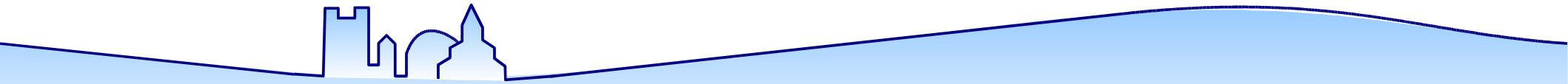
in collaborazione con

l'Università degli studi di Bergamo

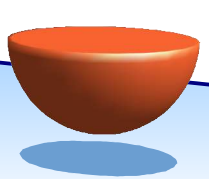
Facoltà d'Ingegneria

presenta:



Un server proxy open source: Squid

Marco Morosini



Un server proxy open source: Squid

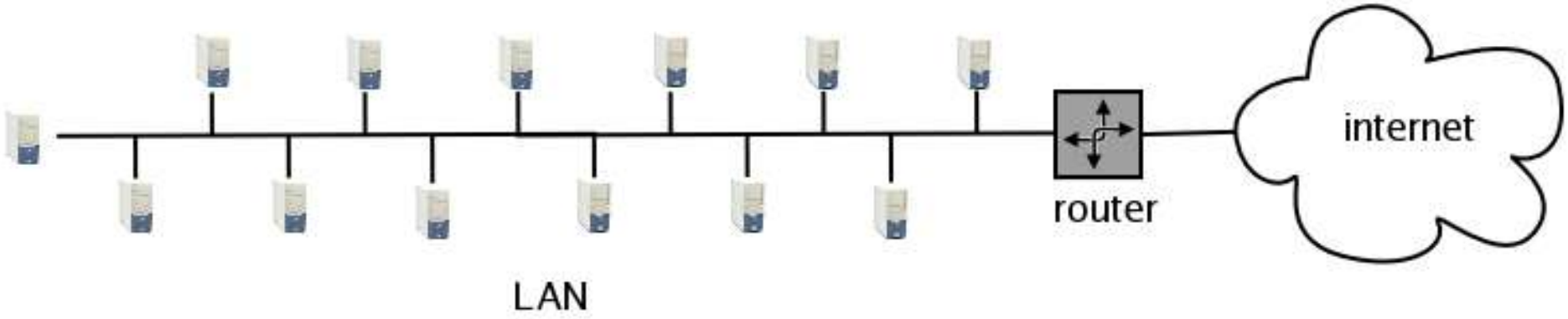
Una breve panoramica sul proxy più utilizzato

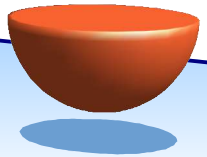
- Che cosa è un proxy web
- Richieste hardware di un proxy web
- File di configurazione
- File di log: access.log
- File di log: cache.log
- File di log: store.log
- Moduli di autenticazione degli utenti
- Programmi per l'analisi dei file di log
- Conclusione – Link utili

Un server proxy open source: Squid

Che cosa è un proxy web

situazione della rete con router

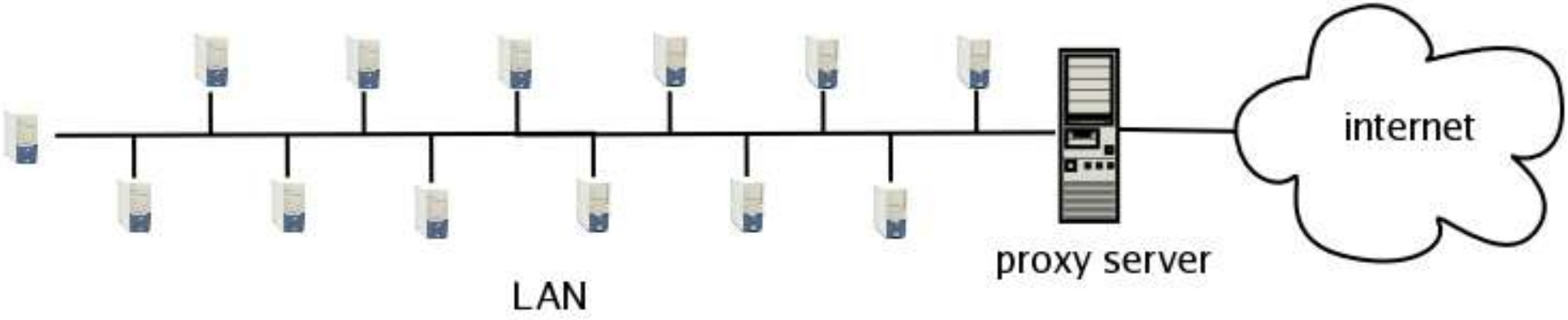


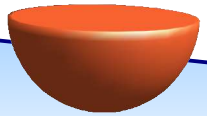


Un server proxy open source: Squid

Che cosa è un proxy web

introduzione di un proxy





Un server proxy open source: Squid

Che cosa è un proxy web

Principali vantaggi

- Risparmio di banda
- Controllo della navigazione in internet
- Amministrazione centralizzata degli utenti

Principali svantaggi

- E' necessario disporre di almeno un server linux
- L'utenza potrebbe sentirsi controllata (privacy)
- Gestisce soltanto il traffico http e ftp

Un server proxy open source: Squid

Richieste hardware di un proxy web

Richieste hardware di un proxy web

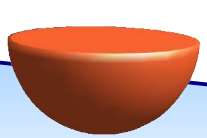
- veloce accesso al disco fisso
- memoria RAM
- CPU veloce

Un server proxy open source: Squid

Punti di forza di Squid

Punti di forza di Squid

- Tecnologia open source
- Progetto maturo e ampiamente diffuso
- Poco esigente in termini di risorse hardware
- Diversi metodi di autenticazione
- Personalizzabile con componenti esterni (log e blacklist)



Un server proxy open source: Squid

File di configurazione

/etc/squid/squid.conf

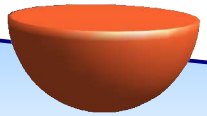
Voci più importanti del file di configurazione (3120 righe):

Sezione NETWORK: *http_port 3128* - porta utilizzata dal servizio

Sezione PEER CACHE SERVERS: *cache_peer* - nel caso di più proxy collegati tra loro

Sezione CACHE SIZE:

- *cache_mem* – RAM usata per gli oggetti in transito (in realtà ne verrà utilizzata 2 o 3 volte questo valore)
- *maximum_object_size* – soglia sopra alla quale i file NON vengono salvati in cache
- *minimum_object_size* - i file più piccoli di questo valore NON vengono salvati in cache
- *cache_replacement_policy* – quando devo considerare un file in cache non abbastanza aggiornato
- *memory_replacement_policy* -quando devo considerare un file in memoria non abbastanza aggiornato



Un server proxy open source: Squid

File di configurazione

/etc/squid/squid.conf

Sezione LOG FILE PATH NAMES AND CACHE DIRECTORIES:

· *cache_dir ufs /var/spool/squid 100 16 256*

posizione – dimensione in megabytes – cartelle di primo livello – cartelle di secondo livello

· *log_fqdn* – rende l'access.log molto più leggibile

ACCESS CONTROLS: http_access – allow/deny – parametro

Esempio: permettere un computer con un determinato mac address:

acl all src 0.0.0.0/0.0.0.0

acl miocomputer arp 00:08:c7:9f:34:41

http_access allow miocomputer

http_access deny all

Un server proxy open source: Squid

File di configurazione

/etc/squid/squid.conf
Access control list

Esempio: permettere la navigazione soltanto durante le ore lavorative:

acl miarete src 192.168.2.0/24

acl orario time M T W H F 9:00-17:00

http_access allow miarete orario

http_access deny all

Esempio un po' più complicato:

acl capo src 172.161.163.85

acl stipendi src 172.161.163.86

acl ragioneria src 172.161.163.86

acl mattino time 06:00-11:00

acl pranzo time 12:00-14:30

acl sera time 16:25-23:59

http_access allow capo mattino

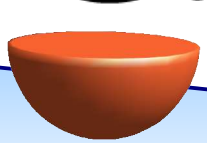
http_access allow stipendi mattino

http_access allow stipendi pranzo

http_access allow ragioneria pranzo

http_access allow ragioneria sera

http_access deny all



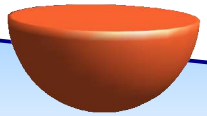
Un server proxy open source: Squid

File di configurazione

/etc/squid/squid.conf

TUNING THE CACHE:

- *reply_body_max_size* – posso limitare le dimensioni di una richiesta di PUT/POST
- *always_direct* – utile per i server locali o per particolari esigenze di pagine dinamiche (sessioni non gestite correttamente)
- *header_replace / anonymize_header* – posso cambiare l'intestazione delle richieste fatte dai miei clients
- *fake_user_agent* – per mascherare il browser utilizzato nella mia lan



Un server proxy open source: Squid

File di log: access.log

/var/log/squid/access.log

- File usato dagli analizzatori di traffico
- Può essere principalmente di due formati: originale e httpd
- Si consiglia il formato standard di Squid – ha più informazioni

Un server proxy open source: Squid

File di log: access.log

Access.log

```
1069951609.664   4723 192.168.0.2 TCP_MISS/200 509 GET http://bglug.linux.it/images/menublu-up-sx.png - DIRECT/62.177.1.107 image/png
1069951610.048   5241 192.168.0.2 TCP_MISS/200 5572 GET http://bglug.linux.it/bglug.css - DIRECT/62.177.1.107 text/css
1069951610.177   7411 192.168.0.2 TCP_MISS/200 14722 GET http://bglug.linux.it/ - DIRECT/62.177.1.107 text/html
1069951610.257    594 192.168.0.2 TCP_MISS/200 513 GET http://bglug.linux.it/images/menu-up-sx.png - DIRECT/62.177.1.107 image/png
1069951610.268   1100 192.168.0.2 TCP_MISS/200 302 POST http://bannerserver.gator.com/bannerserver/bannerserver.dll? - DIRECT/64.152.73.144 text/html
1069951610.318   5381 192.168.0.2 TCP_MISS/200 526 GET http://bglug.linux.it/images/menublu-up-dx.png - DIRECT/62.177.1.107 image/png
1069951610.378    329 192.168.0.2 TCP_MISS/200 526 GET http://bglug.linux.it/images/menu-up-dx.png - DIRECT/62.177.1.107 image/png
1069951610.537    279 192.168.0.2 TCP_MISS/200 508 GET http://bglug.linux.it/images/menu-down-dx.png - DIRECT/62.177.1.107 image/png
1069951610.618    299 192.168.0.2 TCP_MISS/200 505 GET http://bglug.linux.it/images/menublu-down-sx.png - DIRECT/62.177.1.107 image/png
1069951610.707    329 192.168.0.2 TCP_MISS/200 510 GET http://bglug.linux.it/images/menublu-down-dx.png - DIRECT/62.177.1.107 image/png
1069951610.818    630 192.168.0.2 TCP_MISS/200 519 GET http://bglug.linux.it/images/menu-down-sx.png - DIRECT/62.177.1.107 image/png
1069951610.874    336 192.168.0.2 TCP_MISS/200 513 GET http://bglug.linux.it/images/spazio.png - DIRECT/62.177.1.107 image/png
1069951611.737   1029 192.168.0.2 TCP_MISS/200 499 GET http://bglug.linux.it/images/linea_sfumata.png - DIRECT/62.177.1.107 image/png
1069951612.747   1874 192.168.0.2 TCP_MISS/200 1254 GET http://bglug.linux.it/images/icons/vcss.png - DIRECT/62.177.1.107 image/png
1069951614.627   4008 192.168.0.2 TCP_MISS/200 8049 GET http://bglug.linux.it/images/story-lug-96.png - DIRECT/62.177.1.107 image/png
1069951614.937   3199 192.168.0.2 TCP_MISS/200 1414 GET http://bglug.linux.it/images/icons/valid-html401.png - DIRECT/62.177.1.107 image/png
1069951617.347   4600 192.168.0.2 TCP_MISS/200 1861 GET http://bglug.linux.it/images/icons/pngnow.png - DIRECT/62.177.1.107 image/png
1069951618.867   4240 192.168.0.2 TCP_MISS/200 1200 GET http://bglug.linux.it/images/icons/php.png - DIRECT/62.177.1.107 image/png
1069951624.017   9080 192.168.0.2 TCP_MISS/200 4771 GET http://bglug.linux.it/images/lineafinale.png - DIRECT/62.177.1.107 image/png
1069951624.337  13520 192.168.0.2 TCP_MISS/200 31862 GET http://bglug.linux.it/images/newlogo.png - DIRECT/62.177.1.107 image/png
```

1) timestamp

2) tempo trascorso

3) indirizzo del client (se possibile risolto nel nome macchina)

4) TCP_HIT se è stato trovato in cache

TCP_MISS se è stato scaricato

TCP_REFRESH_HIT è stata fatta una richiesta ma il server di destinazione ha risposto “ 304 not modified” e quindi l'oggetto è stato recuperato dalla cache

TCP_REFRESH_MISS l'oggetto era in cache ma il server mi ha comunicato che era vecchio

5) dimensione

6) request method (ad es. GET)

7) URL richiesta

8) mostra il nome dell'utente, se il servizio ident è attivo

9) come e dove l'oggetto è stato scaricato

10) campo content-type della risposta http

Un server proxy open source: Squid

File di log: cache.log

/var/log/squid/cache.log

Contiene messaggi di errore utili per il debug

```
2003/11/27 17:06:54| Starting Squid Cache version 2.5.STABLE1-20030121 for i586-mandrake-linux-gnu...
2003/11/27 17:06:54| Process ID 13184
2003/11/27 17:06:54| With 1024 file descriptors available
2003/11/27 17:06:54| DNS Socket created at 0.0.0.0, port 32774, FD 5
2003/11/27 17:06:54| Adding nameserver 127.0.0.1 from /etc/resolv.conf
2003/11/27 17:06:54| Adding nameserver 192.168.0.2 from /etc/resolv.conf
2003/11/27 17:06:54| User-Agent logging is disabled.
2003/11/27 17:06:54| Unlinkd pipe opened on FD 10
2003/11/27 17:06:54| Swap maxSize 102400 KB, estimated 7876 objects
2003/11/27 17:06:54| Target number of buckets: 393
2003/11/27 17:06:54| Using 8192 Store buckets
2003/11/27 17:06:54| Max Mem  size: 8192 KB
2003/11/27 17:06:54| Max Swap size: 102400 KB
2003/11/27 17:06:54| Rebuilding storage in /var/spool/squid (DIRTY)
2003/11/27 17:06:54| Using Least Load store dir selection
2003/11/27 17:06:54| Set Current Directory to /var/spool/squid
2003/11/27 17:06:54| mimeLoadIconFile: /usr/share/icons/anthony-image.gif: (2) No such file or directory
```

Un server proxy open source: Squid

File di log: cache.log

Seconda metà del file cache.log

```
2003/11/27 17:06:54| mimeLoadIconFile: /usr/share/icons/anthony-unknown.gif: (2) No such file or directory
2003/11/27 17:06:54| Loaded Icons.
2003/11/27 17:06:55| Accepting HTTP connections at 0.0.0.0, port 3128, FD 11.
2003/11/27 17:06:55| Accepting ICP messages at 0.0.0.0, port 3130, FD 12.
2003/11/27 17:06:55| Accepting HTCP messages on port 4827, FD 13.
2003/11/27 17:06:55| Accepting SNMP messages on port 3401, FD 14.
2003/11/27 17:06:55| WCCP Disabled.
2003/11/27 17:06:55| Ready to serve requests.
2003/11/27 17:06:55| Done scanning /var/spool/squid swaplog (0 entries)
2003/11/27 17:06:55| Finished rebuilding storage from disk.
2003/11/27 17:06:55|         0 Entries scanned
2003/11/27 17:06:55|         0 Invalid entries.
2003/11/27 17:06:55|         0 With invalid flags.
2003/11/27 17:06:55|         0 Objects loaded.
2003/11/27 17:06:55|         0 Objects expired.
2003/11/27 17:06:55|         0 Objects cancelled.
2003/11/27 17:06:55|         0 Duplicate URLs purged.
2003/11/27 17:06:55|         0 Swapfile clashes avoided.
2003/11/27 17:06:55|   Took 0.4 seconds (   0.0 objects/sec).
2003/11/27 17:06:55| Beginning Validation Procedure
2003/11/27 17:06:55|   Completed Validation Procedure
2003/11/27 17:06:55|   Validated 0 Entries
2003/11/27 17:06:55|   store_swap_size = 0k
2003/11/27 17:06:55| storeLateRelease: released 0 objects
```

Un server proxy open source: Squid

File di log: store.log

/var/log/squid/store.log

- Debug file – object che sono o sono stati sul disco
- Mappa URL – filename sul disco (parametro cache_dir)
- Permette di fare statistiche sui nomi dei files

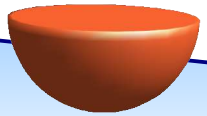
Un server proxy open source: Squid

File di log: store.log

/var/log/squid/store.log

```
1069951610.269 SWAPOUT 00 00000004 FED2136B0B76C7445D87983F65CF1383  200 1069951765 1068503408        -1 image/png 182/182 GET http://bglug.linux.it/images/menublu-up-dx.pr
1069951610.320 SWAPOUT 00 00000005 595AE8C9337BFDFCD8E5252BA07BB938  200 1069951766 1068503401        -1 image/png 182/182 GET http://bglug.linux.it/images/menu-up-dx.png
1069951610.396 SWAPOUT 00 00000006 A0D073B52F1C5350997EFD4AF2C14D6F  200 1069951766 1068503407        -1 image/png 164/164 GET http://bglug.linux.it/images/menu-down-dx.png
1069951610.540 SWAPOUT 00 00000007 4C4B5D6CA3D8CD05BFD6D9DB5176FFCF  200 1069951766 1068503406        -1 image/png 161/161 GET http://bglug.linux.it/images/menublu-down-sx.
1069951610.620 SWAPOUT 00 00000008 B3D73B103ED2BA26E76747EEE3022541  200 1069951766 1068503424        -1 image/png 166/166 GET http://bglug.linux.it/images/menublu-down-dx.
1069951610.708 SWAPOUT 00 00000009 DFCEFD6E806D899EEC020999B5DAE1C0  200 1069951766 1068503399        -1 image/png 175/175 GET http://bglug.linux.it/images/menu-down-sx.png
1069951610.822 SWAPOUT 00 0000000A A828D1347AE692DF11A58B45965FBCD5  200 1069951766 1068503427        -1 image/png 169/169 GET http://bglug.linux.it/images/spazio.png
1069951611.477 SWAPOUT 00 0000000B 7057A1CAAFD2A458126BC10565C74B9A  200 1069951766 1068503426        -1 image/png 155/155 GET http://bglug.linux.it/images/linea_sfumata.pr
1069951612.488 SWAPOUT 00 0000000C D384F02C610369E0AA4BDC569E6932DD  200 1069951767 1068503352        -1 image/png 909/909 GET http://bglug.linux.it/images/icons/vcss.png
1069951614.458 SWAPOUT 00 0000000E A122120D3FED3FA2202CE5FB251BDEDD  200 1069951766 1068503404        -1 image/png 7702/7702 GET http://bglug.linux.it/images/story-lug-96.p
1069951614.628 SWAPOUT 00 0000000F 81EC482C589454EDF0BCDA01BE150336  200 1069951767 1068503350        -1 image/png 1068/1068 GET http://bglug.linux.it/images/icons/valid-ht
```

1) timestamp
2) action (release, swapin, swapout)
3) numero dei file dell'oggetto
4) http reply status code
5) date (valore dell'header della risposta)
6) ultima modifica (valore dell'header della risposta)
7) expires (valore dell'header della risposta)
8) content type (valore dell'header della risposta)
9) content-lenght rispetto alla dimensione reale
10) request method (GET)
11) URL



Un server proxy open source: Squid

Metodi di autenticazione

Moduli di autenticazione degli utenti

- squid_ldap_auth e squid_ldap_group (Domain Controller Windows 2000)
- NTLM – come integrare il login e l'autenticazione dei clients con Internet Explorer
- mysql_auth per usare un database di utenti mysql

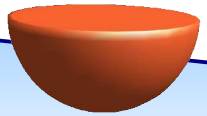
Un server proxy open source: Squid

Programmi per l'analisi dei file di log

Grep – Awk – Perl – Python

Calamaris – script perl con output in HTML

The Webalizer – scritto in linguaggio C – output in HTML



Un server proxy open source: Squid

Conclusione - Links

Documenti e manuali


www.squid-cache.org

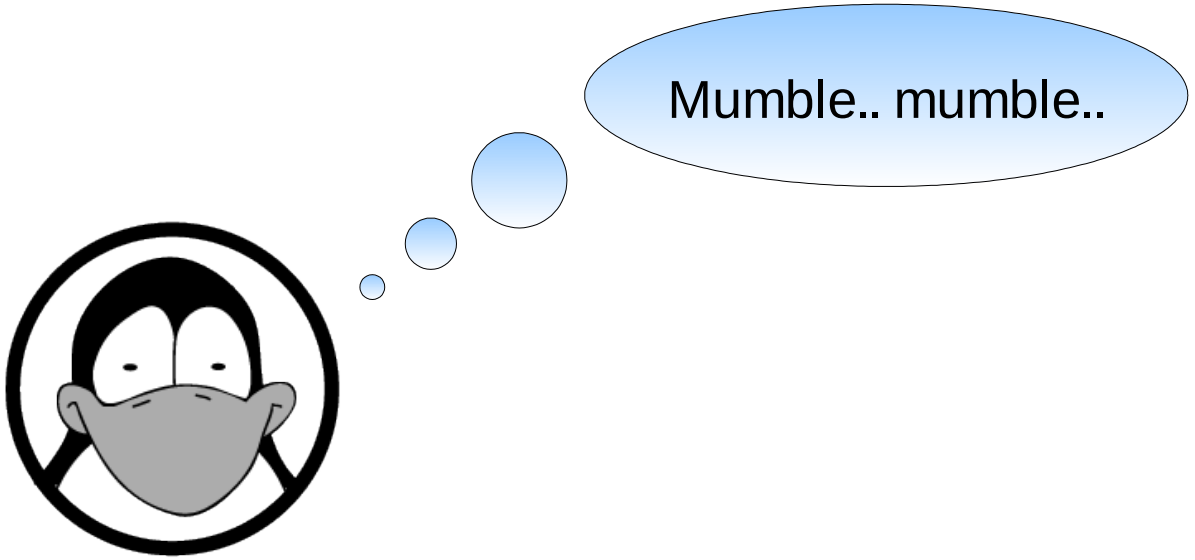

http://squid.visolve.com (manuale di configurazione)


http://squid-docs.sourceforge.net


http://www.marcomorosini.it

Domande ...

Domande ?



Risposte !

Un server proxy open source: Squid

Marco Morosini

Grazie per l'attenzione.