Monitoraggio dei servizi di una intranet

Dai numerosi sondaggi e ricerche che compaiono su internet si desume che si sta andando sempre più verso l'integrazione di servizi e sistemi ogni giorno più complessi. Anche le piccole aziende si stanno dotando di server aziendali dove vengono installate applicazioni e servizi per i clienti e i propri dipendenti. Spesso però si pensa solo all'implementazione e non al controllo degli stessi server che fanno il core bussiness dell'azienda. Le capacità tecniche per fare le integrazioni ci sono ma quello che manca a mio avviso è la cultura dirigenziale per poter proporre o pensare di implementare oltre ai servizi anche un buon monitoraggio degli stessi. Un altro problema che riscontro è la paura da parte dei commerciali delle diverse aziende d'informatica, con cui sono venuto a contatto, di proporre o vendere soluzioni basate su prodotti OpenSource perchè non c'è dietro una società o struttura tecnica di supporto al prodotto. Le aziende si rivolgono alle società che vendono software senza pensare che non esistono solo dei software a pagamento che si occupano di fare monitoraggio dei servizi, ma ne esistono di ottimi anche Open-Source. In questa trattazione parleremo di un monitoraggio attivo/passivo e vedremo come implementarlo usando Nagios (http://www.nagios.org), un programma OpenSource per monitorare servizi e server in una realtà distribuita.

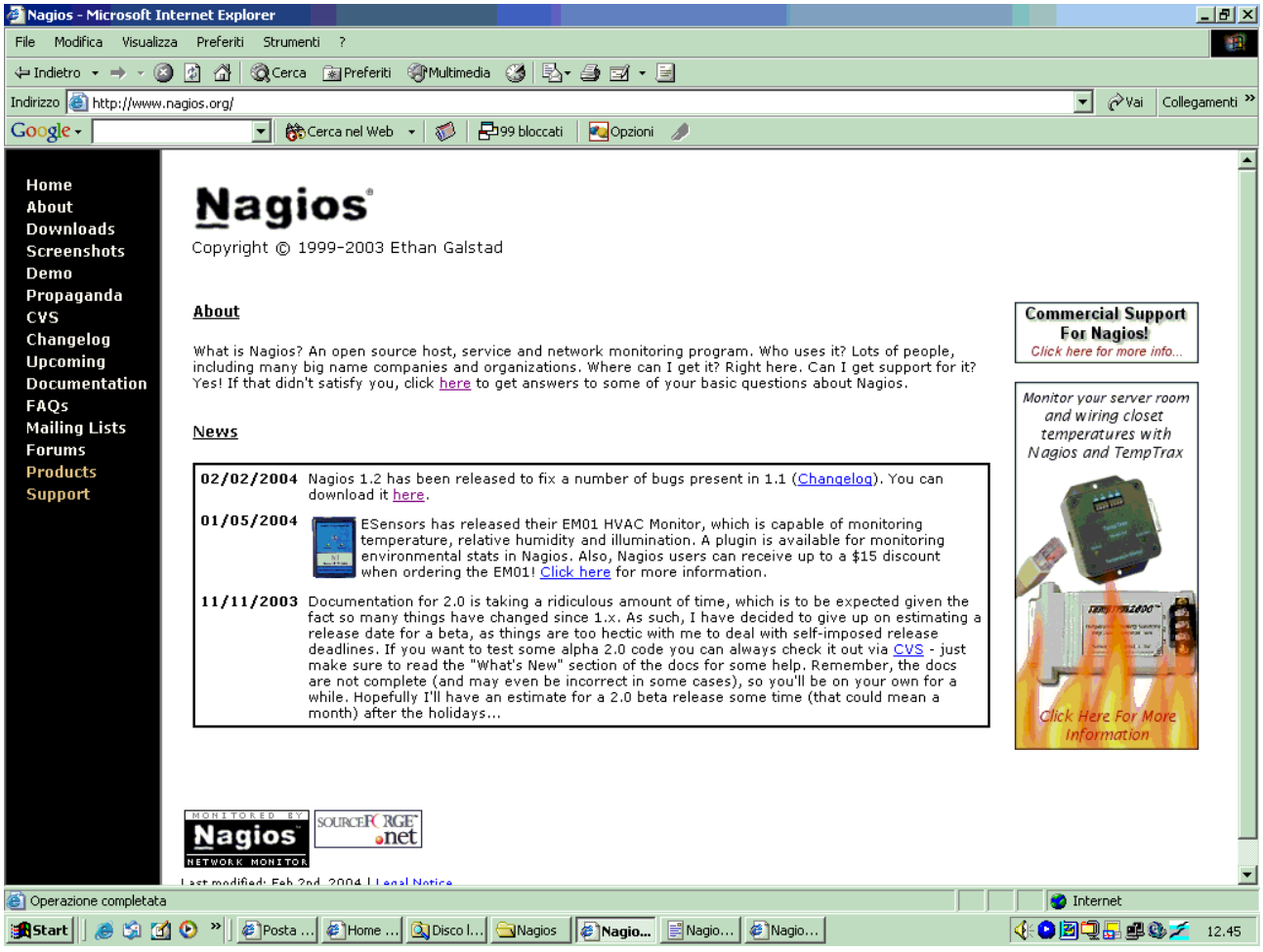

Fig. 1 Sito Ufficiale di nagios

Che cosa è Nagios?

Nagios® è una applicazione per monitorare sistemi e reti, il programma controlla host e servizi che sono stati specificati nel file di configurazione e manda un alert quando questi non sono raggiungibili oppure non rispondono. Descritto in questo modo potrebbe sembrare un programa banale, ma non lo è, se decidete di continuare con la lettura vi accorgerete di quante cose si possono fare con Nagios e di come le fa bene, purtroppo lo spazio è tiranno e non avrò la possibbilità di descrivere bene tutto il prodotto.

Nagios è stato progettato per lavorare con il sistema Operativo Linux, ma funziona bene anche con altri sistemi operativi like unix. Tra i numerosi servizi che possono essere controllati da Nagios® ci sono:

- Monitoring di servizi di network (SMTP, POP3, HTTP, NNTP, etc.)
- Monitoring di risorse dei server (carico della CPU, uso dei dischi, esistenza di un processo, etc.)
- Monitoring di raggiungibilità(PING)

La semplicità dei plugin, inoltre, permette di sviluppare facilmente dei nuovi ceck per i propri servizi. Tutti i controlli, anche quelli implementati ex novo come per quelli di default, possono essere effettuati in parallelo. Una delle caratteristiche peculiari di Nagios® è la possibbilità di definire la "network host hierarchy" usando una parentela tra gli host, "parent". In questo modo si disegna la rete e si può fare una diagnosi veloce in caso di problemi distinguendo tra hosts che sono down e quelli che sono irraggiungibili. Le notifiche, quando un host ha un problema oppure e stato risolto, possono avvenire in diversi modi: via email, via pager, o qualsiasi altro metodo definito dall'utente. E' prevista inoltre la possibilità di far eseguire degli script di risposta all'evento “down” come all'evento “up”. La possibbilità di far generare delle risposte automatiche al programma al succedersi di certi eventi rende il sistema oltre che di monitoraggio un sistema di risposta proattiva limitando il disservizio verso l'utente finale.

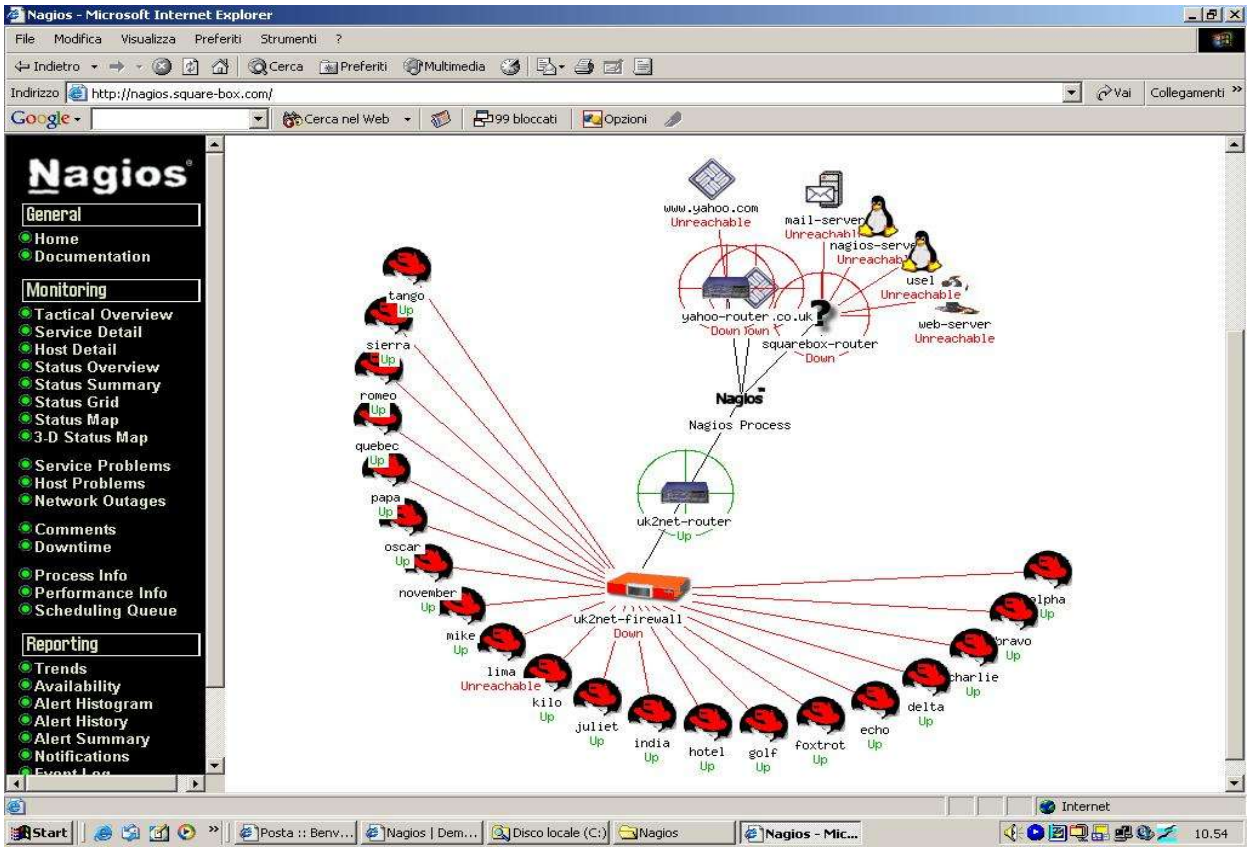

Fig. 2 Mappa di Monitoraggio

Requirements

L'unica cosa che serve per fa girare Nagios è una macchina che abbia come sistema operativo Linux (o una variante UNIX) e un compilatore C. La configurazoione del protocollo TCP/IP è necessaria per poter cotrollare i servizi di rete e i server remoti. Non è necessario usare le CGI che fanno parte del pacchetto Nagios, ma se si vogliono implementare bisogna configurare il web server per l'esecuzione delle CGI. Noi in questa trattazione prenderemo in considerazione il web server Apache. Un altro pacchetto non necessario ma utile per la visualizzazione grafica è la “Thomas Boutell's” libreria, la **gd** version 1.6.3 o superiore. Questa libreria, utilizzata soprattutto insieme ad Apache, serve per la creazione dinamica di immaggini in formato PNG e JPEG, Nagios la usa per

creare le mappe ed i grafici di raggiungibilità dei server.

Installazione

A differenza dei programmi a cui siamo abituati normalmente nel mondo OpenSource compilare e installare Nagios non basta per poi vederlo al lavoro eseguendolo. Esistono una serie di configurazioni che devono essere effettuate prima di avere una console di monitoraggio funzionante e funzionale.
Partiremo da un server Linux con Sistema operativo RedHat 9.0 e assumeremo che Nagios verrà installato nella directory /usr/local/nagios e che sia configurato Apache per usare le CGI, l'installazione che faremo si aspetterà che le CGI di nagios siano accessibili all'url htt://localhost/nagios/cgi-bin/. Se così non fosse si può usare l'opzione --*with-cgiurl* con lo script configure per modificare il path delle CGI.
La prima cosa da fare e scaricare il programma dal sito ufficiale insieme ai plugin, poi seguendo la documentazione si può passare all'installazione ed alla configurazione dei servizi da monitorare.
Vediamolo passo passo:
Una volta scaricato il pacchetto va scompattato in una directory temporanea con il consueto comando
tar cvfz nagios.1.x.tgz
entrare nella directory con il comando cd nagios.1.x/ e leggere il README e INSTALL. Prima di proseguire con l'installazione creiamo l'utente con cui faremo girare il programma con i comandi che seguono:
adduser nagios
poi eseguiamo lo script di configurazione con i parametri necessari al nostro ambiente di lavoro:
../configure --prefix=PREFIX --with-cgiurl=CGIURL --with-htmurl=HTMURL \
--with-nagios-user=SOMEUSER --with-nagios-grp=SOMEGROUP

a) Cambiare PREFIX con la directory dove dovrà essere installato Nagios, di Default viene usata la directory '/usr/local/nagios'

b) Cambiare CGIURL con l'URL che deve essere usata per raggiungere le CGI. Non mettere lo slash finale. Il default è '/nagios/cgi-bin'

c) Cambiare HTMURL con l'URL che deve essere usata per accedere alle pagine di documentazione html ed alla pagina principale di Nagios. Il default è '/nagios'

d) Cambiare SOMEUSER con il nome dell'utente, esistente sul proprio sistema, da essegnare come proprietario dei file e delle directory di Nagios. Il default è 'nagios'

e) Cambiare SOMEGROUP con il nome del gruppo, esistente sul proprio sistema, da associare a tutti i file come proprietario di essi. Il default è 'nagios'
ora compiliamo e installiamo il programma:
make all
make install
make install-config

per ultimo, se la compilazione è andata a buon fine, installiamo lo script di inizializzazione che va a finire nella directory /etc/init.d:
make install-init
lo script va poi editato per effettuare le modifiche relative al nostro ambiente di lavoro, se abbiamo lasciato tutte le configurazioni standard queste ultime non servono, va solo personalizzata la parte relativa la nostro Sistema Operativo come la variabile PATH ecc.
Finita l'installazione vediamo che cosa abbiamo nelle sotto directory del programma che si trova

nella directory /usr/local/nagios:

bin/ Nagios programma principale
etc/ Directory dove troviamo i file di configurazione installati con il comando *make install-config*
sbin/ CGI usate da Nagios
share/ file HTML (per l'interfaccia web e la documentazione ufficiale)
var/ directory vuota per i log file

Installazione dei Plugins
I plugins che si possono usare con Nagios sono tanti, questi possono essere scaricati dal sito ufficiale che è http://nagiosplug.sourceforge.net Dopo aver fatto il download e aver scompattato il file bisogna entrare nella directory e lanciare il comando configure, seguito dal comando di compilazione Make.
./configure
make
make install

Settaggio di apache

Dopo aver installato il programma anche prima di aver configurato i server da monitorare, provvederemo alla configurazione di apache per poter accedere via browser alla console di Nagios ed a tutta la documentazione. Bisogna aggiungere un alias e aggiungere la directory degli script cgi. La configurazione per nagios si può includere in un file che verrà caricato dal file principale di Apache con la direttiva Include.
La modifica da apportare al file di configurazione di Apache dovrebbe assomigliare a quella riportata sotto:

```
ScriptAlias /nagios/cgi-bin/ /usr/local/nagios/sbin/
<Directory "/usr/local/nagios/sbin/">
   AllowOverride AuthConfig
   Options ExecCGI
   Order allow,deny
   Allow from all
</Directory>
Alias /nagios/ /usr/local/nagios/share/
<Directory "/usr/local/nagios/share">
   Options None
   AllowOverride AuthConfig
   Order allow,deny
   Allow from all
</Directory>
```

La parte di ScriptAlias deve precedere la parte Alias altrimenti Apache fa il parsing in maniera diversa e non trova le CGI.

Dopo aver modificato il file di configurazione di Apache per vedere gli effetti della modifca bisogna riavviare il servizio web con il consueto comando:

/etc/init.d/httpd restart

che è uguale al comando :

service httpd restart

Metodi per lanciare Nagios

Nagios può essere lanciato in diversi modi, i metodi classici sono quattro:

1. Manualmente, come processo in foreground (di solito per i test iniziali)

/usr/local/nagios/bin/nagios <main_config_file>

2. Manualmente, come processo in background.

/usr/local/nagios/bin/nagios <main_config_file> &

3. Manualmente, come processo demone

/usr/local/nagios/bin/nagios -d <main_config_file

4. Automaticamente al boot.

Se abbiamo lanciato dopo l'installazione del programma il comando

'**make install-init**

allora abbiamo installato anche lo script per l'avvio automatico al boot.

A questo punto se il nostro processo è in esecuzione puntando il browser all'indirizzo http://localhost/nagios si può accedere all'interfaccia web principale di Nagios che oltre alla documentazione presente nella directory /usr/local/nagios/share, che è anch'essa consultabile via web, permette di avere un quadro completo della rete monitorata.

Una precauzione da prendere se si usa Nagios per monitorare servizi direttamente su Internet è l'accesso alle pagine di visualizzazione di Nagios tramite password, questo prevede di configurare apache per far accedere gli utenti tramite login e password. Come abbiamo accennato sopra bisogna ora pensare alle altre configurazioni e definire i server ed i servizi da tenere sotto controllo.

Configurazione e disegno della mappa di rete

La prima cosa da fare e avere un elenco aggiornato dei server e dei servizi su ogni singolo server, questo elenco ci servirà per costruire il nostro file di configurazione da dare in pasto al programma che farà i controlli.
Il file principale per configurare nagios è:
/usr/local/nagios/etc/nagios.cfg
il file è commentato ed autoesplicativo, inoltre all'interno si trova l'elenco degli altri file di configurazione che sono:
/usr/local/nagios/etc/hosts.cfg
/usr/local/nagios/etc/checkcommands.cfg
/usr/local/nagios/etc/contacts.cfg
/usr/local/nagios/etc/contactgroups.cfg
/usr/local/nagios/etc/hostgroups.cfg
/usr/local/nagios/etc/services.cfg
/usr/local/nagios/etc/timeperiods.cfg
/usr/local/nagios/etc/escalations.cfg
/usr/local/nagios/etc/misccommands.cfg

ogni file è commentato e seguendo gli esempi si possono modificare per raggiungere il nostro scopo.

Questo ci permette di rendere operativo il programma velocemente. Sul sito http://www.nagios.org c'è un link al server di demo preparato da Tom Welsh della squareBOX Technologies dove si possono trovare tutti i file di esempio utilizzati per la demo on-line, il sito è http://demo.square-

box.com

Verifica del file di configurazione
Dopo aver finito la parte di configurazione bisogna provare e testare se tutto funziona, si può lanciare nagios con il flag -v per vedere se i file di configurazione stanno a a posto:

/usr/local/nagios/bin/nagios -v <config_file>

config_file è il file dove abbiamo fatto le configurazioni, nagios verifica se è tutto ok senza lanciare il monitoraggio.

- Verifica che tutti i contatti siano membri di almeno un contact group.
- Verifica che tutti i contatti specificati in ogni contact group siano validi.
- Verifica che tutti gli hosts siano membri di almeno un host group.
- Verifica che tutti gli hosts specificati in ogni host group siano validi.
- Verifica che tutti gli hosts abbiano almeno un servizio associato da monitorare.
- Verifica che tutti i comandi usati per controllare gli host ed i servizi siano validi.
- Verifica che tutti i comandi usati in service and host event handlers siano validi.
- Verifica che tutti i comandi usati in contact service and host notifications siano validi.
- Verifica che tutti i periodi temporali specificati per services, hosts, e contact siano validi.
- Verifica che tutti i periodi temporali specificati per services siano validi.

Se i file di configurazione sono giusti allora si può proseguire con il nostro monitoraggio e vedere come si comporta Nagios, se invece ci viene segnalato una errata configurazione si può modificare il file e riprovare.

Uso di Nagios e Report
Come vediamo nella figura 3, dopo aver completato la nostra configurazione e settaggio della console degli eventi, si ha a disposizine uno strumento di prevenzione e di monitoraggio che aiuta il normale lavoro del sistemista. Inoltre se diamo un'occhiata nella parte sinistra del browser troviamo oltre al link alle diverse pagine di monitoraggio attivo i link ai report. Un tipo di report che spesso serve nel mondo del lavoro per giustificare verso il cliente il proprio operato sono le statistiche di raggiugibilità di un sito, nella figura 4 vediamo una statistica generata sul server della demo on-line:

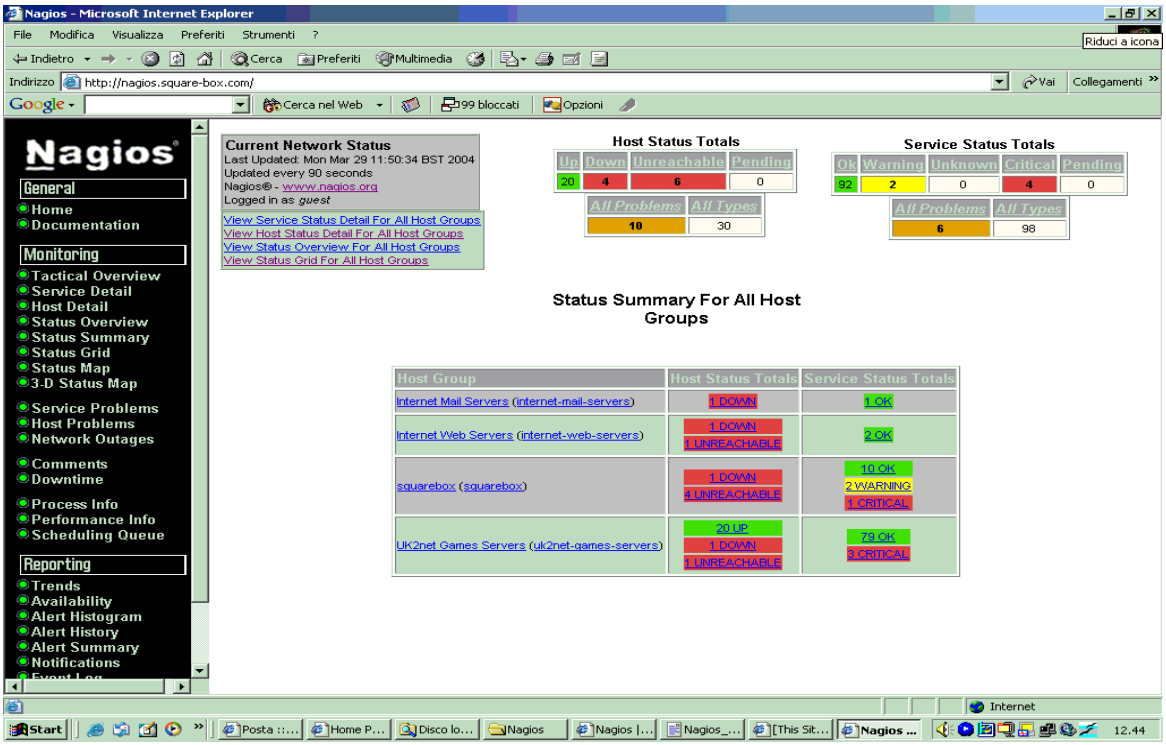

Fig. 3 Sommario dello stato della rete e dei servizi

Poichè Nagios colleziona gli eventi e li registra in un file questi si possono aggregare per fornire statistiche e grafici in tempo reale di quello che è successo nella nostra rete al cliente o al responsabile del servizio. Nella figura vediamo un classico report per host con i tempi di indisponibilità dei servizi di questi. Se questo non serve per avere soto controllo il lavoro da fare può servire per cercare di capire se si può migliorare il tempo di risposta ai problemi oppure se si può intervenire in altri modi e far si che il disservizio sia minimo nei confronti degli utilizzatori finali.

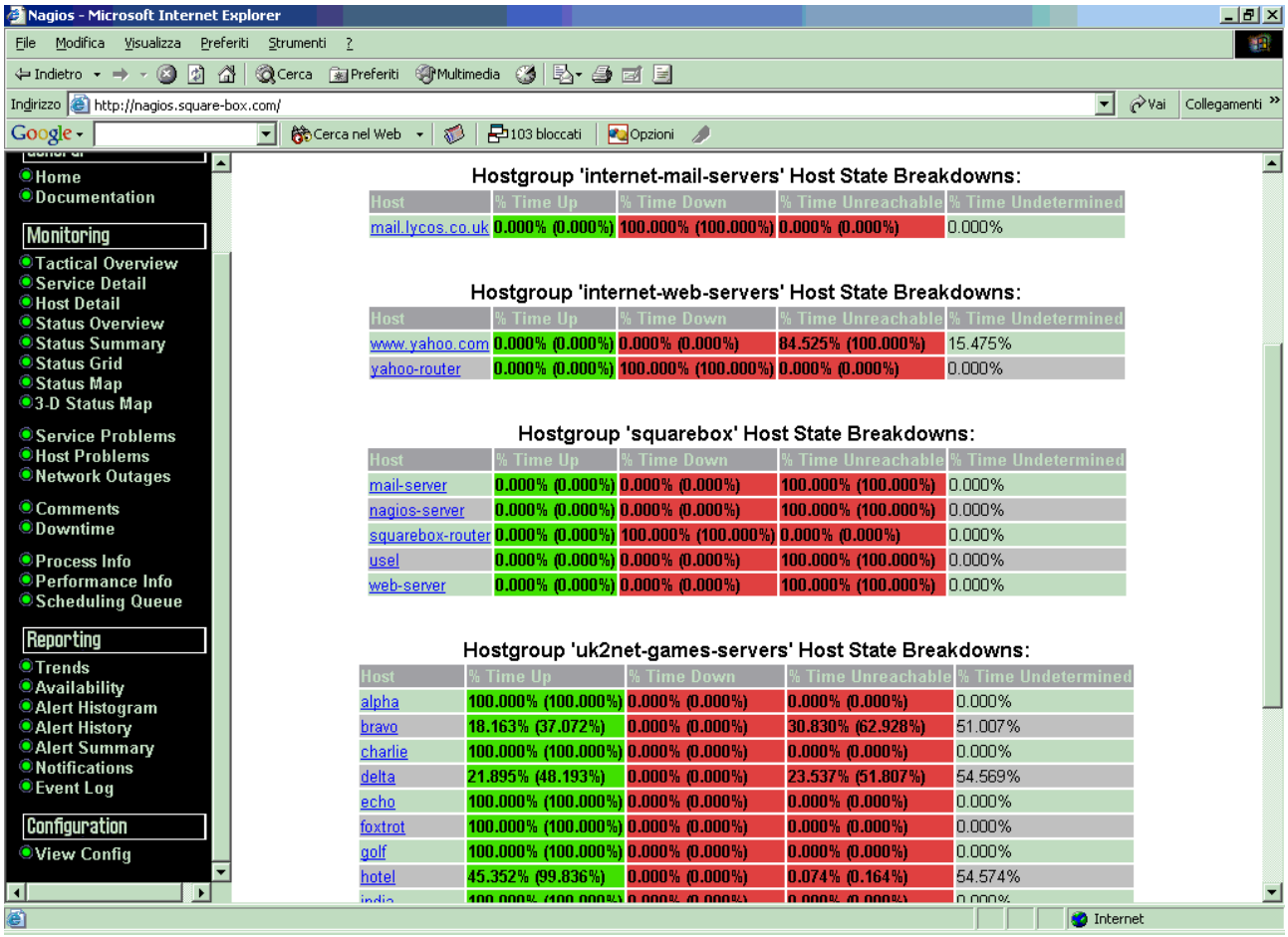

Fig. 4 Report di raggiungibilità dei server

Nonostante io usi Nagios da diversi anni, ho iniziato ad installarlo quando si chiamava “Netsaint”, e ritenendolo un ottimo prodotto, riporto sotto un elenco di software che fanno monitoring o si occupano di fornire un ottimo aiuto in un ambiente distribuito, a qualcuno può far comodo avere un elenco a portata di mano. Queste utility si possono trovare facilmente su Internet, per alcuni riporto direttamente il link, gli altri si possono reperiti utilizzando i motori di ricerca specializzati in software come http://freshmeat.net .

Utility di Monitoring tratte direttamente dalla documentazione di Nagios

Angel Network Monitor	http://www.paganini.net/angel/
Autostatus	http://www.angio.net/consult/autostatus/
HiWAyS	http://www.hiways.org/
MARS	http://www.altara.org/mars.html

Mon	http://www.kernel.org/software/mon/
Netup (French)	
NocMonitor	
NodeWatch	
Penemo	http://www.penemo.org/
PIKT	http://pikt.org/
RITW	
Scotty	
Spong	
Sysmon	

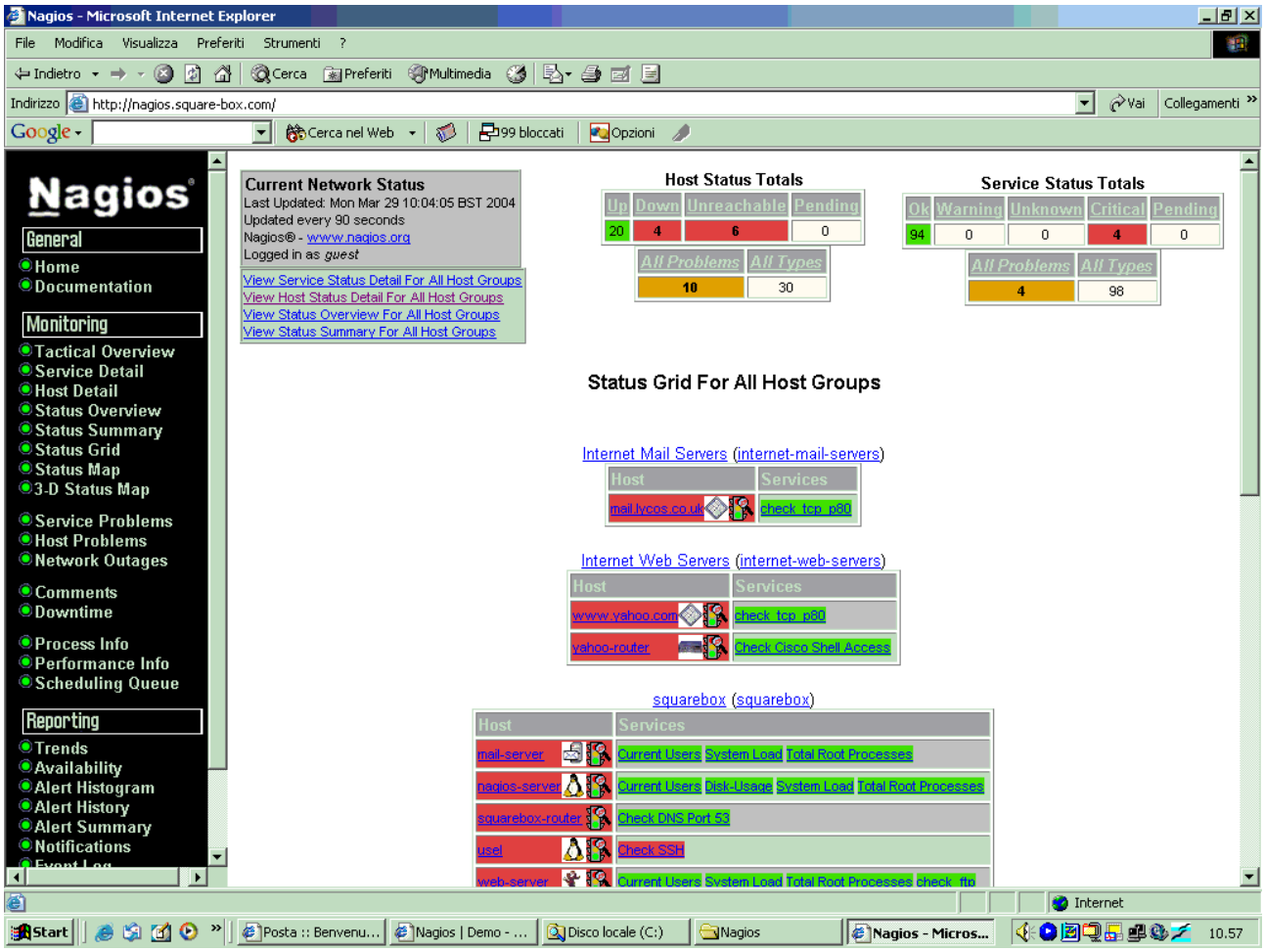

Figura 5 Stato suddiviso per gruppi di Host

Bibliografia e link

Sito principale di Nagios http://www.nagios.org
Download dei plugins http://nagiosplug.sourceforge.net
Demo sul sito della squareBOX Technologies http://demo.square-box.com