

Relazione esercizio d'esame Gestione di Reti 2021

Gabriele Masciotti 578318

Il seguente elaborato riporta una breve relazione riguardante lo svolgimento dell'esercizio d'esame assegnatomi. Il suddetto esercizio consiste nell'utilizzare il tool di monitoraggio via snmp "**Zabbix**" per simulare in piccolo una situazione di monitoraggio di rete. In particolare, come suggerito dal docente, mi sono concentrato nel monitorare le discontinuità di servizio degli agent snmp, implementando dei trigger per l'invio di segnalazioni di allarme in caso di cambiamento di stato e disponibilità degli host selezionati.

Dopo aver installato il programma Zabbix (server e agent), predisposto un database MySQL necessario per il funzionamento del tool, configurato correttamente il programma modificando i file di configurazione e predisposto l'interfaccia front-end con la dashboard zabbix, mi sono recato sul sito www.shodan.io per cercare qualche agent snmp attivo da utilizzare nell'esperimento.

Utilizzando il menù "*configurazione*" del tool ho **aggiunto gli host da monitorare**; come si vede nell'[immagine 1](#), è sufficiente inserire l'indirizzo IP dell'host su cui è in esecuzione l'agent snmp alla porta 161.

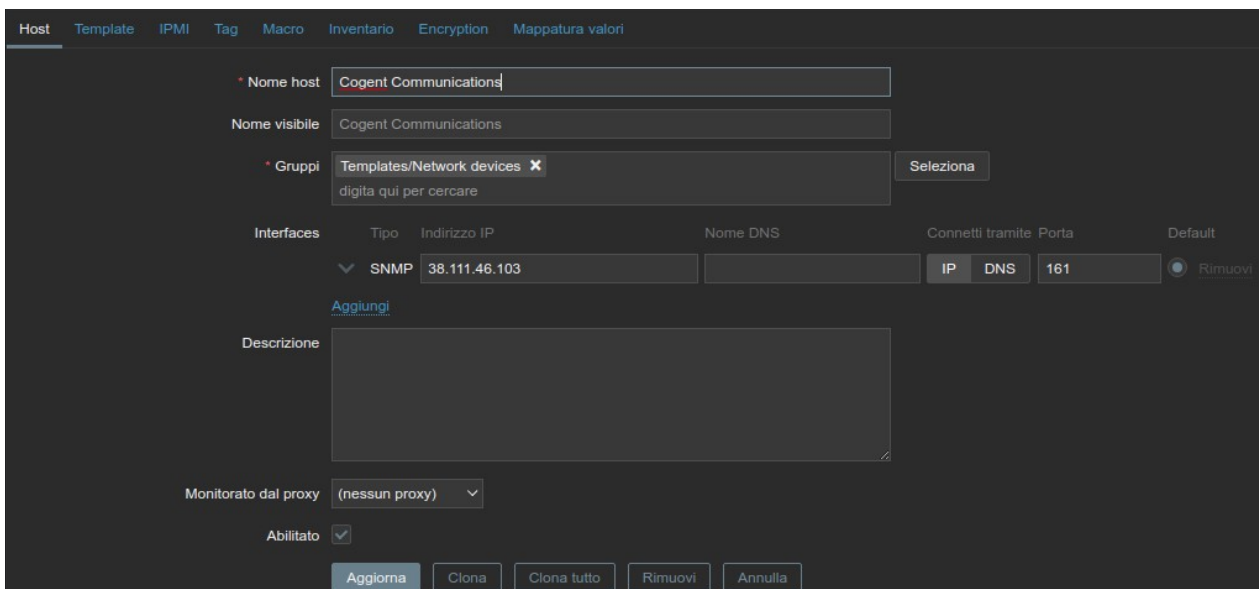
The image shows the Zabbix web interface for adding a new host. The 'Host' tab is selected in the top navigation bar. The form contains the following fields: 'Nome host' with the value 'Cogent Communications'; 'Nome visibile' with the same value; 'Gruppi' with a dropdown menu showing 'Templates/Network devices' and a 'Seleziona' button; 'Interfaces' section with a table containing one entry: 'SNMP' with IP '38.111.46.103', 'Nome DNS' empty, and 'Connetti tramite' set to 'IP' and 'Porta' set to '161'. There is an 'Aggiungi' link below the table. 'Descrizione' is an empty text area. 'Monitorato dal proxy' is set to '(nessun proxy)'. 'Abilitato' is checked. At the bottom are buttons for 'Aggiorna', 'Clona', 'Clona tutto', 'Rimuovi', and 'Annulla'.

Immagine 1

L'agent in questione è in esecuzione in un host di rete della Cogent Communications, un fornitore di servizi Internet multinazionale con sede negli Stati Uniti.

Dopo aver aggiunto l'host è stato necessario **creare degli item da monitorare**. Un item è sostanzialmente una metrica su cui si vuole interrogare l'agent con il polling da parte del server zabbix. Utile al mio scopo è stato impostare l'item mostrato in [figura 2](#).

Questo item contiene un "controllo interno" (*internal check*) di zabbix, utilizzato per verificare la disponibilità del servizio snmp.

Oltre agli item con tipo "interno" possono esserne creati ovviamente anche di altre tipologie, come per esempio quello in [figura 3](#), (di tipo "snmp agent") utilizzato per richiedere all'agent snmp il numero di ottetti in ingresso nell'interfaccia di rete numero 2 dell'host.

Item Tag Preprocesso

* Nome

Tipo

* Chiave

Tipo di informazione

Unità

* Intervallo di aggiornamento

Intervalli personalizzati

Tipo	Intervallo	Periodo	Azione
<input type="button" value="Flessibile"/> <input type="button" value="Schedulazione"/>	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	<input type="button" value="Rimuovi"/>

[Aggiungi](#)

* Periodo storicizzazione History

* Periodo storicizzazione Trend

Mappatura valori

Popola campo inventario host

Descrizione

Abilitato ☒

Immagine 2

Item Tag Preprocesso

* Nome

Tipo

* Chiave

* Interfaccia host

* SNMP OID

Tipo di informazione

Unità

* Intervallo di aggiornamento

Intervalli personalizzati

Tipo	Intervallo	Periodo	Azione
<input type="button" value="Flessibile"/> <input type="button" value="Schedulazione"/>	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>	<input type="button" value="Rimuovi"/>

[Aggiungi](#)

* Periodo storicizzazione History

* Periodo storicizzazione Trend

Mappatura valori

Popola campo inventario host

Descrizione

Abilitato ☒

Immagine 3

Come si nota, nel caso di un item di tipo “snmp agent” è necessario inserire anche l’OID snmp. Questi identificatori possono essere ottenuti con facilità attraverso un terminale richiedendo con un comando **snmpwalk** la struttura dell’albero delle registrazioni dell’host remoto.

A questo punto si può procedere con la **definizione dei trigger**. Un trigger è un controllo effettuato dal tool zabbix sui nuovi dati ricevuti in seguito al poll agli agent snmp; se questi soddisfano una certa condizione, specificata in fase di creazione, il programma mette il trigger in stato *problema* ed esegue le *azioni* che l'utente ha delineato nell'apposito menù (come vedremo poco più avanti).

Immagine 4

L'immagine 4 mostra la definizione di un trigger di gravità media che si attiva nel momento in cui un agent snmp non è più disponibile. L'espressione utilizzata ha il seguente significato: l'ultimo valore ricevuto dall'item per il controllo interno sulla disponibilità del servizio snmp (definito sopra) è 0 (cioè l'agent snmp non è raggiungibile).

Come abbiamo detto, quando il controllo predisposto dal trigger ha successo, il trigger passa dallo stato **ok** allo stato **problema**;

e successivamente il programma esegue le “trigger actions” create dall'utente.

Creare un'azione significa stabilire che cosa si vuole che Zabbix faccia nel momento in cui un trigger passa allo stato problema. Dopo aver stabilito le condizioni che si devono verificare affinché l'azione venga eseguita, come si osserva in figura 5, si procede alla definizione delle operazioni.

Immagine 5

La **definizione delle operazioni** consiste nell'impostare una serie di passi che il tool deve eseguire per gestire il problema. Nel caso di questo esercizio l'obiettivo era far generare un messaggio di errore al programma, che avvisasse sulla non raggiungibilità dell'agent snmp. Per far questo è stato sufficiente compilare il form di dettaglio come mostrato nell'immagine 6, specificando di inviare un'email all'utente con del testo personalizzato (il servizio di notifica funziona soltanto se configurato correttamente nella sezione "User settings", impostando la propria mail per ricevere gli avvisi, e nella sezione "Tipi di supporto" sotto il menù "Amministrazione", in cui, nel caso delle email, è necessario inserire i dati di un server smtp per l'invio delle segnalazioni).

Immagine 6

Immagine 7: impostazioni del tipo di supporto "email"

ATTIVITÀ DI MONITORAGGIO

Dopo aver ripetuto i passi precedenti per un altro paio di host, ho lasciato che il tool raccogliesse dati per poter analizzare l'attività degli agent snmp. In particolare ho notato che negli host con un traffico di rete intenso le discontinuità di servizio snmp non sono affatto rare, anzi si verificano piuttosto spesso. Prendendo per esempio l'host della Cogent Communications, già nominato precedentemente, si nota come l'agent snmp cessi di essere raggiungibile più volte nell'arco della giornata. Osservando il grafico nella figura 8 si vedono le variazioni di valore dell'item per il controllo della disponibilità dell'agent snmp (di cui abbiamo parlato sopra):

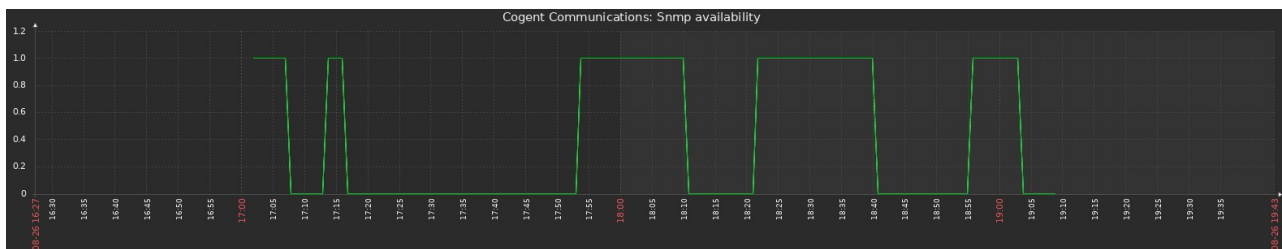


Immagine 8

È evidente che l'agent non abbia un'attività di servizio regolare nel tempo, passando diverse volte dall'essere attivo al non esserlo in poche ore.

Questa irregolarità comporta inevitabilmente il mancato raccoglimento dei dati da monitorare nei periodi "di down", lasciando dei gap nelle misurazioni; questo si evince già dal grafico sottostante

(immagine 9) che banalmente riporta il numero sempre crescente di ottetti in ingresso nell'interfaccia di rete dell'host.

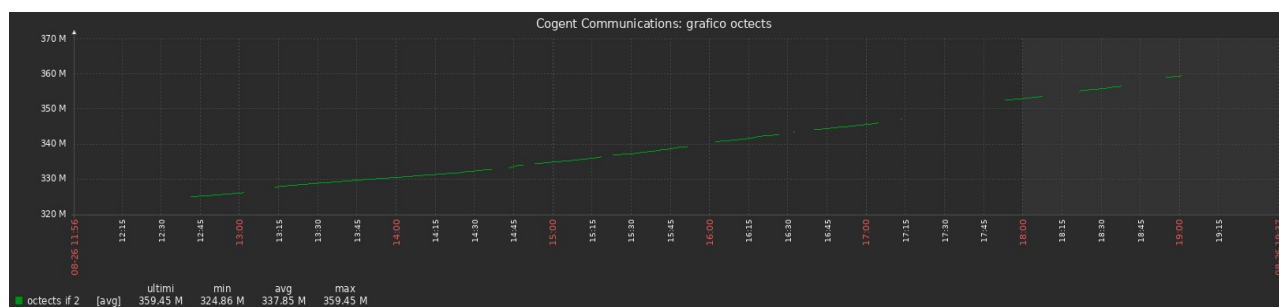


Immagine 9

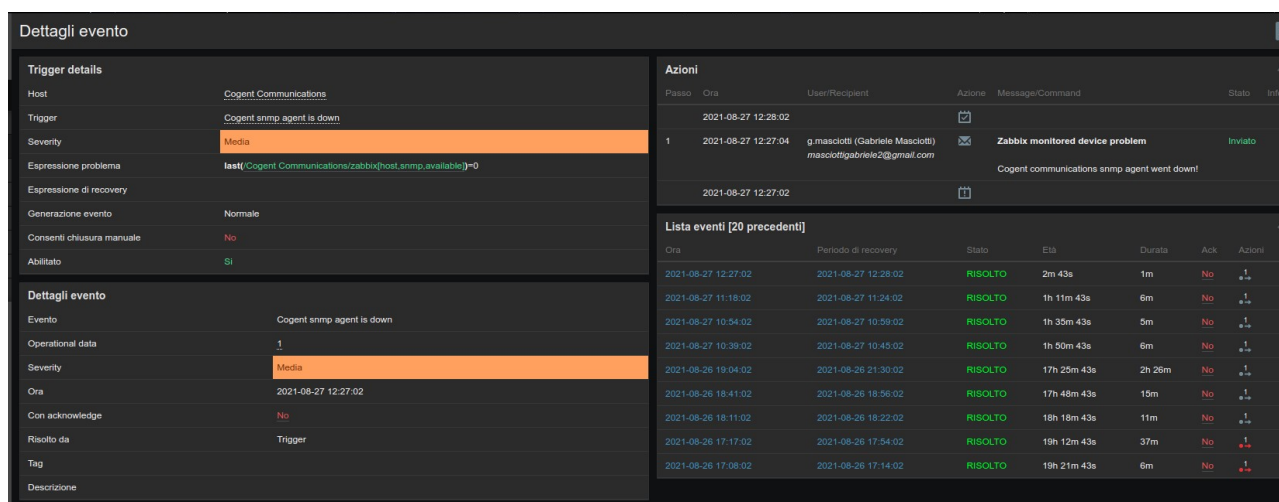


Immagine 10: serie di problemi riscontrati da zabbix sulla disponibilità snmp dell'agent nel tempo

Decisamente migliore è la situazione di un altro host che ho monitorato. Si tratta di un host di rete della Bell Canada, una compagnia di telecomunicazioni canadese con sede a Montreal. L'agent snmp in esecuzione su questo host ha un'attività più stabile di quello visto precedentemente, restando attivo per periodi più lunghi senza cessare di essere raggiungibile. Di seguito riporto il grafico sulla disponibilità.

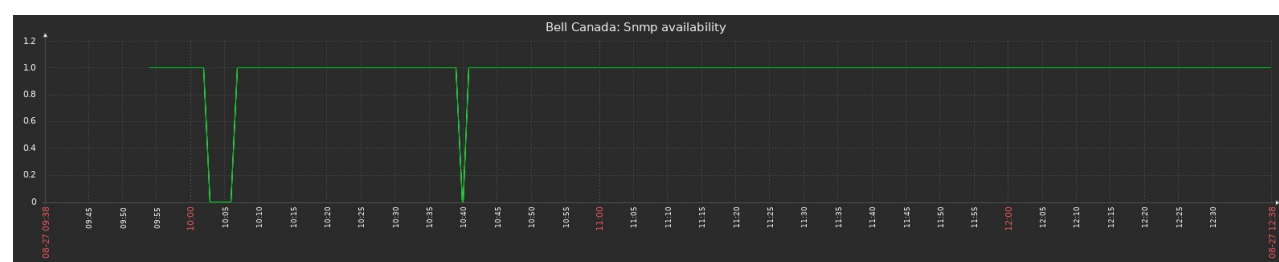


Immagine 11: grafico che mostra la disponibilità dell'agent snmp canadese nel tempo

Un agente snmp attivo senza troppe interruzioni significa poter raccogliere correttamente i dati di monitoraggio dell'host, senza perdite che possano causare difficoltà o impossibilità nell'avere delle stime di funzionamento del sistema verosimili. Anche in questo caso riporto il grafico degli ottetti in ingresso all'interfaccia di rete, che, seppur in modo banale, evidenzia un'attività di raccoglimento dei dati di monitoraggio molto più efficiente di quella precedente, permettendo di effettuare analisi a grana più fine del funzionamento del sistema.

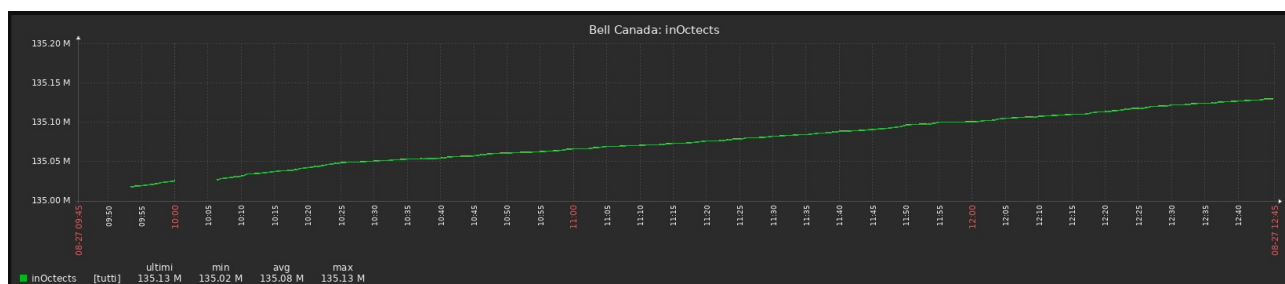


Immagine 12: ottetti in ingresso nell'interfaccia di rete dell'host canadese