

# 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.

## 1. Installazione del tool Zabbix

Per prima cosa ho provveduto ad **installare il programma Zabbix** nel sistema **Ubuntu** (Focal 20.04). Per farlo è stato necessario innanzitutto aprire un terminale e digitare i seguenti comandi per effettuare l'installazione del repository di Zabbix nella **versione 5.4**:

- `wget https://repo.zabbix.com/zabbix/5.4/ubuntu/pool/main/z/zabbix-release/zabbix-release\_5.4-1+ubuntu20.04\_all.deb`
- `dpkg -i zabbix-release_5.4-1+ubuntu20.04_all.deb`
- `apt update`

per poi procedere con l'installazione vera e propria dei vari componenti (server zabbix, agent e interfaccia front-end):

- `apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent`

Ho proseguito con la predisposizione di un **database MySQL** necessario per il funzionamento del programma, definendo anche una **password** di accesso:

- `mysql -uroot -p "password"`
- `mysql> create database zabbix character set utf8 collate utf8_bin;`
- `mysql> create user zabbix@localhost identified by 'password';`
- `mysql> grant all privileges on zabbix.* to zabbix@localhost;`
- `mysql> quit;`

Successivamente ho lanciato il seguente comando per importare lo schema e i dati iniziali del server zabbix. Il sistema chiede di inserire la **password** appena creata in fase di predisposizione del database.

- `zcat /usr/share/doc/zabbix-sql-scripts/mysql/create.sql.gz | mysql -uzabbix -p zabbix`

A questo punto è sufficiente editare il file di configurazione del server nella directory `/etc/zabbix/zabbix_server.conf`, inserendo la **password** del nuovo database: `DBPassword="password"`. In questo modo il server zabbix potrà accedervi.

Terminata l'installazione e la configurazione del tool, si può finalmente procedere con l'abilitazione dei processi server e agent:

- `systemctl restart zabbix-server zabbix-agent apache2`
- `systemctl enable zabbix-server zabbix-agent apache2`

## 2. Configurazione dell'interfaccia web front-end di Zabbix

Mi sono collegato con un browser alla Zabbix frontend digitando l'indirizzo

<http://127.0.0.1/zabbix/>, e ho effettuato l'installazione dell'interfaccia web del servizio.

Dopo aver selezionato la lingua e controllato che tutti i prerequisiti software richiesti fossero rispettati, ho proseguito con la configurazione della connessione con il database creato al paragrafo precedente, come mostrato nell'immagine 1, inserendo la **password** di accesso.

The screenshot shows the 'Configure DB connection' step of the Zabbix installation wizard. On the left is a sidebar with the Zabbix logo and a list of steps: Welcome, Check of pre-requisites, Configure DB connection (highlighted), Zabbix server details, GUI settings, Pre-installation summary, and Install. The main area contains instructions to create a database manually and set configuration parameters. The form includes: Database type (MySQL), Database host (localhost), Database port (0, with a note '0 - use default port'), Database name (zabbix), Store credentials in (Plain text selected, HashiCorp Vault), User (zabbix), and Password (empty). A note about Database TLS encryption states that the connection will not be encrypted due to the use of a socket file on Unix or shared memory on Windows. At the bottom right are 'Back' and 'Next step' buttons.

Immagine 1

Successivamente ho impostato i dettagli del server zabbix (quelli che sono contenuti nel file di configurazione menzionato nel paragrafo precedente) già in esecuzione nel pc:

The screenshot shows the 'Zabbix server details' step of the Zabbix installation wizard. The sidebar is identical to the previous screen, with 'Zabbix server details' now highlighted. The main area contains instructions to enter the host name or IP address and port number. The form includes: Host (localhost), Port (10051), and Name (empty). At the bottom right are 'Back' and 'Next step' buttons.

Immagine 2

Infine ho ultimato la configurazione personalizzando un paio di parametri dell'interfaccia grafica nel passo successivo.

**\*\* In generale e soprattutto se dovessero verificarsi problemi nella connessione tra server Zabbix e database MySQL, è di fondamentale importanza controllare che i parametri**

- DBHost
- DBName
- DBUser
- DBPassword

nei file di configurazione `/etc/zabbix/web/zabbix.conf.php` e `/etc/zabbix/zabbix_server.conf` siano **NON** commentati (senza il `#` all'inizio della riga) e identici. \*\*

### 3. Predisposizione del tool per il monitoraggio

Dopo aver installato e configurato il programma Zabbix mi sono recato sul sito [www.shodan.io](http://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 3, è sufficiente inserire l'indirizzo IP dell'host su cui è in esecuzione l'agent snmp alla porta 161.

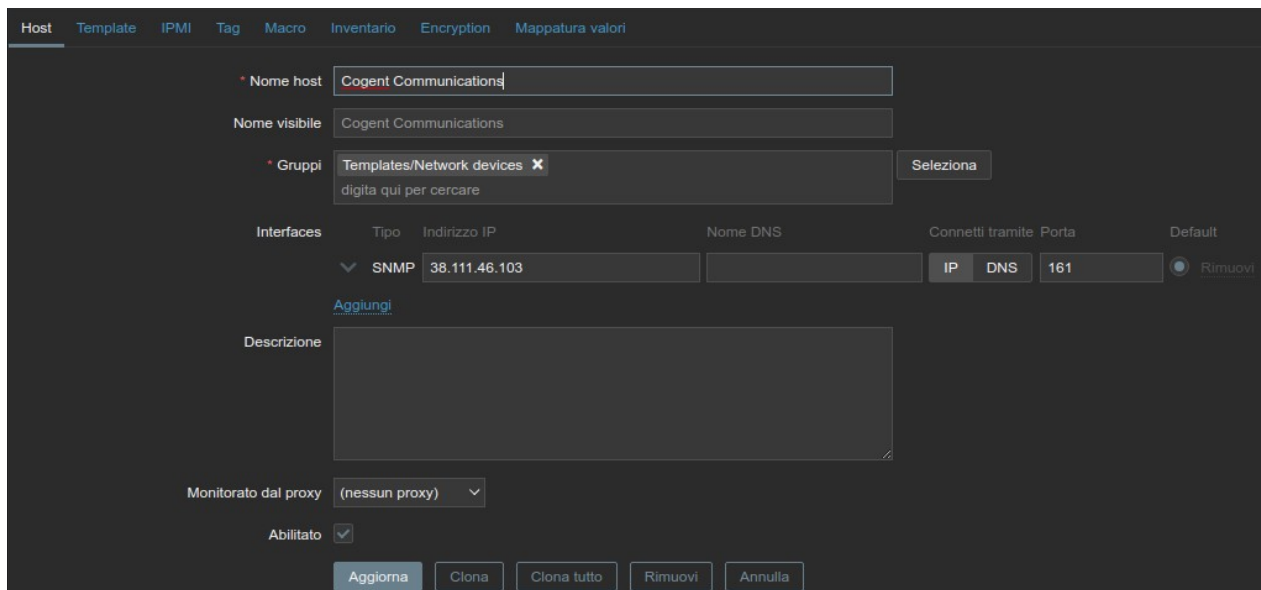


Immagine 3

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 4.

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 5, (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 4

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 5

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 6

L'immagine 6 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 7, si procede alla definizione delle operazioni.

Immagine 7

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 8, 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 8

Immagine 9: impostazioni del tipo di supporto "email"

A questo punto si è pronti per cominciare il monitoraggio. Utile è a questo scopo è sicuramente la creazione di grafici che illustrino i dati raccolti dagli host con il polling. Per **creare un grafico**, nella sezione "Configurazione" – "Host" – "Grafici", basta cliccare sul pulsante "Crea grafico" e personalizzare le impostazioni mostrate, soprattutto aggiungendo gli item che si desiderano rappresentare. Nel caso di questo esercizio ho creato un item, di un tipo differente rispetto a quelli citati precedentemente, per rappresentare le variazioni di traffico di rete in ingresso nell'interfaccia degli host selezionati per il monitoraggio. Si tratta di un item "Calculated", il quale per mezzo della funzione "change", predefinita in Zabbix, rappresenta la differenza di valore di un altro item tra una lettura e un'altra. Nell'immagine 10 si mostra la definizione dell'item calculated utilizzato per rappresentare le variazioni di lettura in lettura dell'item con chiave "octects", del quale abbiamo visto i dettagli nell'immagine 5.

\* Nome

Tipo

\* Chiave

\* Formula

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 10

#### 4. Attività di monitoraggio

Dopo aver ripetuto i passi descritti nel paragrafo precedente 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 11](#) si vedono le variazioni di valore dell'item per il controllo della disponibilità dell'agent snmp (di cui abbiamo parlato sopra):

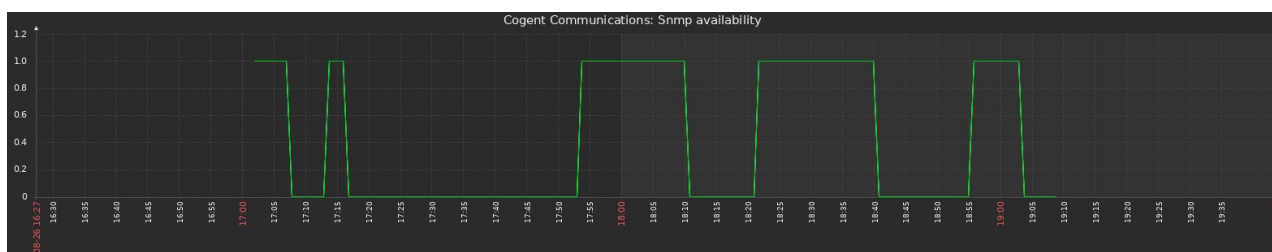


Immagine 11

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.



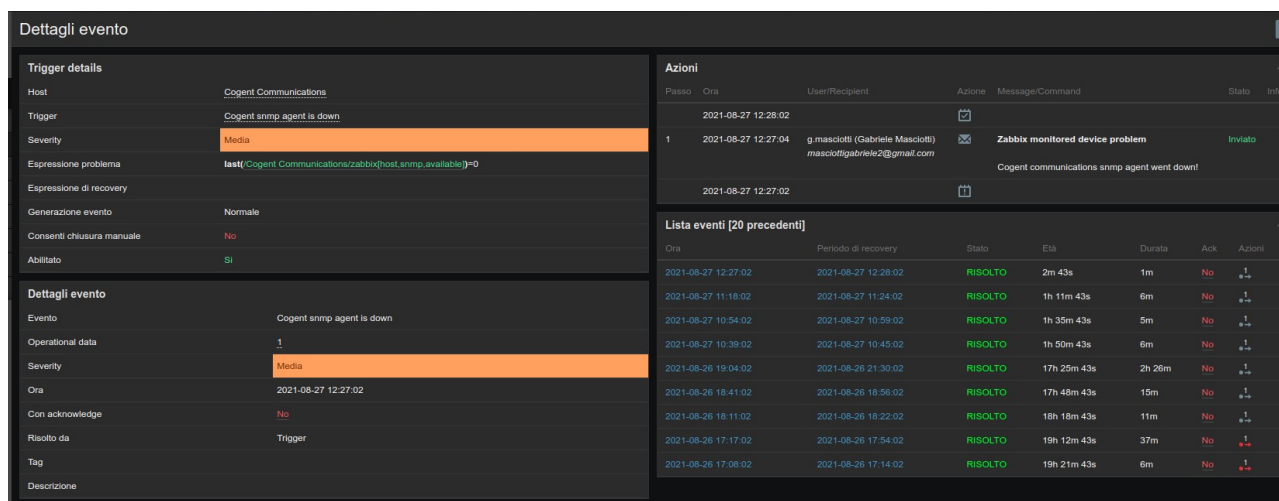


Immagine 12: serie di problemi riscontrati da zabbix sulla disponibilità snmp dell'agent nel tempo

Questa irregolarità comporta inevitabilmente il mancato raccoglimento dei dati da monitorare nei periodi “di down”, lasciando dei gap nelle misurazioni.

I valori mancanti provocano una scorretta rappresentazione della situazione monitorata. Questo fenomeno è evidente nell'esempio riportato nell'immagine 13, immediatamente seguente:

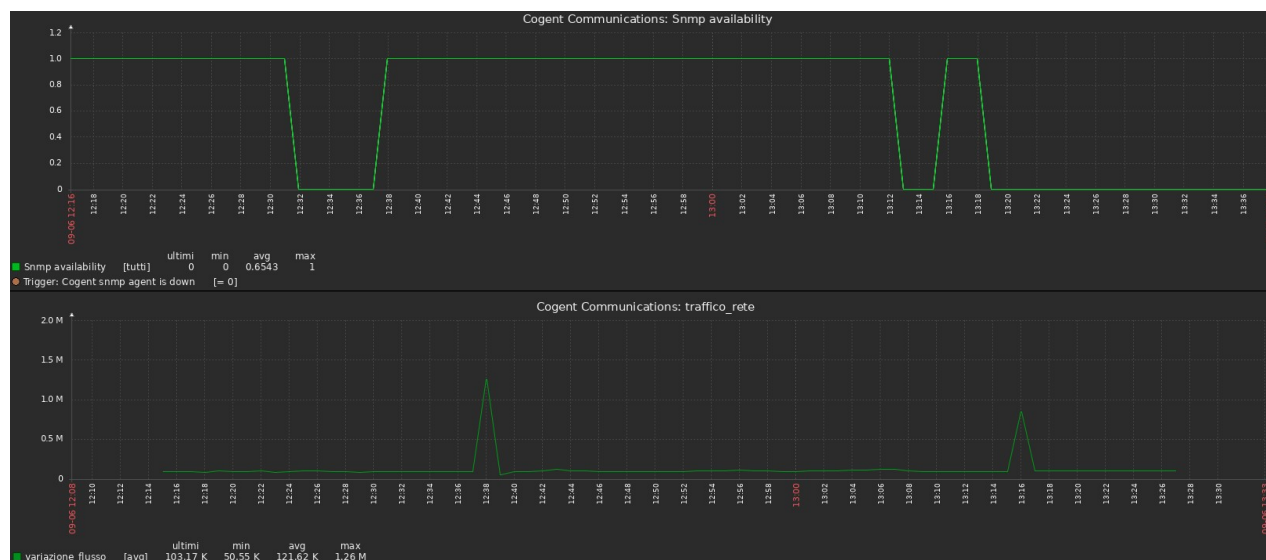


Immagine 13

Come si vede, il grafico che illustra le variazioni di traffico di rete (descritto alla fine del paragrafo precedente) presenta due picchi corrispondenti alla ricezione dei nuovi valori dopo i periodi di non disponibilità dell'agent. Questi valori ovviamente si discostano di molto dagli ultimi ricevuti prima del disservizio (sono aumentati mentre l'agent non era disponibile), causando un appiattimento del grafico nelle altre parti che riguardano il normale monitoraggio e i periodi di valori costanti durante la inattività dell'agent remoto.

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.



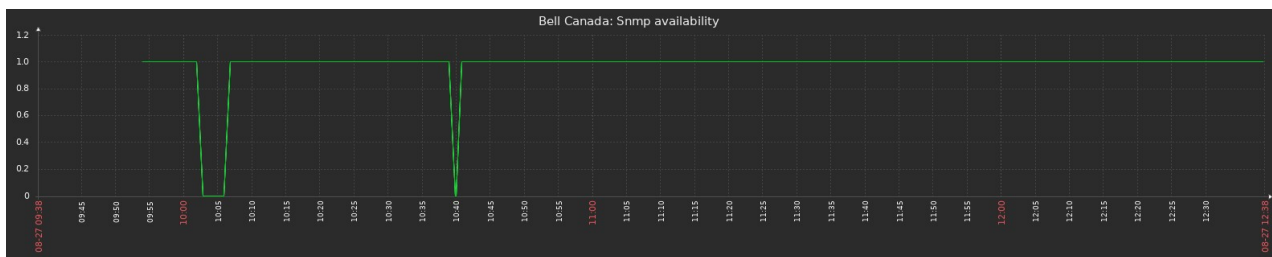


Immagine 14: grafico che mostra la disponibilità dell'agent snmp canadese nel tempo

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, nell'immagine 15, la situazione comparata come fatto prima. Come si nota, nello stesso periodo di misurazione, questo agente non cessa quasi mai di essere disponibile e fornisce un quantità di dati sufficiente a garantire un'attività di monitoraggio molto più efficiente di quella precedente, permettendo di effettuare analisi a grana più fine del funzionamento del sistema.



Immagine 15