



Contribution ID: 36

Type: **Presentazione orale**

NtopInsight an automatic tool for network identification and inventory @ LNS

Thursday, 26 May 2022 14:50 (20 minutes)

L'osservabilità della rete è un aspetto cruciale in un sito come LNS, la cui utenza prevede anche apparati sperimentali dislocati in sedi differenti da quella centrale.

Storicamente l'inventario LNS era basato su un sistema fatto in casa e basato su un database, ed arpwatich. Il sistema faceva un discovery continuo della rete locale, e alla scoperta di un nuovo mac address inseriva l'host nel database, permettendo di associarlo ad un utente. Questo sistema, semplice ma efficace, era limitato principalmente dalla povertà di informazioni associabili all'oggetto inventariato, e quindi la poca aggregabilità delle stesse informazioni inserite: non si poteva raggruppare per locazione, o per gruppo logico di utenti.

Per questo motivo, il sistema è stato completamente rivisto, rivedendo sia lo strumento di discovery, che di gestione vera e propria degli asset. Per il primo scopo, la scoperta di nuove risorse in rete, è stato scelto ntopng, che è in grado di fornire in tempo reale, sia attraverso interfaccia web sia attraverso REST API, vari tipi di dati come il numero di host corredati di utili informazioni accessorie, come hostname, indirizzo IPV4 e IPV6, mac address. Per il secondo scopo è il plugin Insight della suite Jira Software.

Per quest'ultimo era disponibile anche un ulteriore tool, Insight Discovery, che avrebbe potuto sostituire ntopng e che consentirebbe anche l'importazione delle informazioni di rete direttamente su Insight. Discovery ha lo svantaggio di dover essere installato localmente, mentre l'istanza in uso di Insight è installata on-premise sui servizi nazionali. Sostanzialmente quindi il lavoro fatto consiste nell'interfacciare in maniera sicura ntopng e Insight, allo scopo di monitorare lo stato di attività della rete locale dei Laboratori Nazionali del Sud e nello stesso tempo realizzare un inventario degli asset informatici che venga inizializzato riempito ed aggiornato in maniera automatica. Parallelamente, a partire dai template predefiniti di Insight, è stato definito un Object Schema personalizzato per riflettere l'organizzazione logica degli host LNS e gli attributi ritenuti utili, ad esempio il gruppo di ricerca, il responsabile della risorsa, la locazione fisica e così via.

Gli script che interfacciano Ntop e Insight girano su una macchina pivot che esegue operazioni schedate manipolando dati in formato json provenienti da ntop e li scrive su Insight rispettando l'object schema dell'albero dell'inventario. La manipolazione dei file in locale sulla macchina pivot consente di fare una serie di analisi sia di tipo quantitativo, monitorando il numero di host complessivo, sia di tipo qualitativo monitorando le informazioni specifiche degli host, come il cambio di macaddress a parità di IP.

Gli host scoperti da ntop vengono inizialmente inseriti su Insight in un ramo d'ingresso, dal quale possono successivamente essere processati manualmente ed assegnati ad altri rami dell'albero. Questa operazione deve necessariamente fatta manualmente perchè nessuno strumento automatico potrebbe classificare ed assegnare a una categoria un oggetto della rete aggiungendo gli attributi necessari alla completa classificazione,

Questo sistema è tuttora in via di sviluppo, e ulteriori features saranno aggiunte discutendole all'interno del gruppo di lavoro nazionale recentemente costituito relativo alla gestione dell'asset management IT, nel quale gli LNS contribuiranno mettendo a disposizione quanto sviluppato.

Primary authors: GIORGIO, Emidio Maria (Istituto Nazionale di Fisica Nucleare); CANNIZZARO, Stefano (Istituto Nazionale di Fisica Nucleare)

Presenter: CANNIZZARO, Stefano (Istituto Nazionale di Fisica Nucleare)

Session Classification: Servizi ICT

Track Classification: Servizi ICT