Event Driven Monitoring
(Monitorare la rete sfruttando le segnalazioni degli apparati)

Autori: Stefano Gargiulo – GARR

ABSTRACT

Nella presentazione verrà illustrato TrapMon il framework per la collezione e l'elaborazione di Trap SNMP realizzato al GARR. Il software, grazie alla sua flessibilità ed indipendeza dagli oggetti monitorati (ascolta le sengalazioni provenienti da qualsiasi tipo di apparato) permette di ampliare lo spettro di eventi monitorabili in diversi ambienti, adattandosi a diversi contesti in maniera automatica.

Verranno quindi illustrate le principali caratteristiche dello strumento, quali la sua architettura a plugin che permette di definire trigger real-time sugli eventi e di estendere facilmente il framework, nonché il livello di astrazione iAlarms che offre una UI per la creazione di allarmi a partire da qualsiasi tipo di trap, aumentando così la leggibilità e la carica semantica associata a quest'ultime (offrendo strumenti avanzati quali aggregazione di eventi, grafici, algoritmi di filtraggio dei farsi allarmi, ticketing interno, statistiche, storicizzazione degli eventi salienti ecc.).

Sarà inoltre illustrato come lo strumento possa essere utilizzato al fine di scoprire nuove soglie e stati monitorabili nei MIB dei vari oggetti, divenendo così una sorta di strumento per la rilevazione dei problemi latenti, punto che lo renderà molto utile anche nelle fasi di migrazione a GARR-X ove l'introduzione di nuove tecnologie ed apparati, con il consequenziale e repentino aumento delle variabili e degli elementi da monitorare richiederà un adeguata e rapida risposta da parte dell'infrastruttura di monitoring.