Domain Name System

Massimo Ianigro *

Maurizio Martinelli **

Daniele Vannozzi **

*** Area della Ricerca CNR - Bari**

**** Istituto Applicazioni Telematiche - Pisa**

Massimo.Ianigro@area.ba.cnr.it

Maurizio.Martinelli@iat.cnr.it

Daniele.Vannozzi@iat.cnr.it

DNS: caratteristiche principali

- database distribuito
- basato sul modello client/server
- tre componenti principali:
  - spazio dei nomi e informazioni associate (Resource Record - RR)
  - nameserver (application server che mantiene i dati)
  - resolver (client per l'interrogazione del nameserver)
- accesso veloce ai dati (database in memoria centrale e meccanismo di caching)

Lo spazio dei nomi

- lo spazio dei nomi è organizzato secondo il modello gerarchico:
  - il database del DNS ha una struttura logica “ad albero rovesciato”
  - ciascun nodo dell’albero rappresenta un *dominio*
  - ogni dominio può essere suddiviso in altri domini: *sottodomini*
  - ogni nodo ha una etichetta che lo identifica rispetto al padre

  La radice dell'albero è unica, e la sua etichetta è vuota. In certi casi si indica anche come “.”
- struttura dello spazio dei nomi:
  - domini generali (gTLD)
  - domini nazionali (ccTLD)
  - domini per la risoluzione inversa (arpa)

Gli attacchi al DNS

Gli attacchi più comuni sono di cinque tipi:

- Denial of service
- Buffer overrun
- Cache corruption (spoofing)
- Acquisizione di informazioni non autorizzate
- Modifica dei dati (dynamic update)

Attacchi: denial of service

Descrizione: Questo genere di attacchi mira ad impedire il funzionamento del name server (‘denial of service’) alterando i dati in suo possesso o mandando in ‘crash’ il processo stesso. Tipicamente vengono condotti inviando al server DNS delle query artefatte (‘malformed’) la cui elaborazione provoca, in versioni di Bind antecedenti alla 4.9.7 e 8.1.2, accessi errati ai dati in memoria o a volte il crash del processo named.

Soluzioni:aggiornare il Bind

Attacchi: buffer overrun

Descrizione: Questo genere di attacchi mira ad ottenere l'accesso al sistema con i privilegi del processo named (tipicamente root). In genere vengono utilizzate delle inverse-query errate, la cui elaborazione può portare a un buffer overrun e all'esecuzione di codice arbitrario.

Soluzioni:aggiornare il Bind alla 4.9.7 o a versioni non inferiori alla 8.1.2 e verificare che nel file di configurazione del named non compaia l'opzione "fake-iquery" (4.9.x) o "fake-iquery yes" (8.x)

Attacchi: cache corruption

Descrizione: utilizzando i meccanismi di caching del named, combinato con l'esecuzione di queries ricorsive, un name server può essere forzato a contattare dei name server non autoritativi per l'ottenimento delle informazioni. Inoltre alcune vecchie versioni di named e named-xfer (antecedenti alla 4.9) conservano in memoria i 'glue record' e utilizzano tali informazioni per i processi di risoluzione.

Soluzione: aggiornare il bind alla versione 4.9.x o 8.x e disabilitare la ricorsione (oppure restringere l'accesso al nameserver solo alle macchine 'di fiducia')

Attacchi: acquisizione di informazioni non autorizzate

Descrizione: utilizzando named-xfer (o altre utility come host, nslookup, etc) è possibile richiedere l'intero contenuto di una zona.

Soluzione: utilizzare le opzioni xfernets (4.9.x) o allow-transfer (8.x) per specificare quali indirizzi IP sono abilitati al trasferimento del contenuto di una intera zona. Ricordarsi di applicare tail restrizioni a tutti i name server autoritativi (primari e secondari)

Attacchi: modifica dei dati

Descrizione: in bind 8.x è stata introdotta la funzionalità del dynamic update (disabilitata per default). Essa consente di inserire o rimuovere delle informazioni da una zona in modo dinamico, utilizzando il tool nsupdate.

Soluzioni: verificare che nel file di configurazione non vi siano istruzioni di ‘allow-update’. Nella eventualità si decidesse di utilizzare tale funzionalità, è opportuno ricordare che nell’opzione allow-update è possibile specificare solo l’indirizzo IP della macchina autorizzata (e non username e/o password).

Alcune regole pratiche per la sicurezza del named

Alcune regole pratiche per migliorare il livello di sicurezza di un named:

- restringere lo zone-transfer solo ai nameserver secondari
- restringere la possibilità di effettuare update dinamici (nsupdate)
- disabilitare la ricorsione
- eseguire named senza i privilegi di root (named -u xxx)
- nel caso di utilizzo di un firewall per proteggere una rete, predisporre un nameserver esterno con le sole informazioni relative alle macchine visibili su Internet (es. www server, mail server, etc) e uno interno, utilizzabile solo dalle macchine locali, con le informazioni complete della zona.

Le piattaforme hardware e software

- hardware
  - disponibile su quasi tutte le attuali piattaforme (PC, Macintosh, workstation, mainframe)
- software
  - prodotti di pubblico dominio (BIND per Unix e WinNT/Win95, MIND/NonSequitur per MacOS)
  - prodotti commerciali (MacDNS, QuickDNS Pro, distribuzione di WinNT server 4.0)
- BIND (Berkeley Internet Name Domain)
  - è l'implementazione di nameserver più diffusa su Internet
  - sviluppata per Unix BSD, ne esistono *porting* per molti altri ambienti
  - spesso ne è inclusa una implementazione nel software di corredo di piattaforme Unix
  - vi sono attualmente due versioni:
    - la versione "storica" 4.x.y (l'ultima rilasciata è la 4.9.7)
    - la "nuova" versione 8.x.y (l'ultima rilasciata è la 8.2.5)

http://www.isc.org/bind.html

Le maggiori differenze tra le due versioni

File di configurazione

- named.boot (4.x.y)
  - formato ormai in uso da anni
  - consente solo alcune “personalizzazioni” generali
- named.conf (8.x.y)
  - nuovo formato (stile linguaggio c)
  - funziona con IPv6 (http://www.6bone.net)
  - consente una personalizzazione completa sia generale che zona per zona

- Esiste una procedura perl (*named-bootconf.pl*) per la conversione dal formato 4.x.y al formato 8.x.y

rimangono inalterati i file delle singole zone

Un esempio del file *named.boot*

```
; Boot file on nameserver.cnr.it
; dns-adm@nameserver.cnr.it 19990615
;
; directory where all the data files are stored
directory  /usr/local/domain
;
xfrnets   193.0.0.0
xfrnets   194.119.192.0
xfrnets   193.205.245.8&255.255.255.255
;
primary            0.0.127.in-addr.arpa                          named.local
primary            cnr.it                                        cnr/soa.cnr-it
primary            pi.cnr.it                                     cnr/pisa/soa.pi-cnr-
    it
primary            48.146.in-addr.arpa                           cnr/soa.pi-cnr-it-lan
secondary          iat.cnr.it          146.48.65.2 146.48.127.2  backup/iat-cnr-it
secondary          65.48.146.in-addr-arpa     146.48.65.2        backup/iat-lan
;
; Root Nameservers
cache              .                                             named.root
```

La funzionalità di logging

- Nella versione 4.x.y non è possibile avere una personalizzazione accurata dei file di log
  - logging di sistema (syslogd, syslog.conf, /var/adm/messages, /var/log/syslog)
  - customizzazione del file …/bind-4.x.y/conf/options.h

    #ifndef LOGFAC

    #define LOGFAC LOG_LOCAL0

    #endif
  - customizzazione del file /etc/syslog.conf

    local0.none **/dev/console**

    local0.none **/var/log/messages**

    local0.debug **/var/log/named.log**

    local0.alert **/var/log/named-lame.log**

Nuove funzionalità della versione 8.x.y

- meccanismo del notify
  - permette l'aggiornamento quasi in tempo reale tra nameserver primario e secondari
- meccanismo di logging flessibile e personalizzabile, senza uso obbligato del logging del sistema (syslog)
- controllo degli accessi personalizzabile per zona
- migliore ottimizzazione della memoria centrale
  - migliora notevolmente le prestazioni del servizio, specialmente per implementazioni con molte zone attive sulla stessa macchina
- numero max di zone incrementato a 4.294.967.295 (2^{32})
- supporto iniziale di DNSSEC
- supporto di WindowsNT
- update dinamico (NSUPDATE)
- $GENERATE

Installazione del BIND 8 in ambiente UNIX

- Sistemi supportati: AIX 4, A/UX 3.1.1, BSD/OS 2.1 - 3.x - 4.0, Digital ULTRIX 4.5, Digital UNIX 3.2C - 4.0, FreeBSD 2.x - 3.0, HP MPE, HP-UX 9.x - 10.20, IRIX 5.3 - 6.2 - 6.4, LynxOS, NetBSD 1.2 - 1.3, OpenBSD 2.1, QNX Red Hat Linux 4.x, 5.0, SCO UNIX 3.2v4.2, SCO OSE 5.0.4, UnixWare 2.0.x, 2.1.2, SunOS 4.1.4, SunOS 5.5 - 5.6, Windows NT
- Compilatore ANSI/ISO C oppure GCC (http://prep.ai.mit/edu)
- Personalizzare il Makefile.set relativo al proprio sistema (…./bind-8.2.2/src/port/XX/Makefile.set) dopo aver opportunamente salvato quello originale
  - DESTDIR, DESTLIB, DESTINC, DESTBIN, DESTSBIN, DESTEXEC, DESTRUN, DESTETC, CC, ecc.
  - applicare le eventuali patch
  - cancellare i file …./bind-8.x.y/src/.settings e …./bind-8.x.y/src/.systype (se esistenti)
  - make depend
  - make
  - make install
- Spazio necessario: circa 25MB

Il file *named.conf*

- il file *named.conf* è il file di configurazione principale per il funzionamento del processo nameserver nella versione 8.x.y
- principali direttive:
  - definisce la directory in cui si trovano gli altri file necessari al funzionamento del nameserver *(directory)*
  - definisce la raccolta dei dati statistici relativi al processo nameserver *(statistics-interval* - default 60 min.*)*
  - definisce l'ordine con cui il server sceglie un NS a cui rivolgersi per effettuare una interrogazione *(topology)*
  - definisce quali sono i nameserver che possono prelevare le zone per cui il nameserver è autoritativo *(allow-transfer)*
  - definisce quali macchine possono effettuare richieste "ordinarie" (ad es. su una particolare zona) e quali inserire nella blacklist (sia in entrata che in uscita) *(allow-query, blackhole)*
  - definisce il livello e la distribuzione dei "log" prodotti dal processo nameserver senza dover necessariamente fare uso del syslog del sistema *(logging/channel/category)*
  - definisce se una richiesta deve essere inoltrata ad un'altro NS *(forward/forwarders)*
  - definisce l'interfaccia locale della macchina su cui il processo nameserver è attivo
  - definisce i domini per i quali il nameserver è autoritativo *(master e slave)*
  - definisce i riferimenti ai root nameserver *(hint)*

  Attenzione alla sintassi ….è diversa dalla vecchia versione (/ */, //, # invece di ;)*

Il file named.conf: dichiarazioni generali

```
controls {
        unix "/usr/local/bind-8.2.2/run/ndc" perm 0600 owner 0
        group 0;
};
options {
        directory "/usr/local/dns/data";
        statistics-interval 5;
        allow-transfer {
            193.205.245/24;    // *.nic.it
            193.0.0/24;        // LAN di RIPE
            194.119.192.34;    // nameserver.cnr.it
        };
        datasize 12M;      // coresize 4M;
        transfer-format many-answers;
            /* migliora la performance - più RR in una singola risposta
        */
        transfers-in 4;
```

La funzionalità di *logging*

- La versione 8.x.y permette una personalizzazione completa e flessibile del logging
- dichiarazione ***logging*** (va messa come prima istruzione del named.conf)
- concetto di categoria per identificare e raggruppare i messaggi di log desiderati
  - insieme di categorie predefinite (*default*, *lame-servers*, *statistics*, *panic*, *notify*, *xfer-in*, *xfer-out*, *security*, *cname*, *load*, *update*, *ecc.*)
- definizione di un canale per personalizzare i log relativi a ciascuna delle categorie predefinite
  - è possibile associare ad ogni canale un livello di gravità, in modo da memorizzare quei messaggi con un livello di gravità >= a quello del canale
  - livelli di gravità previsti (in ordine decrescente):
    - ⇨ critical
    - ⇨ error
    - ⇨ warning
    - ⇨ notice
    - ⇨ info
    - ⇨ debug 1 ….debug 99

Il file named.conf: dichiarazioni di logging

```
logging {
        channel syslog_errors {
                syslog local0;
                severity info;
        };
channel statistics {
                file "/var/log/named/named-stat";
                print-time yes;
};
channel security {
                file "/var/log/named/security.log” size 10M versions 7;
                print-time yes;
                severity debug 3;
};
category statistics {
                statistics;
};
category cname {
                null
 };
```

Restrizione degli accessi

La restrizione degli accessi avviene mediante le Access Control Lists, che consentono di specificare un gruppo di indirizzi:

Esempio:

```
// indirizzi da 194.119.200.0 a 194.119.207.255
    acl cnr-bari {
          { 194.119.200.0/21 };
    };
// solo l'indirizzo 194.119.192.34
    acl singola_macchina {
          { 194.119.192.34/32 };
    };
```

Restrizione degli accessi 2

Le ACL possono essere applicate in vari contesti:

- allow-query — autorizzazione a effettuare query
- allow-transfer — autorizzazione a richiedere zone-transfer
- blackhole — indirizzi di ns o client da ignorare
- listen-on — interfacce e porte su cui ascoltare
- topology/sortlist — consentono di stabilire una preferenza nelle reti da contattare

Il file named.conf: la restrizione degli accessi

```
options {
    // consento zone-transfer solo alle macchine presenti sulla rete del
    // CNR di Bari 194.119.200.0->194.119.207.255 ed alla macchina
     // 193.205.245.8

    allow-transfer {
          cnr-bari;              //definita nell'acl precedente
          193.205.245.8;
    };
    // consento le query solo alle macchine
    // 194.119.0.0 -> 194.119.255.255
    allow-query {
          194.119/16;
    };
}
```

Il file named.conf: dichiarazione delle zone

```
zone "0.0.127.in-addr.arpa" in {
        type master;
        file ”named.local";
};
zone ”cnr.it" in {
        type master;
        file "cnr/soa.cnr-it";
};
zone "65.48.146.in-addr.arpa" in {
        type slave;
        file "backup/iat-cnr-it-lan";
        masters {146.48.65.3;
                  146.48.127.2;
                 };
};
zone "." in {
        type hint;
        file "named.root";
};
```

Named: analizzare il funzionamento

Il processo Named utilizza dei contatori che registrano il tipo di informazioni che vengono fornite in risposta alle varie queries.

Solo i contatori con valori maggiori di 0 vengono visualizzati.

In fase di logging queste informazioni vengono fornite suddivise in tre categorie:

- NSTAT (RR principali: CNAME, A, PTR, HINFO, AAAA, SOA, MX, ANY...)
- XSTAT (informazioni estese: Rerr, Serr, SNXD)
- USAGE (CPU utilizzata dai processi named)

Quali dati abbiamo a disposizione

Il formato nel quale named registra i dati nei file di log è:

`TIPO timestamp1 timestamp2 RR=val RR=val ..`

dove `timestamp1` e `timestamp2` indicano l'ora in cui è stato effettuato il log delle informazioni e l'ora di avvio del processo named

Esempio:

21-Jun-1999 15:58:43.176 NSTATS 929973523 929973295 A=1234 NS=1 CNAME=4 SOA=32 PTR=415 MX=84 AAAA=2 AXFR=1 ANY=100

Quali dati abbiamo a disposizione 2

Informazioni di tipo XSTAT

RR	risposte ricevute dal named
RQ	query ricevute
RNXD	messaggi di tipo ‘no such domain’ ricevuti da altri ns
RFwdR	risposta ricevuta e inviata all’applicazione richiedente (libresolv)
RDupR	risposte duplicate
Rfail	risposta SERVFAIL ricevuta - errore del ns remoto
RFErr	risposta FORMERR ricevuta dal ns remoto- errore nel formato della query inviata
Rerr	errore generico
RAXFR	zone transfer iniziati
Rlame	lame delegations ricevute
Ropts	pacchetti IP ricevuti con il campo ‘Options’ attivo
RIQ	query inverse (utilizzate dalle vecchie versioni di nslookup)
RFwdQ	query ricevute che necessitano di ulteriori elaborazioni prima di essere esaudite (forward)

Quali dati abbiamo a disposizione 3

Informazioni di tipo XSTAT (cont.)

RDupQ	query duplicata ricevuta
RTCP	query di tipo TCP ricevute
SFwdQ	query forwarded a un ns server
SDupQ	query duplicate inviate a un ns
Serr	errori nella system call sendto()
SFwdR	risposte ricevute da un ns e forwarded a un altro ns
Sfail	messaggi di tipo SERVFAIL inviati
SFErr	messaggi di tipo FORMERR inviati
SNaAns	risposte di tipo ‘not autoritative answer’
SNXD	risposte di tipo ‘no such domain’ inviate
SSysQ	system queries inviate dal ns (es. query ai root server)
Sans	totale delle risposte inviate

Abilitare le statistiche

Le statistiche si abilitano mediante i costrutti channel e logging nel named.conf.

Esempio:

```
logging {
    channel named-debug {
      file “/var/tmp/named.debug” versions 10 size 1M;
      severity debug;
      print-severity yes;
      print-time yes;
    };
    category statistics {
      named-debug;
    };
};
```

Come analizzarli - strumenti testuali

Il comando `Kill -ILL named-PID` produce il seguente output in `named.stats`:

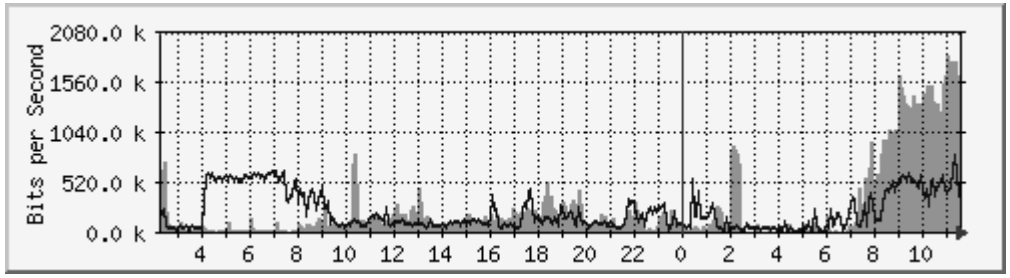
```
+++ Statistics Dump +++ (912279183) Sat Dec 18 19:53:03 1999
    1492475 time since boot (secs)
    1492475 time since reset (secs)
    15              Unknown query types
    514989          A queries
    ...
    81566           ANY queries

++ Name Server Statistics ++
(Legend)
    RR     RNXD   RFwdR  RDupR  Rfail    RFErr   Rerr    RAXFR
    RLame  ROpts  SSysQ  SAns   SFwdQ    SDupQ   SErr    RQ
    RIQ    RFwdQ  RDupQ  RTCP   SFwdR    SFail   SFErr   SNaAns  SNXD
(Global)
    143751 20437  79205  370    1387     0       24      16
    5471   0      56093  1183974 76630   67797   0       1258411
    0      76630  675    189    79205    10068   0       564681  197071
[194.119.200.41]
     0             0              2759             0               0
     0             0              0                0               0
```

Come analizzarli - strumenti grafici

Esistono vari strumenti di tipo *general-purpose* per visualizzare graficamente le statistiche.

MRTG (http://www.ee.ethz.ch/stats/mrtg/) consente di acquisire e rappresentare graficamente vari tipi di dati.

Esempio:



Un esempio di procedura di acquisizione (scritta in perl) dei dati dai file di log in un formato MRTG-compatibile è disponibile su:

ftp://ftp.nic.it/pub/DNS/tools/mrtg-collect-dns.pl

Named e la sicurezza

I principali meccanismi implementati da named sono:

- restrizione degli accessi
- inibizione dei *zone-transfer*
- autenticazione
- views (in fase di discussione da parte di ISC)
- dnsec

Autenticazione (RFC 2065)

BIND v. 8.2 supporta dei meccanismi per l'autenticazione che consentono di 'firmare' elettronicamente le informazioni fornite dai nameserver.

E' possibile creare chiavi per:

- autenticazione (validazione) di zone
- host keys
- user keys

con vari algoritmi (DSA/DSS - RSA - …) e di varie lunghezze.

Le chiavi vengono inserite nei RR di tipo KEY:

<name> IN KEY <flags> <algorithm> <protocol> <exponent|modulus>

Views

Con il meccanismo delle views sarà possibile effettuare un forward selettivo delle query a dei nameserver.
Esempio:

```
view {
 client { 194.119.200.0/24;
          193.205.35.100/24 };
 domain { "!area.ba.cnr.it" };
 forward on no-domain to { 194.119.192.34};
};
```

consentirà di effettuare un forward di tutte le query provenienti dagli indirizzi 'client' e relative ai domini diversi da "area.ba.cnr.it" al nameserver 194.119.192.34 nel caso il nostro nameserver ottenga un errore di tipo "no such domain"

DNSSEC

DNSSEC: Domain Name System Security Extension

- Descritto nel RFC 2065
- Verifica dell'integrità dei dati
- Controllo dell'autenticità dei dati
- Utilizza crittografia basata su chiave pubblica
- Tool per la generazione delle chiavi (dnskeygen) e 'firma' delle zone (dnssigner)

Nuovi RR:

- **KEY:** contiene la 'public key' della zona
- **SIG:** contiene la 'digital signature' di un RRset
- **NXT:** specifica il 'successivo' nome a dominio nella zona

BIND & Windows NT

Sono disponibili varie versioni:

- Distribuzione ufficiale Microsoft
- Distribuzione ISC (www.isc.org): BIND 8.2.x
- Varie distribuzioni di derivazione 4.9.x

http://www.microsoft.com/NTServer/nts/exec/vendors/freeshare/DNS.asp

BIND ISC: caratteristiche

Caratteristiche salienti:

- disponibile a partire dalla 8.2.x
- porting per NT effettuato da BayNetworks (supporto ‘nativo’ ISC a partire dalla v. 9.0)
- assenza di interfaccia grafica
- makefile (project file) disponibili solo per VisualC++ 6.0
- distribuito solo in formato sorgente

BIND Microsoft: caratteristiche

Caratteristiche salienti:

- non è un porting di BIND ma una riscrittura ‘from scratch’
- la configurazione può essere definita a livello di registry oppure di file (sintassi compatibile boot file v. 4.9)
- supporto del notify e del round-robin
- integrazione con il servizio WINS
- interfaccia grafica
- assenza del supporto Ipv6 e DNSSEC
- RFC: 1033, 1034, 1035, 1101, 1123, 1183, 1536
- introduce dei resource record proprietari: WINS/WINS-R (implica che tutti i nameserver autoritativi debbano essere NT)
- il file HOSTS, se presente, viene interrogato sempre dopo il DNS