Capitolo 4

Implementazione di un DNS con Bind

In questo capitolo

- **Generalità sul DNS**
- **Utilità del DNS in una rete Windows**
- **Nuove strategie di risoluzione nomi**
- **Gestione di una rete Windows**
- **Configurazione del DNS**
- **Esempio pratico**
- **Gabbie chroot**
- **Sincronizzare due DNS**
- **Configurazione dei client Windows**
- **Checklist**

La semplicità di Internet è un fenomeno recente, frutto della capillare diffusione creatasi a seguito della trasformazione da progetto governativo a mezzo disponibile al più ampio pubblico privato e commerciale.

Prima di questo passaggio epocale la Grande Rete era un ambiente specialistico, realizzato da tecnici per tecnici. L'immediatezza del web, navigabile digitando nomi facili da ricordare era qualcosa ancora lungi da venire.

In passato, per accedere a qualunque sistema della Rete, era necessario conoscere l'indirizzo numerico che identificava in maniera certa la risorsa. Era possibile creare elenchi statici memorizzabili localmente per accedere con più facilità alle destinazioni online abituali.

Con l'aumentare del numero dei nodi e degli utenti divenne chiara la necessità di superare il mero indirizzamento numerico fatto di valori IP e di elenchi statici.

Serviva una buona soluzione e una proposta dei primi anni Ottanta si rivelò efficace: fornire a ogni computer online un nome testuale facile da ricordare, per esempio `www.apogeonline.com`, e creare un elenco online, liberamente accessibile, contenente il nome esteso e l'indirizzo IP corrispondente. Per accedere a un server sarebbe così bastato digitare il nome mnemonico e fare in modo che un automatismo eseguisse la conversione all'indirizzo numerico tramite l'elenco pubblico.

Questa soluzione non imponeva un cambiamento radicale della struttura tecnica di Internet: gli indirizzi numerici rimanevano alla base della Rete. Era

solo necessaria l'aggiunta di un server in grado di eseguire la conversione dal nome esteso al valore numerico IP corrispondente. Tale soluzione è valida ancora oggi, se pur con alcune modifiche, e gli utenti di Internet ne fanno uso in maniera costante. Il nome di questo meccanismo è DNS (*Domain Name Server*).

Generalità sul DNS

Il DNS è un servizio di rete che viene installato su un server raggiungibile a tutti i nodi di una rete. Il suo scopo è ricevere interrogazioni dai client (per esempio `www.apogeonline.com`) e fornire in risposta il relativo indirizzo IP (nel caso precedente, `212.239.45.42`). Nessun sistema o utente dovrà così conoscere l'indirizzo IP di `www.apogeonline.com`. Basterà digitare il nome e il computer provvederà a interrogare il DNS per ottenere l'indirizzo numerico ed eseguire l'accesso attraverso i protocolli TCP/IP.
Il DNS ha utilità anche in ambito locale. Si consideri il caso di un'azienda che intenda attivare un sistema web per la vendita dei propri prodotti. Il primo passo consiste nello stipulare un contratto di connettività. Un carrier, per esempio Telecom Italia, allaccerà un cavo dati ad alta velocità presso l'azienda richiedente, connettendola a Internet.
Si dovrà richiedere allo stesso tempo l'assegnazione di un indirizzo IP fisso: serve un valore univoco e permanente che identifichi il proprio server web in modo che chiunque possa sempre accedervi digitando quel numero.
Gli indirizzi IP sono rilasciati da un organismo internazionale preposto alla distribuzione secondo regole ben precise
Gli indirizzi non vengono quasi mai assegnati all'utente finale, bensì ad aziende che operano nel settore delle telecomunicazioni o di Internet e dotate di comprovati requisiti tecnici. L'utente finale riceve in genere uno o più indirizzi statici solo a seguito della stipula di un contratto di connettività con uno di questi operatori.
Le connessioni professionali, anche quelle più accessibili basate su ADSL, sono di solito corredate di pacchetti di indirizzi statici proprio per andare incontro a coloro che intendono pubblicare servizi online.
Ottenuta la connessione veloce e l'indirizzo IP è possibile rendere operativo il negozio online. Il servizio di vendita può essere connesso a Internet a tempo pieno e reso accessibile da qualunque browser. Basterà digitare l'indirizzo numerico assegnato.
Difficilmente però si avrà successo se i potenziali acquirenti dovranno ricordarsi un lungo indirizzo numerico quando vorranno fare shopping. Bisogna quindi acquistare un nome di dominio attraverso un'apposita struttura di rilascio, per esempio Network Solutions (`www.netsol.com`). L'operazione è facile e permette di ottenere il dominio entro pochi minuti (Figura 4.1) al costo di pochi dollari.
Ora entra in gioco il DNS per l'associazione tra il nome simbolico acquistato e l'indirizzo numerico assegnato. L'obiettivo viene raggiunto installando un apposito servizio sulla stessa macchina che opera come server web oppure su un server a parte, purché raggiungibile dal mondo esterno. Si sceglie per questo esempio la seconda soluzione.
L'elenco delle associazioni deve essere compilato manualmente dall'amministratore di sistema. Nel caso esaminato bisogna inserire una riga per l'indirizzo esteso acquistato (nella forma `www.example.com`) e abbinare l'indirizzo IP relativo. Con lo stesso principio si dovranno indicare eventuali altri servizi o nomi che si vogliono rendere pubblici.

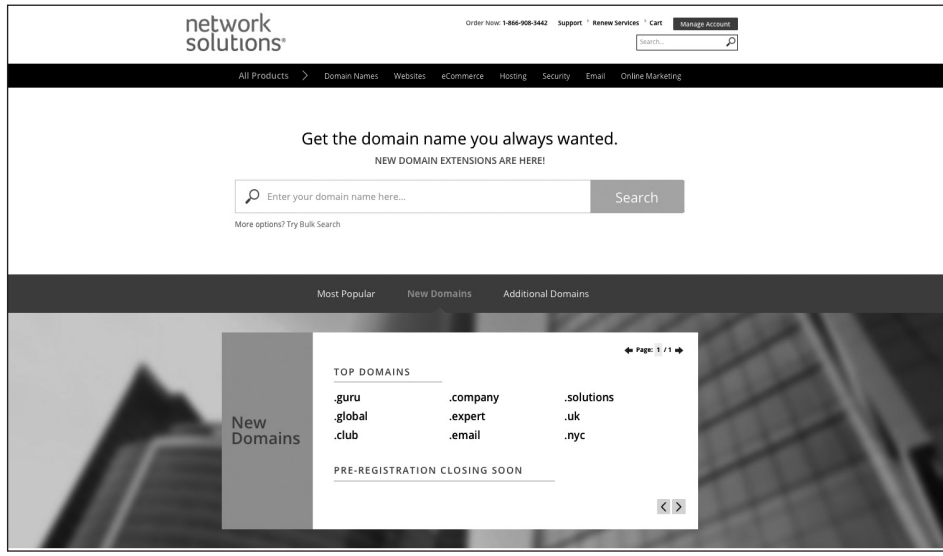

Figura 4.1 Network Solutions è uno dei più famosi servizi internazionali per la registrazione di domini.

Il DNS dovrà infine essere collegato ad altri sistemi DNS per fare in modo che l'elenco dei nomi delle proprie macchine sia consultabile da tutto il mondo; in caso contrario sarà visibile solo localmente. Per farlo, si deve tornare di nuovo su Network Solutions, entrare nel pannello di gestione dell'account e indicare che il DNS che gestisce il dominio acquistato non è più il server di Network Solutions, ma un computer sotto la propria gestione, di cui si deve fornire l'indirizzo. Confermando la nuova configurazione si avvia una procedura di aggiornamento a livello internazionale e nel giro di alcune ore le nuove impostazioni saranno diffuse in tutti gli angoli del pianeta.
Quando un utente digiterà sul browser l'indirizzo mnemonico del negozio online otterrà l'indirizzo numerico dalla gerarchia di server DNS presenti sulla rete Internet mondiale. A questo punto il browser eseguirà un accesso diretto a questo indirizzo in maniera trasparente, visualizzando le pagine.

Utilità del DNS in una rete Windows

L'esempio del negozio online dimostra l'importanza di un sistema DNS quando esiste la necessità di pubblicare un servizio per il largo pubblico. L'utilità del DNS non è però limitata alle applicazioni Internet, quando è necessario pubblicare in tutto il mondo un server di contenuti o di servizi. Anche Windows necessita di un meccanismo di risoluzione dei nomi. Le reti Microsoft, come quelle Internet, sono composte da computer che hanno nomi simbolici descrittivi, per esempio Amm1, Amm2, UffTec1, Server01 e così via. I computer funzionano però in rete locale per mezzo di indirizzi IP numerici. Nasce quindi, ancora una volta, l'esigenza di un sistema in grado di convertire i nomi estesi in valori numerici.

In passato, nelle reti dotate di Windows 95, 98, ME o server Windows NT, sussisteva un meccanismo di conversione molto semplice. Se UffTec1 aveva bisogno di accedere al pc Amm1 per leggere un file di Excel, veniva prima di tutto cercato un server WINS. Si trattava di un componente di sistema su Windows NT 4 Server che era in grado di memorizzare in maniera automatica i nomi dei computer e i relativi indirizzi numerici. Era un servizio molto simile al DNS, ma limitato all'ambito della rete locale Windows e aggiornato automaticamente dal server stesso.
UffTec1 eseguiva allora un accesso al server dove era installato il WINS e interrogava il sistema per conoscere l'indirizzo di Amm1. Il sistema WINS verificava il proprio database e forniva la risposta a UffTec1.
Come faceva però UffTec1 a conoscere l'ubicazione del server WINS? Ogni client Windows ha un campo nel pannello di configurazione del TCP/IP dove indicare l'indirizzo di questo servizio. UffTec1 avrebbe quindi eseguito un accesso al WINS presente all'indirizzo IP indicato dall'amministratore in fase di configurazione del client.
Non era però obbligatorio disporre di un server NT4 o di un sistema WINS per ottenere la risoluzione dei nomi. Le reti Windows basate su Windows 9x/ME o NT4 sfruttavano anche altri meccanismi. Se non c'era il sistema WINS, veniva fatta la ricerca all'interno del file `hosts`, localizzato dentro la directory di sistema di Windows. Questo non è altro che un file di testo con un elenco di associazioni tra nomi simbolici e indirizzi numerici.
Se non era presente neppure il file `hosts`, veniva impiegata una politica drastica: si effettuava il broadcast. UffTec1 mandava una comunicazione a tutti i computer presenti in rete, richiedendo ad Amm1 di rispondere fornendo il proprio indirizzo.
È un metodo comodo in quanto non richiede configurazione ma comporta traffico sulla rete locale. È inefficiente interpellare tutti i computer ogni volta che si intende dialogare con un singolo sistema. Si tratta inoltre di una strada non percorribile in reti locali ampie perché una parte consistente di banda passante sarebbe occupata dai continui broadcast.

Nuove strategie di risoluzione nomi

La situazione è cambiata in maniera significativa a partire da Windows 2000, quando è divenuta necessaria la presenza di un server DNS per l'implementazione di una rete Windows.
A partire da questa versione i nomi estesi vengono risolti in un primo momento con il DNS e solo in seguito con i vecchi meccanismi basati su WINS, file `hosts` e `broadcast` (nel caso il nome non sia presente nel DNS o non vi sia addirittura un server DNS).
C'è un punto di attenzione in questa strategia. Se si decide di non usare un DNS locale per censire nomi e indirizzi dei sistemi interni vi saranno rallentamenti durante gli accessi. Non bisogna dimenticare che i client di una rete locale dispongono di un indirizzo DNS per gli accessi a Internet. Se manca un DNS per la risoluzione dei nomi interni sarà interrogato questo server DNS esterno ogni volta che si dovrà accedere per nome a un computer della rete locale. Naturalmente sui DNS mondiali non ci saranno indicazioni sulla macchina interna denominata Amm1. L'interrogazione restituirà un messaggio di host non trovato. Questa procedura non è istantanea e richiede un tem-

po relativamente alto per essere portata a termine. Solo dopo questo lasso di tempo verranno eseguiti altri tentativi di risoluzione interni (WINS, file `hosts` e broadcast). Gli utenti sperimenteranno in tal caso una notevole lentezza nell'uso dei servizi della LAN e si creerà un disservizio misurabile.
In alcuni casi si possono avere ripercussioni anche economiche. In molte città non sono disponibili accessi a Internet flat. Il problema della connettività viene allora risolto con un accesso on demand, per esempio un accesso UMTS che si attiva ogni qualvolta serve l'accesso a una risorsa Internet. La connessione rimarrà attiva per un lasso di tempo e poi verrà interrotta automaticamente.
In un simile contesto ogni accesso a un computer interno comporterà l'accesso a Internet tramite rete cellulare per l'interrogazione di un DNS esterno. I tempi di accesso alle risorse saranno elevati e i costi in bolletta cresceranno senza motivo. Per risolvere tutti questi problemi è necessario installare un server DNS locale. Se si hanno però pochi client Windows non risulterà conveniente acquistare una licenza server di Windows. Il problema può essere allora risolto con una soluzione Linux e il pacchetto Bind, disponibile in tutte le distribuzioni ma comunque scaricabile dall'indirizzo `https://www.isc.org/downloads/bind` (Figura 4.2).

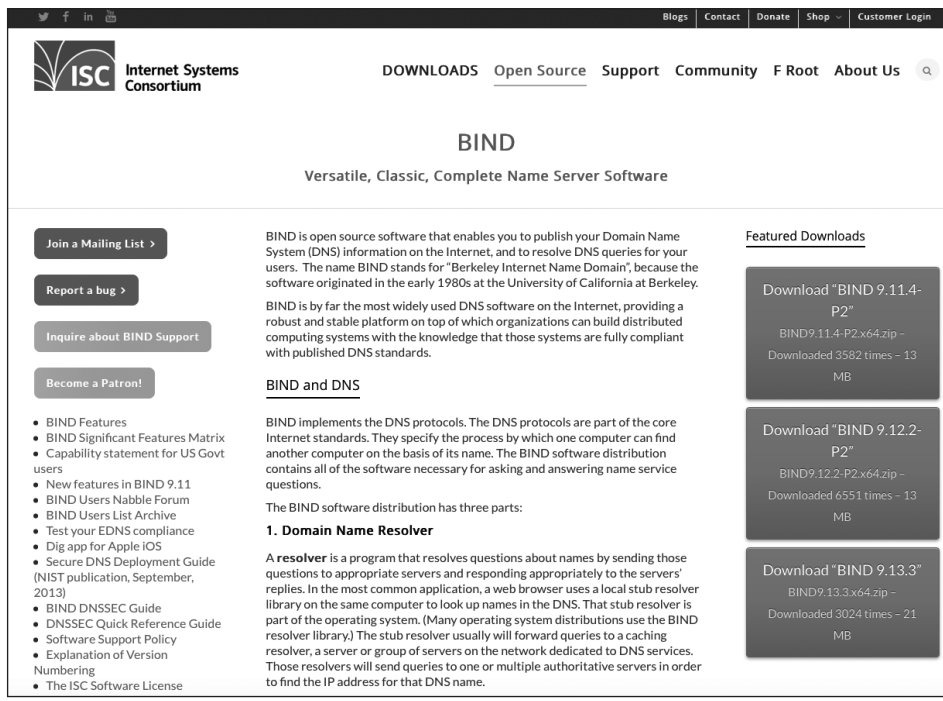

Figura 4.2 Sito ufficiale di Bind.

Bind permette di gestire un sistema DNS in maniera completamente standard e può essere di aiuto sia nel caso in cui si voglia rendere operativo un servizio pubblico su Internet, sia quando serve un'infrastruttura di risoluzione dei nomi per una rete locale basata su Windows.

Gestione di una rete Windows

Si supponga di voler gestire con Bind la risoluzione degli indirizzi per una rete locale composta da tre client Windows, un print server e una connessione a Internet tramite ADSL. Le macchine si chiamano PC1, PC2 e PC3 e hanno indirizzi IP interni, rispettivamente 192.168.100.10, 192.168.100.11 e 192.168.100.12. Il print server è invece configurato per rispondere all'indirizzo IP 192.168.100.50.
Come si può notare, gli indirizzi sono impostati manualmente e non rilasciati con meccanismi di assegnazione automatica come DHCP. È stata operata questa scelta perché il servizio DNS è di tipo statico e perciò tutte le macchine listate nel DNS devono mantenere lo stesso IP nel tempo. Se un client cambia indirizzo, bisogna aggiornare manualmente anche il DNS. In caso contrario Bind fornirebbe il vecchio indirizzo non più valido a qualunque sistema che ne facesse richiesta.
Il sistema Linux può essere installato su una macchina anche datata, purché fornita di sufficiente memoria RAM e di un disco rigido veloce. Anche questo server avrà un indirizzo IP statico, 192.168.100.4 (Figura 4.3).

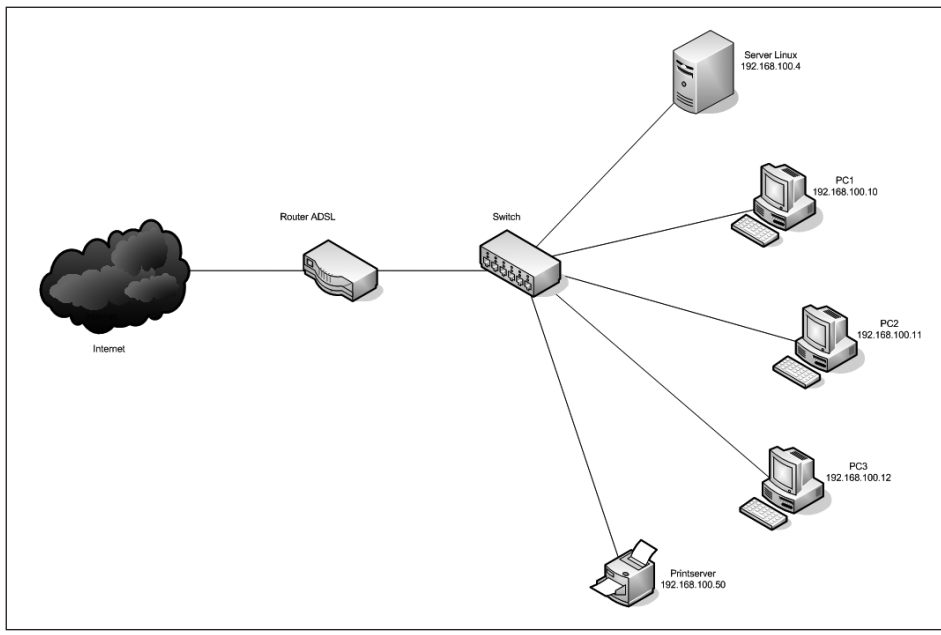

Figura 4.3 Schema di rete dell'esempio in esame.

Configurazione del DNS

Per personalizzare Bind bisogna innanzitutto cercare il file di configurazione principale che, a seconda delle distribuzioni, può trovarsi dentro la directory `/etc` oppure in `/etc/bind` con il nome `named.conf`.

Il file contiene una configurazione generica di default applicata in fase di installazione della distribuzione. Probabilmente si avrà un file molto simile al seguente, tratto da una distribuzione CentOS.

Listato 4.1

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 127.0.0.1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; };
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";
};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

In alternativa si potrebbe avere un file molto stringato, con una serie di direttive `include` che non fanno altro che caricare altri file di configurazione. Si tratta di un modo per mantenere le configurazioni più modulari e ordinate, come nell'esempio del Listato 4.2 tratto da una distribuzione Ubuntu Server.

Listato 4.2

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

Il file `named.conf` può essere idealmente suddiviso in due parti: una sezione contenente impostazioni generali di funzionamento (in Ubuntu nel file `named.conf.options`) e una sezione contenente le definizioni delle "zone" (in Ubuntu nei file `named.conf.local` e `named.conf.default-zones`).
Nelle impostazioni generali bisogna verificare la configurazione di due direttive:

```
listen-on port 53 { 127.0.0.1; };
allow-query     { localhost; };
```

Queste righe sono tratte dalla configurazione CentOS riportata più in alto. La prima direttiva specifica la porta su cui il servizio Bind ascolterà le richieste. Il valore di default per il DNS è `53`, perciò specificato nel modo corretto. Bisogna invece modificare l'indirizzo IP. L'impostazione in alto permetterebbe richieste provenienti solo dall'interfaccia locale. Si desidera invece servire tutta la rete. È necessario modificare la riga sostituendo il valore con l'indirizzo IP della scheda di rete:

```
listen-on port 53 { 192.168.100.1; };
```

La riga successiva permette di applicare una restrizione di sicurezza. Saranno cioè servite le interrogazioni provenienti solo dall'host locale. Qualunque richiesta proveniente dalla rete locale sarebbe ignorata. Per rendere possibile query da qualunque computer si deve modificare la riga nel seguente modo:

```
allow-query     { any; };
```

In questo modo le interrogazioni saranno permesse a qualunque computer, qualunque sia la rete di provenienza. Se si desidera un'impostazione intermedia e limitare le interrogazioni alla sola sottorete IP locale si può usare invece la seguente sintassi:

```
allow-query     { 192.168.100.0/24 };
```

Le altre impostazioni di default dovrebbero essere già funzionali. Si può così dirigere l'attenzione alla sezione di definizione delle zone.
Una *zona* è un insieme di computer raggruppati secondo un criterio arbitrariamente scelto dall'amministratore. Nelle piccole realtà si sceglie di solito di identificare una zona con il dominio stesso. Se cioè si ha un dominio registrato per la propria azienda, si può creare una zona DNS con tutti i computer aziendali raggruppati con questo stesso nome.
Il sistema DNS non è comunque privo di zone appena completata l'installazione. Vi sono alcune zone di default caricate dal file `/etc/named.rfc1912.zones` su CentOS e dal file `/etc/bind/named.conf.default-zones` su Ubuntu. Tra queste `localhost` e `1.0.0.127.in-addr.arpa`.

Si tratta di nomi standard che si riferiscono al sistema locale, il primo per le ricerche dirette e il secondo per le ricerche inverse (l'etichetta `in-addr.arpa` è una formula storica che rappresenta sempre un dominio di ricerca inversa).
Una ricerca diretta è un'interrogazione che punta a determinare l'indirizzo IP a partire dal nome esteso, per esempio fornendo il nome `www.apogeonline.com`. Ogni volta che si scrive un indirizzo mnemonico nel browser e si preme il tasto Invio della tastiera si genera un'interrogazione diretta al DNS per ottenere l'indirizzo IP del sistema che si vuole raggiungere.
La ricerca inversa si ha invece quando si vuole sapere quale nome è associato a un determinato IP.
Per convenzione il sistema locale è sempre associato all'IP 127.0.0.1. Questo valore, detto *indirizzo di loopback*, è stato introdotto per fare in modo che ogni macchina possieda sempre un indirizzo valido, anche se l'amministratore non ne imposta uno. L'utilizzo del loopback è rigorosamente interno. Non si troverà cioè mai un computer esterno con questo IP.
Un ping verso 127.0.0.1 genererà un "anello" locale: la richiesta sarà gestita dal sistema TCP/IP del proprio computer, senza uscire dalla scheda di rete. Questa operazione è molto utile per verificare che lo stack TCP/IP stia funzionando nel modo corretto.

L'INDIRIZZO DI LOOPBACK COME SINONIMO DELLA MACCHINA LOCALE

L'indirizzo di loopback è un modo comune per fare riferimento alla macchina locale stessa. Molte applicazioni e servizi di rete usano questo indirizzo nei file di configurazione per funzionare. In questo modo gli script di installazione non hanno bisogno di conoscere l'indirizzo IP che è stato assegnato dall'amministratore di sistema alla macchina locale. Molte configurazioni di default risultano così funzionanti appena installate nel sistema.

Su CentOS la configurazione della zona localhost contiene un riferimento al file `named.localhost` mentre la specifica di zona `1.0.0.127.in-addr.arpa` contiene un riferimento al file `named.loopback`. Questi file si trovano in `/var/named`. Su Ubuntu i file si trovano invece in `/etc/bind/db.local` e `/etc/bind/db.127`.
Il file `localhost.zone` su CentOS è così strutturato.

Listato 4.3

```
$TTL 1D
@     IN SOA      @ rname.invalid. (
                                    0        ; serial
                                    1D       ; refresh
                                    1H       ; retry
                                    1W       ; expire
                                    3H )     ; minimum
      NS @
      A  127.0.0.1
      AAAA        ::1
```

Il file inizia con una chiave `$TTL 1D`, che non deve essere cambiata e un preambolo contraddistinto da `SOA` (*Start Of Authority*). Questo inizia con il simbolo `@`, finisce alla chiusura della prima parentesi tonda e contiene alcuni dettagli necessari al funzionamento del sistema DNS.

Il simbolo @ è un sinonimo per quella che si chiama *origine*. Il file named.localhost che si sta esaminando è stato specificato in named.conf nella zona localhost. L'origine è perciò localhost, il nome di zona specificato in named.conf.
La prima riga del preambolo viene quindi tradotta in questo modo:

```
localhost.          IN  SOA  localhost.  rname.invalid. (
```

Il punto alla fine di localhost indica che l'indirizzo è assoluto e letterale. Se non c'è il punto, si ha invece un indirizzo relativo, costruito aggiungendo il nome di zona. Ricapitolando, localhost. significa semplicemente localhost, mentre localhost (senza punto) viene automaticamente espanso in localhost.localhost ogni volta che viene usato. Questa scelta sintattica permette alcuni automatismi in Bind e serve per rendere più corti i file di configurazione, evitando di dover sempre scrivere la zona per esteso nel caso in cui i nomi siano molto lunghi. Niente infatti vieta di avere una zona chiamata ufftec.bologna.italia.example.com. Sarebbe però scomodo riscrivere questa stringa di testo ogni volta che si volesse inserire un indirizzo nel DNS. Invece di scrivere per esempio pc1.ufftec.bologna.italia.example.com è sufficiente scrivere pc1 (senza il punto). Il sistema espanderà automaticamente il nome.
Subito prima dell'apertura della parentesi tonda compare l'indicazione rname.invalid. Questo è l'indirizzo email del gestore del DNS in una notazione priva di @ (se usato, il simbolo sarebbe interpretato come nome di origine, causando un errore). Al suo posto viene invece usato un punto. L'esempio rappresenta perciò rname@invalid. Questa stringa andrebbe modificata in un indirizzo mail esistente, per esempio szanzi.example.com, espanso in fase di funzionamento in szanzi@example.com.
Le righe seguenti contengono indicazioni importanti ai fini della sincronizzazione del server DNS locale con altri server DNS. Vista l'importanza della risoluzione dei nomi in una rete si impostano in genere due o più server DNS con le stesse informazioni, tipicamente ubicati in punti diversi della propria struttura. In caso di down di un DNS si potranno risolvere i nomi attraverso i DNS superstiti. Quando si deve aggiornare un record su un DNS ridondante è sufficiente applicare la modifica sul server DNS principale, definito *master* e poi incrementare il campo serial. Gli altri server rileveranno il diverso numero seriale e richiederanno l'intera zona per aggiornarsi.
Gli altri campi presenti all'inizio della definizione di zona servono per specificare il tempo di refresh, ovvero ogni quanto tempo i DNS devono aggiornarsi, il tempo di retry, ovvero dopo quanto tempo ritentare l'operazione in caso di mancata sincronizzazione e il tempo di expire che specifica il valore temporale oltre il quale il DNS perde validità se non riesce più a sincronizzarsi con gli altri DNS.
Nella riga successiva compare NS che sta per *nameserver*. Qui è indicato che il DNS si trova sul sistema locale localhost. Di seguito si ha la specifica A che sta per *Address*. Questa è un'associazione nome/indirizzo che segnala che localhost è presente all'indirizzo 127.0.0.1. L'ultima riga esegue di nuovo l'associazione ma all'interno del dominio di indirizzi IPv6.

LA STRINGA IN

La stringa IN ricorre all'interno della configurazione delle zone DNS. Si tratta di una convenzione sintattica che specifica la classe. Il valore di classe IN è descritto nel RFC 1035 come "Internet". Si può omettere l'indicazione IN dato che il sistema DNS lo applicherà automaticamente in fase di funzionamento.

Esempio pratico

Le configurazioni esaminate fin qui sono molto generiche e regolano il funzionamento del proprio sistema Linux dopo un'installazione del tutto standard. Per servire la rete locale è necessario specificare i nomi dei computer, i relativi indirizzi e creare una zona di pertinenza. Per fare questo si deve andare nel file di configurazione generale `named.conf` e inserire una nuova zona.

Listato 4.4

```
zone  "example.com" {
  type master;
  file  "example.com.zone";
};
```

In Ubuntu si consiglia di inserire la zona nel file `named.conf.local`.
In questo caso si sta specificando che esiste una nuova zona denominata `example.com` dentro il file `example.com.zone`.
Il tipo è definito `master` perché tutte le informazioni sulla zona sono presenti in maniera esaustiva dentro il file `example.com.zone`. Si sta in pratica affermando che questo DNS ha la piena autorità sulla zona.
In alternativa esiste anche il tipo `slave`. In tal caso si afferma che la zona è specificata in un altro DNS e che il sistema locale deve trarre tutte le informazioni sulla zona da un preciso DNS esterno. Viene così creato un file locale costruito grazie alle informazioni scaricate da un sistema remoto. Questo file ha una scadenza, dopo la quale sarà aggiornato con un nuovo accesso al DNS di riferimento. Questo permette ai due sistemi DNS di rimanere sempre sincronizzati.
Il file `example.com.zone` dovrà contenere riferimenti ai sistemi presenti nel proprio ufficio, per esempio `pc1`, `pc2`, `pc3` e `printserver`.

Listato 4.5

```
$TTL 86400

@ IN SOA @ info.example.com (
        4       ; serial
        28800   ; refresh
        7200    ; retry
        604800  ; expire
        86400   ; ttl
        )

                        NS      127.0.0.1.

pc1             IN      A       192.168.100.10
pc2             IN      A       192.168.100.11
pc3             IN      A       192.168.100.12
printserver     IN      A       192.168.100.50
```

Si può notare che il preambolo contiene la forma standard vista in precedenza, ma con l'indirizzo dell'amministratore locale `info.example.com` (notazione per `info@example.com`).

La specifica NS punta al sistema locale (indirizzo di loopback 127.0.0.1). Poi si hanno una serie di specifiche A (*address*), una per ogni sistema da registrare. Qui diventa finalmente chiara l'associazione tra i nomi estesi e gli indirizzi IP numerici.
Quando un utente digiterà il comando ping pc1 dalla shell dei comandi di un client interno, il computer interrogherà questo DNS, scandirà la lista delle specifiche A, troverà la riga pc1, otterrà l'indirizzo IP numerico e potrà così eseguire effettivamente la richiesta con un ping a 192.168.100.10.

INTERROGAZIONI A RISORSE PUBBLICHE

Lo stesso meccanismo accade quanto si visita un qualunque sito web. Quando si digita, per esempio, www.linux.org, il proprio computer esamina un archivio DNS che fa riferimento a linux.org e scorre i record A per trovare la voce www. Una volta individuata, legge l'IP corrispondente e lo fornisce al browser per la connessione.

La configurazione mostrata nel Listato 4.5 può essere arricchita con il riferimento per il server Linux locale e il gateway Internet:

```
server   IN  A  192.168.100.1
gateway  IN  A  192.168.100.5
```

A questo punto i file di configurazione risultano creati. Per renderli operativi bisogna attivare il demone DNS o procedere al riavvio nel caso il servizio sia già in funzione. Per attivare il demone, si deve digitare il seguente comando:

```
systemctl start named
```

Se il demone è stato lanciato in fase di boot bisogna riavviare il servizio per attivare le modifiche appena inserite. Su CentOS:

```
systemctl restart named
```

In alcune distribuzioni, lo script di avvio ha un nome differente. Per avviare Bind su una distribuzione Ubuntu si utilizza questa sequenza:

```
systemctl start bind9
```

Il DNS è pronto e attivo. Ora occorre configurare il server locale per fare in modo che usi il DNS interno appena creato. Prima di tutto bisogna tornare nella directory /etc e aprire il file host.conf.
Questo file specifica l'ordine con cui viene eseguita la risoluzione dei nomi. Di default si ha la configurazione seguente:

```
order hosts, bind
```

Questo significa che viene prima esaminato il file hosts, presente anch'esso dentro /etc e poi il sistema DNS.
Il file hosts è un elenco che associa i nomi estesi agli indirizzi IP ed è molto simile al DNS, ma più semplice e privo della strutturazione gerarchica del DNS. Di default contiene la riga seguente:

```
127.0.0.1 localhost.localdomain localhost
```

Si tratta dell'associazione dell'indirizzo di loopback locale al nome localhost, un alias di solito usato dalle applicazioni Linux per fare riferimento al sistema locale. Un ping a localhost equivale a un ping a 127.0.0.1. La configurazione di default di host.conf e di

`hosts` può essere lasciata inalterata anche se alcuni utenti preferiscono invertire l'ordine di ricerca in `host.conf` per avere prima l'interrogazione sul DNS e poi quella nel file `hosts`:

```
order bind, hosts
```

Per concludere, bisogna controllare un ulteriore file di sistema: `/etc/resolv.conf`. Questo file contiene gli indirizzi dei server DNS che il computer locale deve interrogare per risolvere i nomi. Bisogna semplicemente specificare che si vuole usare il DNS appena configurato:

```
nameserver 127.0.0.1
```

Questa configurazione attiva il DNS per le operazioni locali. Un ping dalla shell di Linux a `pc2.example.com` sarebbe correttamente risolto nell'indirizzo `192.168.100.11`.
Sussiste però un problema. Sono stati specificati unicamente i sistemi locali. Se si tentasse di accedere con il browser a qualunque sito esterno o a qualunque altro tipo di servizio si verificherebbe un errore. Il DNS non contiene infatti riferimenti al mondo esterno. Il problema può essere risolto in maniera molto rapida aggiungendo nuove righe in `resolv.conf` con gli indirizzi dei DNS del proprio provider o altri DNS pubblici, come quelli di Google:

```
nameserver 127.0.0.1
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Se la ricerca sul primo DNS fallisce, viene interrogato il server DNS seguente e poi quelli successivi fino a quando il nome viene risolto o quando l'elenco dei DNS viene visitato completamente senza esito.

Gabbie chroot

Potrebbe succedere che le impostazioni sul DNS non abbiano effetto e qualunque operazione porti a errori o a comportamenti del tutto inaspettati.
Questo avviene se nella propria distribuzione il DNS è implementato all'interno di quella che si definisce una *gabbia chroot*. Si tratta in sostanza di un "file system in piccola scala", isolato dal resto del sistema per motivi di sicurezza. Se un utente malintenzionato riuscisse a violare il DNS non potrebbe alterare il sistema, in quanto si troverebbe confinato nella gabbia chroot, un'area con un numero estremamente limitato di comandi critici.
Se il DNS funziona all'interno di una gabbia chroot, significa che il file di configurazione principale non è localizzato in `/etc` e le specifiche di zona non sono in `/var/named`. La struttura operativa è in realtà altrove.
Alcune distribuzioni creano una gabbia chroot per Bind e qualunque configurazione sui file in `/etc` non porterebbe ad alcun risultato. Bisogna piuttosto accedere a `/var/named/chroot` (la gabbia chroot) e utilizzare il file `named.conf` presente in `/etc` della gabbia.
È importante verificare questo aspetto per non perdere ore cercando di configurare i file sbagliati.
Dentro una gabbia chroot i percorsi devono essere indicati come se si lavorasse dentro le directory "ordinarie" del sistema. Per esempio, il file di zona `example.com.zone` che

viene creato dentro /var/named/chroot/etc, sarà specificato nel file di configurazione di Bind con questo formato.

Listato 4.6

```
zone "example.com"
      {
       type master;
       file "/etc/example.com.zone";
       allow-update { key SERVERKEY; };
      };
```

Come si può notare, viene indicato /etc/example.com.zone e non l'intero percorso.

Sincronizzare due DNS

Nelle pagine precedenti si è accennato alla possibilità di sincronizzare due server DNS presenti su macchine differenti per ottenere ridondanza e garantire la risoluzione dei nomi anche in caso di crash o down di uno dei sistemi.
Per sincronizzare una zona è necessario stabilire un nodo che si definisce *master* dove saranno applicate le modifiche di zona quali l'inserimento o la rimozione dei nodi. Il secondo nodo sarà invece lo *slave* che riceverà gli aggiornamenti. I nodi avranno rispettivamente indirizzo 192.168.0.10 e 192.168.0.20.
La zona di esempio example.com viene configurata nel nodo master nel seguente modo.

Listato 4.7 Nodo master all'indirizzo 192.168.0.10.

```
zone  "example.com" {
        type master;
        file  "example.com.zone";
        allow-transfer { 192.168.0.20; };
       };
```

Il nodo slave viene invece configurato come segue.

Listato 4.8 Nodo slave all'indirizzo 192.168.0.20.

```
zone  "example.com" {
        type slave;
        file  "example.com.zone";
        masters { 192.168.0.10; };
};
```

Come si può osservare bisogna indicare in modo preciso quale è il nodo master e quali sono i nodi slave designati, in questo esempio uno solo attraverso la rispettiva direttiva. Naturalmente il nome di zona deve essere identico nei vari nodi DNS.
Nel nodo master si deve inserire la direttiva allow-transfer seguita dagli indirizzi dei nodi slave. Si tratta di una misura di sicurezza per impedire che qualunque nodo possa scaricare l'intera zona. Sullo slave si deve invece indicare l'indirizzo del server master con la direttiva masters. Completata la configurazione si devono riavviare entrambi i sistemi.

Attenzione al fatto che non si ottiene una sincronizzazione ogni volta che si esegue una modifica sul master. Il caricamento avviene infatti secondo i tempi indicati nelle direttive `refresh` ed `expire`. È per questo motivo che quando si acquista un dominio pubblico e si apportano modifiche occorre attendere alcune ore per avere le modifiche propagate ovunque nel mondo. Si devono attendere i tempi di aggiornamento automatici dei DNS pubblici.
Per forzare un aggiornamento si può accedere al server slave, cancellare il file di zona e riavviare Bind. In questo modo la configurazione verrà ricaricata.
Non si deve infine dimenticare di incrementare il seriale ogni volta che si aggiornare il master, in caso contrario non si avrebbe comunque l'aggiornamento dello slave.

FORMATO PER LA STESURA DEL NUMERO SERIALE

Esiste un formato convenzionale per la stesura dei seriali dei DNS attraverso un numero che comprende anno, mese, giorno e un numero incrementale come in 2014051001, ovvero il primo aggiornamento del giorno 10 Maggio 2014. Un aggiornamento eseguito il giorno seguente dovrebbe avere il seriale 2014051101. Un aggiornamento successivo, effettuato nello stesso giorno, avrebbe invece seriale 2014051102.

Se i seriali di master e slave coincidono, non avviene alcuna sincronizzazione tra i due sistemi.

Configurazione dei client Windows

Per configurare i client Windows occorre andare nel pannello di configurazione di rete e aprire la configurazione del protocollo TCP/IP. In basso, nella configurazione DNS, bisogna specificare l'indirizzo del sistema Linux, 192.168.100.4. Come indirizzi secondari bisogna invece mettere i DNS del proprio provider o di un servizio pubblico. In questo modo si impiega il proprio DNS per gli indirizzi interni e i DNS pubblici per tutti gli altri indirizzi Internet (Figura 4.4).
Per verificare che stia tutto funzionando nel modo corretto si può aprire una shell dei comandi e tentare alcune risoluzioni nomi. Per farlo si accede al menu *Windows* in basso a sinistra e si digita `cmd`. Il sistema proporrà *Prompt dei comandi*, da confermare con un Invio. Comparirà la shell dei comandi. Si deve digitare `nslookup`, seguito di nuovo da Invio. Il programma `nslookup` indicherà il server DNS di riferimento interno 192.168.100.4 e resterà in attesa di nomi estesi da convertire in indirizzi numerici.
Vi è un dettaglio da tenere in considerazione. I nomi sono sempre composti da un nome host e da un dominio. Per esempio `pc2` è il nome host, mentre `example.com` è il dominio. Windows aggiunge automaticamente il suffisso ai nomi host digitati. Scrivendo `pc2` in `nslookup` si avrà così il completamento, evitando la necessità di scrivere per esteso `pc2.example.com`. Si dovrebbe ottenere come risposta `192.168.100.11`. Inserendo invece un indirizzo esterno come `www.apogeonline.com` si avrà il corretto indirizzo IP ottenuto dal sistema DNS del proprio provider.

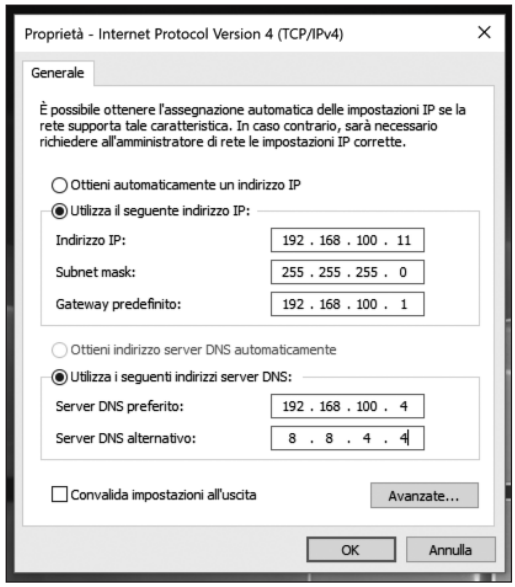

Figura 4.4 Configurazione del pannello di rete in Windows.

È possibile verificare e impostare il suffisso che viene inserito da Windows accedendo al pannello di rete del TCP/IP, facendo clic sul bottone *Avanzate*. Per default viene usato il suffisso della zona DNS ma è possibile specificare manualmente un valore (Figura 4.5) nel box inferiore *Aggiungi i seguenti suffissi DNS (nell'ordine indicato)*.

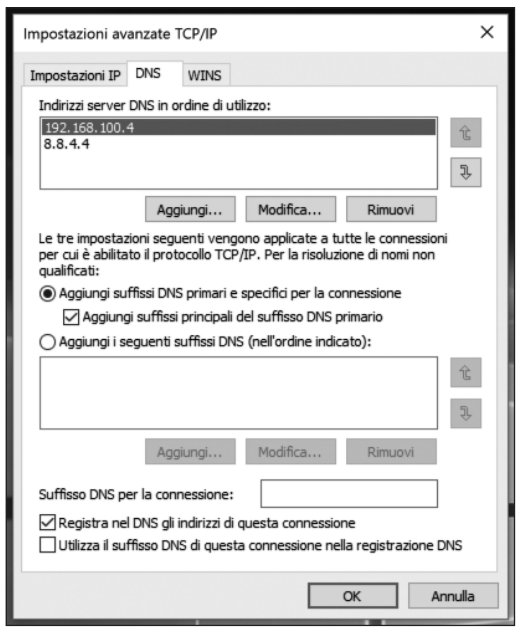

Figura 4.5 Configurazione del pannello di rete in Windows.

Per uscire da `nslookup` basta digitare `exit` e poi scrivere nuovamente `exit` per chiudere la shell di comandi.

Checklist

1. Installare il pacchetto Bind nel sistema.
2. Verificare se il sistema DNS è installato in una gabbia chroot. In caso affermativo i file di configurazione indicati di seguito saranno memorizzati dentro la gabbia anziché in `/etc`.
3. Aprire il file `named.conf`, che si può trovare all'interno della directory `/etc` oppure in `/etc/bind` oppure dentro la gabbia chroot.
4. Specificare le zone che si intendono configurare nel DNS e le opzioni generali.
5. Creare, all'interno della directory `/etc/bind`, i file per le zone specificate in `named.conf`.
6. Riavviare il servizio con il comando `/etc/init.d/named restart` oppure `/etc/init.d/bind9 restart`.
7. Aprire il file `/etc/host.conf` e modificare l'ordine con cui il sistema risolve gli indirizzi, specificando prima `bind` e poi `hosts`.
8. Aprire il file `/etc/resolv.conf` e indicare l'indirizzo IP del DNS appena configurato. È sufficiente l'indirizzo di loopback locale 127.0.0.1.
9. Configurare i client, inserendo l'indirizzo IP del sistema DNS appena creato. Come indirizzi secondari si possono specificare gli indirizzi IP dei DNS del provider o di un servizio pubblico.