

Servizio di notifica degli Alerts di ntopng su Slack.com

Sauro Pollastrini

Relazione

Slack è un servizio di messaggia appositamente pensato per team di lavoro, e mette a disposizione dei suoi utenti diverse app e integrazioni che è possibile aggiungere alla messaggia del proprio team.

Tra queste c'è la “Incoming Webhook”, che permette di mandare messaggi su uno specifico canale Slack mediante un semplice comando POST http, con un file JSON contenente il testo del messaggio ed altri eventuali attributi (ad esempio l'icona da utilizzare).

Sfruttando questa “Incoming Webhook”, con il presente progetto è stato messo a punto, per il programma ntopng, un servizio di notifica degli allarmi.

E' possibile scegliere:

- se ricevere o meno tali notifiche
- quali notifiche ricevere, in relazione alla gravità del pericolo
- il nominativo che sarà visualizzato su Slack come mittente del messaggio.

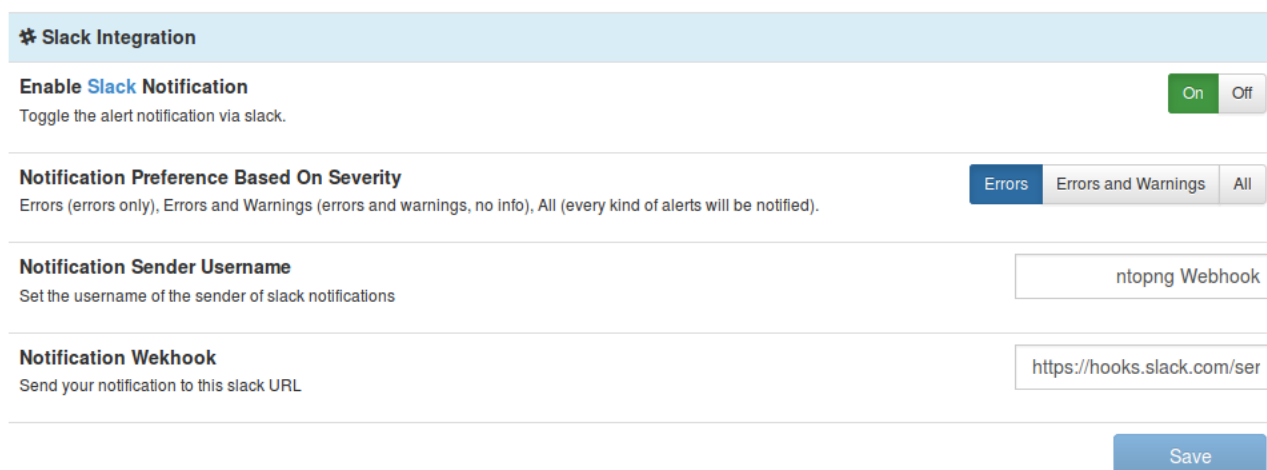
Vediamo come fare.

Dalla pagina principale di ntopng, scegliendo “Preferences” e poi “Alerts” si apre la pagina in figura:

Runtime Preferences

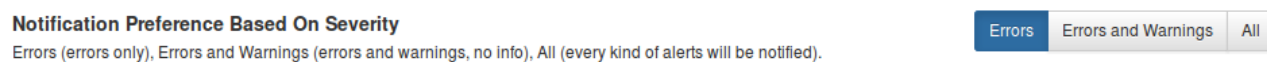
Users	Alerts
Network Interfaces	Enable Alerts Toggle the overall generation of alerts. On Off
In-Memory Data	Maximum Number of Alerts per Entity The maximum number of alerts per alarmable entity. Alarmable entities are hosts, networks, interfaces and flows. Once the maximum number of entity alerts is reached, new alerts raised by the same entities will be discarded. Default: 1024. <input type="text" value="1024"/>
On-Disk Timeseries	Enable Probing Alerts Enable alerts generated when probing attempts are detected. On Off
On-Disk Databases	Enable Hosts Malware Blacklists Enable alerts generated by traffic sent/received by malware-marked hosts. On Off
Alerts	Alerts On Syslog Enable alerts logging on system syslog. On Off
Units of Measurement	* Slack Integration
Log Level	Enable Slack Notification Toggle the alert notification via slack. On Off
	Save

Ponendo su ON l'interruttore di "Enable Slack Notification", in fondo alla pagina, si abilitano le notifiche degli alerts su Slack e si visualizzano i campi da completare per poterle ricevere:



Ntopng divide gli alerts, in base alla gravità, in tre categorie: errori, avvertimenti (warnings), e informazioni.

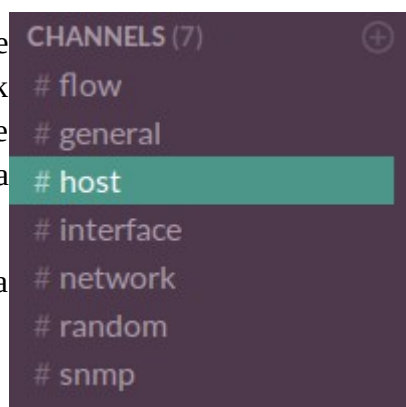
Tramite il pulsante di scelta multipla nella figura seguente, è possibile scegliere se ricevere notifiche solo relativamente agli errori (Errors), sia ad errori che a warnings (Errors and Warnings), oppure tutti i tipi, info incluse (All)



E' necessario poi inserire, negli appositi campi, il nome con cui si desidera che le notifiche vengano spedite e, cosa fondamentale, l'indirizzo della Webhook ricevuto da Slack.

A questo punto manca solo un ulteriore passo, cioè la creazione sulla messaggeria del team di 5 canali: flow, host, interface, network e snmp. Questo perché ntopng divide ulteriormente gli alerts in base alle cause, e spedirà la notifica sul canale corrispondente a quella rilevata.

Nella figura di destra si vede la parte Channels del menù della propria messaggeria Slack dopo aver creato i canali necessari.



Fatto tutto quanto sopra si riceveranno, in base alle scelte, le notifiche su Slack.

Appariranno in questo modo:



Il nome del mittente riporterà la gravità dell'alert, e anche l'icona sarà diversa in base ad essa:



Errors

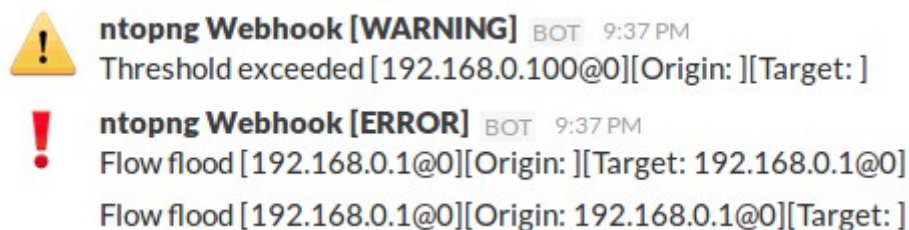


Warnings



Info

Al variare della gravità per notifiche successive l'icona cambierà, purtroppo però, e questo dipende dall'attuale layout di Slack, in caso di notifiche successive di alerts della stessa gravità, queste si accumuleranno sotto la prima senza una netta divisione fra di esse, un esempio:



Slack dispone anche di una app per dispositivi mobile, per cui è possibile ricevere le notifiche di ntopng anche su tali dispositivi (di solito con alcuni secondi di ritardo rispetto all'utilizzo su computer, da quanto rilevato con i test).

Realizzazione

La parte dell'interfaccia grafica, scritta in lua, è stata realizzata facendo uso delle procedure già utilizzate nell'interfaccia stessa in tutta la parte relativa alle preferenze, chiaramente adattandole, tramite i parametri passati, alle esigenze proprie della realizzazione del servizio notifiche.

La realizzazione del servizio vero e proprio è stata fatta tramite l'inserimento nel codice di *AlertsManager.cpp* (parte di ntopng che, come si intuisce dal nome, gestisce gli alerts), di due funzioni: la prima, *notifySlack*, decide in base alle scelte fatte nelle preferenze se sia necessario o meno effettuare la notifica su Slack. In caso positivo invoca la seconda funzione, *notifyAlert*, la quale si occupa invece di costruire il file JSON contenente il testo del messaggio, lo username del mittente e l'icona. Una volta costruito, il messaggio viene inserito come stringa di testo in una coda contenuta in un server-redis, tool al quale ntopng si appoggia in diverse occasioni.

Ntopng ha alcuni thread che si occupano di svolgere attività periodiche. Uno di questi, denominato *housekeepingLoop*, ogni 3 secondi esegue uno script lua (*housekeeping.lua*), all'interno del quale viene chiamata la funzione *SendSlackMessages()*. Tale funzione, contenuta in *slack_utils.lua*, non fa altro che svuotare la coda nel server-redis, estraendo e finalmente spedendo i messaggi uno a uno alla messaggeria Slack.