	2	:::1	seclogo
FINMATICA\backup	Finmatica_ts01	Windows Login	19/10/2010 11:40:11	19/10/2010 11:40:11	Chiusura per PID	2	:::1	seclogo
FINMATICA\loliveri	Finmatica_ts01	Windows Login	19/10/2010 11:47:56	19/10/2010 11:50:41	Chiusura per PID	10	10.97.200.98	User32
FINMATICA\loliveri	Finmatica_ts01	Windows Login	19/10/2010 11:47:56	19/10/2010 11:47:59	Chiusura per PID	10	10.97.200.98	User32
FINMATICA\backup	Finmatica_ts01	Windows Login	19/10/2010 11:49:50	19/10/2010 11:49:50	Chiusura per PID	2	:::1	seclogo
FINMATICA\backup	Finmatica_ts01	Windows Login	19/10/2010 11:49:50	19/10/2010 11:49:50	Chiusura per PID	2	:::1	seclogo
FINMATICA\loliveri	Finmatica_ts01	Windows Login	19/10/2010 11:51:13	19/10/2010 11:53:40	Chiusura per PID	10	10.97.200.98	User32
FINMATICA\loliveri	Finmatica_ts01	Windows Login	19/10/2010 11:51:13	19/10/2010 11:51:14	Chiusura per PID	10	10.97.200.98	User32
FINMATICA\loliveri	Finmatica_ts01	Windows Login	19/10/2010 11:52:57	19/10/2010 11:53:40	Chiusura per PID	10	10.97.200.98	User32
FINMATICA\loliveri	Finmatica_ts01	Windows Login	19/10/2010 11:52:57	19/10/2010 11:52:58	Chiusura per PID	10	10.97.200.98	User32

Questions



No questions
allowed because...

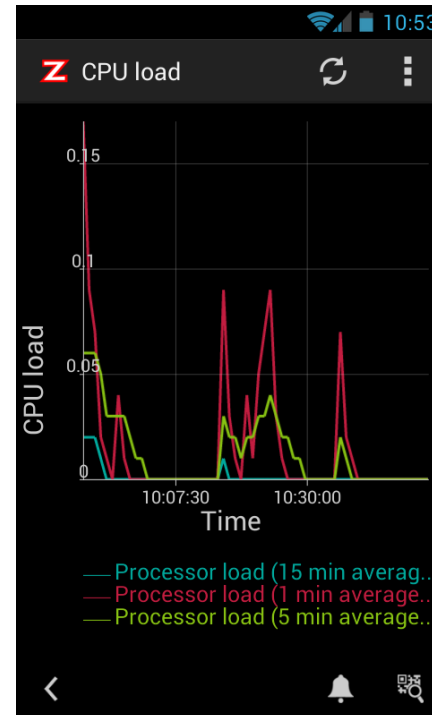
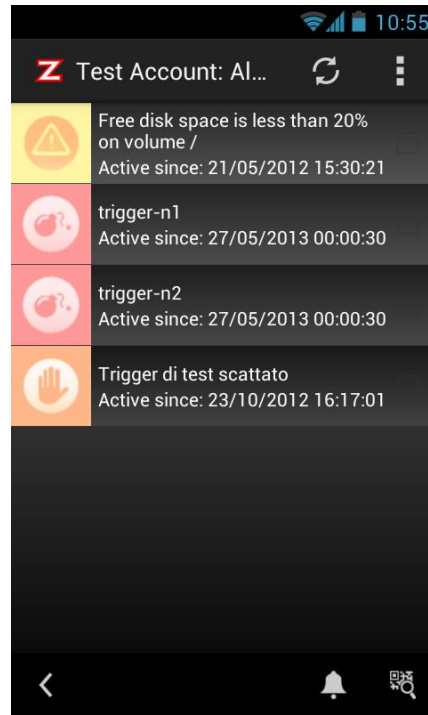
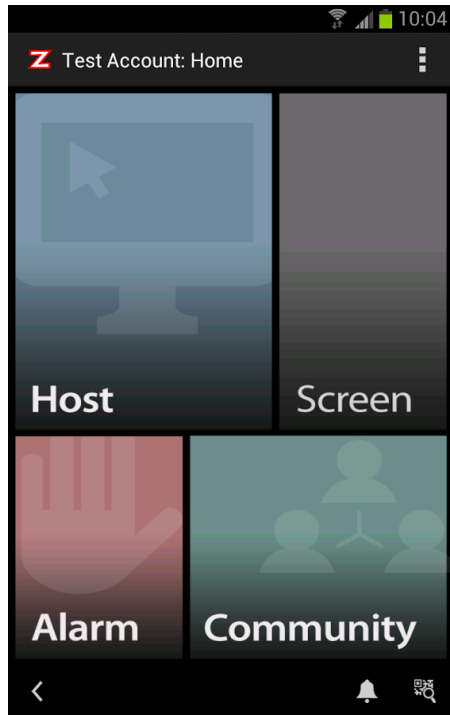


ZABAPP!



ZABBIX 2013
Conference

- OpenSource Android Zabbix App
- Community based



- Interested? <http://www.zabapp.it>

Seriously now, questions?



Thank you!