SNMP Watch Dog

(Specifiche)

Progetto di Esame di Reti di Calcolatori

Corso di laurea in Ingegneria delle Telecomunicazioni

Realizzato da Scocco Gianfranco, matricola n. 21 03 50701

SNMP Watch Dog

Sistema di management e gestione delle emergenze SNMP.

Scenario.

La presenza di risorse a criticità elevata all'interno dei moderni sistemi informativi, siano esse dispositivi hardware (router, stampanti condivise, dispositivi di storage, ecc.) o risorse software (application servers, firewall, ecc.), rende necessario adottare adeguati strumenti di controllo per fare fronte ad eventuali emergenze (failures, attacchi esterni) che potrebbero compromettere la funzionalità delle risorse stesse.

A questo proposito si vuole realizzare un sistema distribuito che sia in grado di ricevere le segnalazioni di allarme da parte dei dispositivi e reagire agli eventi inviando contemporaneamente un messaggio e-mail e uno Short Message GSM all'amministratore del sistema.

Requisiti del sistema.

Il sistema dovrà essere in grado di:

- ricevere correttamente le segnalazioni da parte del dispositivo controllato
- gestire la segnalazione nel più breve tempo possibile e reagire di conseguenza
- far fronte ad eventuali guasti del sistema stesso (ad esempio down dell'elaboratore su cui gira il programma di management)

Dovremo dunque risolvere i problemi di:

- comunicazione sistema/managed resources
- fault tolerance del sistema
- comunicazione del sistema con entità esterne.

Comunicazione tra il sistema e le risorse.

La scelta del protocollo di comunicazione tra sistema e dispositivi deve necessariamente andare nella direzione di massima compatibilità, per dare modo al sistema di essere in grado di gestire il maggiore numero possibile di risorse in maniera trasparente.

Si decide allora di utilizzare il protocollo SNMP (Simple Network Management Protocol) che rappresenta allo stato attuale uno standard de facto per quanto riguarda i protocolli di management.

Il sistema sarà dunque in grado di ricevere e interpretare correttamente le trap SNMP inviate dalle risorse sulla porta UDP 162 come previsto dal protocollo SNMP stesso.

Capacità di fault tolerance del sistema.

Il sistema di management deve essere in grado di garantire il proprio servizio in maniera continuativa (*dependability*) anche in caso di guasto del sistema stesso. Per questo motivo si è scelto di ricorrere ad un sistema

distribuito con un certo grado di replicazione. Avremo cioè un certo numero di servitori fra loro coordinati, operanti su host diversi, ciascuno in grado di espletare la propria funzione in maniera indipendente dagli altri.

Ipotesi di guasto: non vengono fatte ipotesi di guasto a priori. Si vuole ottenere un sistema in grado di aumentare o diminuire su richiesta dell'amministratore il proprio grado di replicazione. In pratica l'amministratore del sistema deve essere in grado di decidere sulla base delle esigenze della propria rete quale grado di replicazione ottenere, bilanciando così il carico di rete introdotto dal sistema con le esigenze di robustezza del sistema stesso.

Comunicazione del sistema con entità esterne.

Il sistema comunica con l'amministratore attraverso il protocollo SMTP, inviando una mail direttamente alla casella postale dell'amministratore e inviando una mail al gateway SMS della Omnitel. Questo servizio provvederà a trasferire la mail al GSM dell'amministratore sotto forma di Short Message.

Modello del sistema.

Modello di comunicazione.

Il sistema si configura con uno schema di comunicazione con *cliente ed agenti multipli.*

Il cliente è rappresentato dalla risorsa da gestire, la quale invia le proprie richieste al sistema (v. Fig. 1).

Scendendo maggiormente nel dettaglio, l'entità gestita invierà una comunicazione SNMP a tutti gli agenti, i quali si coordineranno per servire la richiesta. Gli agenti si coordinano tra loro attraverso messaggi inviati tramite connessioni

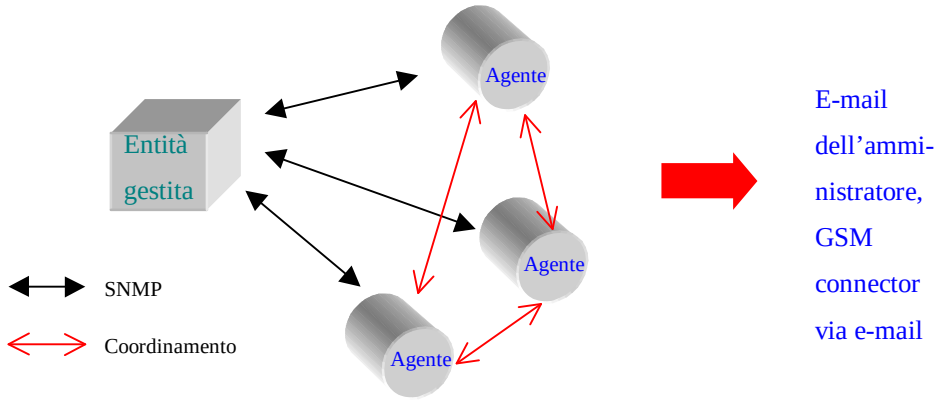

Figura 1

Nota: è evidente che questa soluzione non è per nulla trasparente dal punto di vista della risorsa gestita, la quale deve conoscere l'esistenza di tutti gli agenti. Inoltre molte risorse SNMP-capable non sono in realtà in grado di inviare le proprie traps a più di un agente. Questo problema potrebbe essere risolto introducendo un agente di interfaccia tra risorsa e sistema, il quale si occupa di replicare la richiesta ai vari agenti. In questo caso si introdurrebbe però un elemento di debolezza del sistema (se cade l'interfaccia cade tutto) e quindi la soluzione andrebbe ulteriormente studiata (anche a livello hardware) per aggirare il problema. In questa implementazione questo aspetto viene trascurato e si accetta la non trasparenza del sistema.

Modello di replicazione.

L'azione da intraprendere in caso di intervento è ben definita e unica. Il sistema deve inviare un messaggio direttamente alla casella postale dell'amministratore, e un messaggio al gateway GSM. Questo significa che è sufficiente che uno solo degli agenti si occupi di servire la richiesta, purchè qualcuno se ne occupi (si adotta cioè una semantica di tipo *exactly once*). Possiamo pensare allora di utilizzare un modello *passivo* di replicazione, cioè un modello *master/slave*. Gli agenti sono organizzati in un sistema con priorità decrescente assegnato dall'amministratore. (Introduciamo qui l'ipotesi semplificativa di priorità assegnate staticamente). In ogni istante un solo agente è master (tipicamente quello con priorità 0) e si occupa di gestire le richieste (trattandosi di un sistema di controllo per eventi eccezionali, è ragionevole pensare che il master non venga mai sovraccaricato). Gli slave controllano il funzionamento del master inviando ad intervalli regolari (ad esempio 30 secondi, ma è un parametro che può essere reso configurabile) delle richieste, a cui il master deve rispondere. In caso di mancata risposta da parte del master lo slave attivo a più alta priorità deve prendere il suo posto comunicandolo agli altri. Per fare questo si deve avviare un meccanismo di elezione tra gli agenti del sistema (problema di sincronizzazione). L'algoritmo di elezione utilizzato è l'algoritmo *bully*.

Una situazione da considerare è la possibilità che il master non riceva nessuna richiesta da parte degli slave. Questo avviene se tutti gli slave sono down oppure il master è isolato dagli slave. In questo caso il master non è in grado di accertare quale dei due eventi si sia verificato. Si fa allora la seguente ipotesi: il master continua il proprio lavoro, notificando la situazione all'amministratore, accettando in questo caso l'adozione di una semantica di tipo *at least once*, accettando cioè la possibilità di ricevere messaggi di errore duplicati.

La reintegrazione di un agente caduto avviene attraverso una notifica a tutti gli altri agenti. Questo deve forzare una rielezione del master.

Protocollo di comunicazione tra gli agenti

Gli agenti comunicano tra loro attraverso il protocollo TCP.

Ciascun agente ascolta le connessioni in arrivo attraverso la porta TCP 2055; su questa porta arrivano i messaggi dagli altri pari del sistema. Un agente che deve comunicare utilizza la prima porta disponibile, assegnata automaticamente dal supporto di rete.

Formato dei messaggi.

I messaggi scambiati dagli agenti sono nel formato:

x	y	z	n

Dove *xyz* indica il messaggio ed *n* è un byte che indica l'agente che ha inviato il messaggio (identificato dal grado di priorità assegnato all'agente stesso).

MIA	*Master is alive*	Inviato dallo slave al master per verificare che sia in vita
MAC	*Master acknowledge*	Inviato dal master agli slave che fanno richiesta MIA
FEL	*Force election*	Inviato dallo slave che non riceve il MAC oppure dall'agente appena entrato nel sistema, in base all'algoritmo *bully*.
EAC	*Election acknowledge*	Inviato dall'agente che ha ricevuto una richiesta di elezione da parte di un altro agente a priorità inferiore
MHA	*Master has*	Inviato dal master a tutti gli slave per indicare che ha gestito la

	answered	richiesta della risorsa
IAM	*I am Master*	Quando, dopo l'avvio di un elezione uno slave non riceve nessuna risposta da parte degli agenti più prioritari, si autodefinisce master e lo dichiara ai suoi sottoposti

Gestione della richiesta

La richiesta, nel caso in esame, altro non è che l'invio di una trap SNMP a tutti gli agenti. Ciascun agente gestisce una *tabella delle richieste*, che viene aggiornata:

- all'arrivo della richiesta da parte della risorsa in osservazione
- dopo il servizio della richiesta da parte del master

La richiesta viene gestita dal master, che al completamento dell'operazione invia un MHA agli slaves, per indicare che la richiesta stessa può essere eliminata dalla tabella di ciascuno slave.

Nel caso in cui il master cada prima di poter servire la richiesta, lo slave che ne prende il posto, non avendo ancora ricevuto l'MHA da parte del master, è in grado di operare al suo posto.