6

Tecniche e strumenti per il troubleshooting di un sistema DNS

Introduzione

In questo capitolo vengono presentate alcune tecniche e strumenti (*utility*) per procedere con l'analisi e la risoluzione di eventuali problemi riscontrati operando all'interno di un'infrastruttura DNS pubblica e/o privata. In particolare, verranno prese in considerazione problematiche legate alla risoluzione dei nomi. Viceversa, dei problemi, delle tecniche e degli strumenti connessi alla gestione delle zone e dei domini DNS si è già discusso nel Capitolo 5, "Progettazione, implementazione e gestione di un sistema DNS".

Prima di effettuare le prove indicate nei paragrafi seguenti è necessario accertarsi della disponibilità delle porte utilizzate dai relativi protocolli (e.g.: Whois → 43/tcp; DNS → 53/tcp e 53/udp), nel caso in cui la connessione a Internet è mediata da proxy e/o firewall.

Interrogazione di un database Whois per risalire alle coordinate di registrazione di un dominio o agli assegnatari di un indirizzo IP

Come trattato nel Capitolo 3, "Gli organismi che governano Internet", e nell'Appendice C, "Client Windows Whois", mediante un client Whois (sia tramite interfaccia grafica Web che dal prompt dei comandi), è possibile ottenere molte informazioni riguardanti i nomi di dominio registrati, ed in particolare alcuni loro attributi (e.g.: coordinate degli assegnatari, *admin-c*, *tech-c*, server DNS di riferimento, data di scadenza del contratto di assegnazione di un nome a dominio, ecc.), come anche eventuali assegnatari di indirizzi IP pubblici assegnati dai *Regional Internet Registry* (RIR).

Ad esempio, tramite una query Whois su un nome di dominio è possibile accertare se un nome a dominio è già registrato oppure individuare i server DNS autoritativi per la relativa zona.

Esempio: whois guidadns.it

```
*******************************************************************************
Whois server: whois.nic.it
*******************************************************************************

************************************************
* Please note that any results obtained are a     *
* subgroup of the data contained in the database *
*                                                 *
* The full objects' data can be visualised at:    *
* http://www.nic.it/RA/database/index.html        *
************************************************

domain:                 learning-solutions.it
org:                    Silmar Consulting sas di Randazzo Leone
admin-c:                LR2916-ITNIC
tech-c:                 AB91-ITNIC
postmaster:             AB91-ITNIC
zone-c:                 AB91-ITNIC
nserver:                212.25.160.10 dns.seeweb.it
nserver:                217.64.196.10 dns2.seeweb.it
mnt-by:                 STT-MNT
created:                20050204
expire:                 20060204
source:                 IT-NIC

person:                 Leone Randazzo
address:                IT-NIC
address:                piazza Durante 8
address:                I-20131 Milano
nic-hdl:                LR2916-ITNIC
source:                 IT-NIC

person:                 Antonio Baldassarra
address:                C.so Lazio, 9/a
address:                I - 03100 - Frosinone
address:                Italy
nic-hdl:                AB91-ITNIC
mnt-by:                 STT-MNT
source:                 IT-NIC
```

Oppure, conoscendo un indirizzo IP, è possibile risalire all'assegnatario (oltre che al registro competente).

```
C:\etc\dig>whois -r whois.ripe.net 198.41.0.4
********************************************************************************
Whois server: whois.ripe.net
********************************************************************************
% This is the RIPE Whois query server #2.
% The objects are in RPSL format.
%
% Note: the default output of the RIPE Whois server
% is changed. Your tools may need to be adjusted. See
% http://www.ripe.net/db/news/abuse-proposal-20050331.html
% for more details.
%
% Rights restricted by copyright.
% See http://www.ripe.net/db/copyright.html

% Note: This output has been filtered.
%       To receive output for a database update, use the "-B" flag

% Information related to '0.0.0.0 - 255.255.255.255'

inetnum:        0.0.0.0 - 255.255.255.255
netname:        IANA-BLK
descr:          The whole IPv4 address space
country:        EU # Country is really world wide
org:            ORG-IANA1-RIPE
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
status:         ALLOCATED UNSPECIFIED
remarks:        The country is really worldwide.
remarks:        This address space is assigned at various other places in
remarks:        the world and might therefore not be in the RIPE database.
mnt-by:         RIPE-NCC-HM-MNT
mnt-lower:      RIPE-NCC-HM-MNT
mnt-routes:     RIPE-NCC-RPSL-MNT
source:         RIPE # Filtered

organisation:   ORG-IANA1-RIPE
org-name:       Internet Assigned Numbers Authority
org-type:       IANA
address:        see http://www.iana.org
remarks:        The IANA allocates IP addresses and AS number blocks to RIRs
remarks:        see http://www.iana.org/ipaddress/ip-addresses.htm
remarks:        and http://www.iana.org/assignments/as-numbers
e-mail:         bitbucket@ripe.net
```

```
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
mnt-ref:        RIPE-NCC-HM-MNT
mnt-by:         RIPE-NCC-HM-MNT
source:         RIPE # Filtered

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
e-mail:         bitbucket@ripe.net
admin-c:        IANA1-RIPE
tech-c:         IANA1-RIPE
nic-hdl:        IANA1-RIPE
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         RIPE-NCC-MNT
source:         RIPE # Filtered
```

Per ulteriori informazioni sul formato di un database Whois e sull'uso del client Whois si rimanda il lettore ai capitoli ed all'appendice sopra indicati.

Nslookup

Nslookup (il cui nome deriva da *Name Server Lookup*) è uno strumento distribuito in qualsiasi sistema operativo nel quale è utilizzato il protocollo TCP/IP (Linux/Unix, Novel, MAC OS X, Windows NT/2K/XP/2K3/2K3-R2/Vista, ecc.).

Esso consente di verificare il corretto funzionamento del processo di risoluzione dei nomi tramite il servizio DNS e di simulare l'invio di query da parte di un DNS resolver (*stub* o *full*). Infatti, è possibile far agire *nslookup* allo stesso modo di come agirebbe un DNS client normale (*stub resolver*) oppure un DNS server (*full resolver*), nel caso in cui quest'ultimo si trovi coinvolto in un processo di risoluzione di una query ricorsiva per conto di un DNS resolver di tipo *stub*, laddove si richiede la capacità di emettere delle query iterative e seguire l'iter della risoluzione dei nomi attraverso l'interazione con i server DNS autoritativi per i domini/zone intermedie.

Gli esempi seguenti sono stati effettuati in ambiente Win2K/2K3/2K3-R2/XP/Vista, Linux Red Hat 9.0 e Fedora Core 4. Da notare che, nel caso dei sistemi operativi Linux, la versione di *nslookup* disponibile non implementa tutte le funzionalità previste per la versione Microsoft Windows; addirittura, in alcune distribuzioni, l'uso del comando nslookup è *deprecated* a beneficio di dig, il quale non è di default compreso in ambiente Windows (tranne se si effettua l'installazione del *package* BIND per Windows XP/2K/2K3/2K3-R2/Vista).

Come utilizzare nslookup

È possibile utilizzare l'applicazione *nslookup* in due modi: non-interattivo e interattivo.

Di seguito vengono presentate le due modalità.

Qualche osservazione relativa all'uso di nslookup

- *Prestare attenzione al fatto che nslookup accetta comandi solo in minuscolo.*
- *Inserendo dei comandi in maiuscolo (e.g.: SET ALL) questi vengono considerati dei nomi da risolvere.*
- *Naturalmente ci possono essere degli effetti collaterali, utilizzando il comando nslookup, se per caso esistono sulla rete degli host che si chiamano "set" o "help".*

Modo "non-interattivo"

La modalità non-interattiva è utilizzata per verificare occasionalmente (i.e.: *una-tantum*) la risoluzione di singoli nomi, mediante l'invio di un apposito comando.

La sintassi da utilizzare in tal caso è la seguente:

nslookup [-opzione] hostname [server]

Esempio di query nslookup in modalità debug (-ds) con FQDN completo (i.e.: terminato dal dominio Root DNS (punto))

```
C:\>nslookup -ds www.nic.it.
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NOERROR
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        201.0.168.192.in-addr.arpa, type = PTR, class = IN
    ANSWERS:
    ->  201.0.168.192.in-addr.arpa
        name = calajunco-2k3.isoleeolie2003.org
        ttl = 3600 (1 hour)

------------
Server:  calajunco-2k3.isoleeolie2003.org
Address:  192.168.0.201

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0
```

Da notare la query di reverse lookup scatenata in fase di avvio di nslookup (cf. la sezione "Troubleshooting nslookup", alla fine di questo capitolo).

È importante osservare che la suddetta query viene emessa solo se esiste la zona di reverse corrispondente alla subnet IP all'interno della quale ricade l'indirizzo IP del server DNS contattato.

```
QUESTIONS:
    www.nic.it, type = A, class = IN
ANSWERS:
->  www.nic.it
    internet address = 193.205.245.13
    ttl = 101 (1 min 41 secs)

------------
Non-authoritative answer:
Name:    www.nic.it
Address:  193.205.245.13
```

Esempio per il reperimento dei record MX relativi al dominio silmarconsulting.it:

nslookup -querytype=mx silmarconsulting.it. dns.seeweb.it

Modo interattivo

La modalità interattiva viene utilizzata quando è necessario effettuare una serie di verifiche e prove di funzionamento avanzate (e.g.: simulare la modalità di risoluzione dei nomi di un DNS server). In tal caso, inserendo il comando *nslookup* si entra nell'ambiente, o *shell*, dell'applicazione, caratterizzato dal prompt dei comandi identificato dal carattere ">". L'uscita dalla modalità interattiva avviene tramite il comando *exit* oppure inviando la sequenza di controllo "*Control-C*".

Esempio

```
nslookup
Default Server:    ns1.isoleeolie.org
Address:           192.168.1.250

>
```

Guida/Help

Per ottenere una guida sui comandi disponibili, digitare *help* o il carattere "*?*" dal prompt dei comandi ">" di *nslookup*:

```
> ?
Commands:              (identifiers are shown in uppercase, [] means optional)
NAME                   - print info about the host/domain NAME using default server
NAME1 NAME2            - as above, but use NAME2 as server
help or ?              - print info on common commands
set OPTION             - set an option
   all                 - print options, current server and host
   [no]debug           - print debugging information
   [no]d2              - print exhaustive debugging information
   [no]defname         - append domain name to each query
   [no]recurse         - ask for recursive answer to query
   [no]search          - use domain search list
   [no]vc              - always use a virtual circuit
   domain=NAME         - set default domain name to NAME
```

```
   srchlist=N1[/N2/.../N6]   - set domain to N1 and search list to N1,N2, etc.
   root=NAME                 - set root server to NAME
   retry=X                   - set number of retries to X
   timeout=X                 - set initial time-out interval to X seconds
   type=X                    - set query type (ex. A,ANY,CNAME,MX,NS,PTR,SOA,SRV)
   querytype=X               - same as type
   class=X                   - set query class (ex. IN (Internet), ANY)
   [no]msxfr                 - use MS fast zone transfer
   ixfrver=X                 - current version to use in IXFR transfer request
server NAME                  - set default server to NAME, using current default server
lserver NAME                 - set default server to NAME, using initial server
finger [USER]                - finger the optional NAME at the current default host
root                         - set current default server to the root
ls [opt] DOMAIN [> FILE]     - list addresses in DOMAIN (optional: output to FILE)
   -a                        -  list canonical names and aliases
   -d                        -  list all records
   -t TYPE                   -  list records of the given type (e.g. A,CNAME,MX,NS,PTR etc.)
view FILE                    - sort an 'ls' output file and view it with pg
exit                         - exit the program
```

Interpretazione delle query: query autoritative e non-autoritative

In caso di query rivolte alla risoluzione di nomi di computer remoti (i.e.: non appartenenti a nessuna delle zone per le quali il DNS server locale è autoritativo), la prima risposta sarà sempre autoritativa, mentre quelle successive saranno non-autoritative. Infatti, mentre la prima volta il DNS server locale contatta il DNS server remoto autoritativo per il RR richiesto (tramite una query ricorsiva), le volte successive che si richiederà lo stesso RR (nei limiti di valita del TTL ad esso associato) sarà il DNS server locale a rispondere non-autoritativamente, prelevando il RR dalla propria cache, nella quale era stato precedentemente inserito a seguito della prima query.

In tal caso la risposta sarà esplicitamente segnalata come "*Non-authoritative answer*".

Attenzione al "conflitto" tra cache del server e cache del client/resolver in ambiente Win2K/XP/2K3/2K3-R2/Vista

Nel caso di verifica dell'elaborazione delle query ricorsive e delle query iterative in ambiente Win2K/XP/2K3/2K3-R2/Vista, ricordarsi sempre di azzerare, oltre alla cache DNS del server (fare clic con il pulsante destro del mouse sul DNS server e selezionare la voce "Clear Cache"), anche la cache DNS del resolver/client, in uno dei due seguenti modi:

- *ipconfig –flushdns.*
- *Restart del servizio DNS Client, tramite il comando: net stop dnscache && net start dnscache.*

Configurare la modalità di debug

Per visualizzare in dettaglio i messaggi di interrogazione e di risposta che intercorrono tra un client ed un DNS server, è necessario abilitare la modalità di debug inserendo i comandi seguenti dal prompt di *nslookup*, secondo il livello di accuratezza desiderato:

- *set debug*: livello di debug base.
- *set d2*: livello di debug esaustivo o debug di livello 2.

Esempi di interrogazione e configurazione delle opzioni avanzate di nslookup

Configurando opportunamente le opzioni di *nslookup*, è possibile modificare il suo comportamento in modo tale da simulare delle query più o meno avanzate, su qualsiasi tipo di classe e di RR DNS. In particolare, è anche possibile far agire nslookup allo stesso modo di un DNS server in fase di risoluzione di query ricorsive per conto di un *resolver di tipo stub*.

Di seguito vengono mostrati alcuni esempi di utilizzo delle opzioni avanzate di *nslookup* e di invio di query. Tutti i comandi di seguito indicati devono essere inseriti dalla *shell* (i.e.: prompt dei comandi) di *nslookup*:

- Verificare le opzioni di default o configurate in un determinato istante durante l'utilizzo di *nslookup* in modalità interattiva: *set all*.
- Abilitare/disabilitare l'utilizzo della lista di ricerca (per default è sempre abilitata): *set [no]search*.
- Modificare la lista di ricerca: *set srchlist=dominio1/dominio2/..../dominioN*.

Configurazione della lista di ricerca in ambiente Win2K/2K3/2K3-R2/Vista

- *Normalmente la lista di ricerca comprende il nome del dominio di appartenenza del computer, indicato come "Primary suffix for this computer" e specificato sulla scheda Network Identification nelle proprietà di My Computer (o in Control Panel, System), più eventuali domini specificati come ulteriori domini da aggiungere in fase di risoluzione dei nomi. Ad esempio nel caso dei sistemi operativi Win2K/2K3/2K3-R2/Vista (cf. Fig. 1), nelle proprietà di una connessione TCP/IP è possibile specificare:*
  - *"DNS suffix for this connection"*
  - *"Append these DNS suffixes (in order)"*
- *La lista di ricerca non viene presa in considerazione nel caso in cui il nome da risolvere è in formato FQDN "qualificato" ovvero terminato dal "." finale (www.nic.it.).*

Configurazione della lista di ricerca in ambiente Linux/Unix

In caso di utilizzo di computer con sistema operativo Unix/Linux (e.g.: Apple Mac OS X, Red Hat, Fedora Core, Suse, Knoppix, ecc.), è possibile configurare gli indirizzi IP dei server DNS Primary, Secondary e Tertiary e i domini DNS utilizzati per la ricerca, inserendoli nel file /etc/resolv.conf.

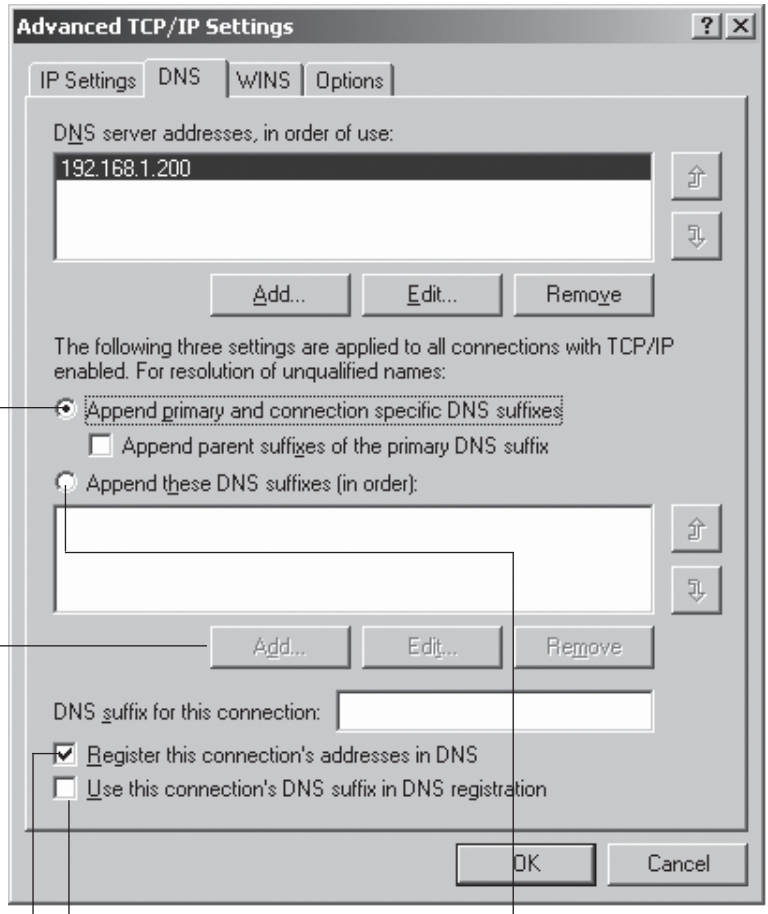
Un esempio di file resolv.conf è il seguente:

```
search        isoleeolie.org.    silmarconsulting.it
nameserver    192.168.1.200
nameserver    192.168.1.201
nameserver    192.168.1.202
```

Come evidenziato nella figura questa serie di tre opzioni servono per istruire il DNS Client/Resolver su come agire per gestire la risoluzione di nomi DNS non "qualificati" (i.e.: nomi o FQDN non terminati dal "."). Per default il nome non qualificato viene completato con il suffisso primario specificato nella scheda Identification (nel caso di Win2K) o Computer Name (nel caso di WinXP/2003) e con il suffisso specifico di questa connessione se indicato nel campo "DNS suffix for this connection" seguente. Selezionando la successiva casella "Append parent suffixes of primary DNS suffix" vengono aggiunti anche i suffissi parziali presenti nel suffisso primario fino al secondo livello (e.g.: se il suffisso primario è lipari.isoleeolie.org verrà aggiunto prima il suffisso lipari.isoleeolie.org e poi isoleeolie.org).

Permette di specificare un suffisso DNS specifico per questa connessione di rete. In caso di client DHCP, viene presa in considerazione l'opzione configurata a livello di server DHCP nel caso il campo sia vuoto. Viceversa assume priorità il valore specificato localmente (come sempre).

Specifica che il computer deve tentare la registrazione dinamica del proprio indirizzo IP e del nome completo del computer, come indicato in Control Panel, System, Network Identification, puntando al server DNS locale.



Se abilitata la registrazione dinamica (casella superiore) è possibile forzare una doppia registrazione (RR A e PTR) oltre che in base al suffisso primario specificato nella scheda Identification (nel caso di Win2K) o Computer Name (nel caso di WinXP/2003) anche utilizzando il suffisso specifico di questa connessione indicato nel campo "DNS suffix for this connection".

Consente di specifica una lista di suffissi DNS da utilizzare per la risoluzione di nomi DNS "non qualificati" (i.e.: FQDN non terminati con il "."). Selezionando questa opzione non viene preso in considerazione nè il suffisso primario nè quello specifico alla connessione.

Figura 6.1 Configurazioni avanzate DNS/DDNS

- Selezionare una porta UDP/TCP diversa da quella default (53):
  set port=xx: dove xx deve coincidere con la porta specificata sul server DNS. Per default è 53.

- Selezionare il tipo di RR da ricercare:
  set q=<queryType-del-RR> oppure set type=<tipo-di-RR>: dove <*tipo-di-RR*> può essere SOA, A, MX, CNAME, SRV, ecc.
  Di default viene utilizzato il tipo di RR A e l'abbreviazione q al posto di *querytype*.

- Selezionare una classe di RR da ricercare:

  set class=<IN | Hesiod | Chaos | Any>.

  IN=Internet è la classe di default; ANY considera tutte le classi.
- Selezionare un DNS server diverso da quello di default:

  server <indirizzo-IP> oppure *server <Nome-Server>*.
- Selezionare un dominio DNS server diverso da quello di default, se esistente (e.g.: computer con sistema operativo Windows XP/2K/2K3/2K3-R2/Vista, appartenente ad un dominio Active Directory):

  set domain=<nomeDominio>.

  Esempio: set domain=isoleeolie2003.org.

  Così facendo, eventuali nomi FQDN "non-ben-qualificati" verranno completati con il suffisso specificato con la precedente direttiva.
- Simulare il funzionamento di un server DNS, tracciando i vari passi di risoluzione tra vari server DNS seguendo un percorso iterativo, a partire dai server DNS di root Internet:
  - Dopo aver lanciato il comando *nslookup*, posizionarsi su uno dei tredici server DNS di root di Internet (e.g.: a.root-servers.net.). Da notare che inserendo il comando *set all* dal prompt di *nslookup* viene visualizzato il nome del server DNS di root di riferimento.
  - *set norecurse*: disabilita la ricorsione e forza *nslookup* ad inviare query di tipo iterative.
  - *set nosearch*: disabilita l'utilizzo da parte del resolver della "search list". Ciò è necessario, in quanto un DNS server, contrariamente ad un resolver DNS, non utilizza la funzione "lista suffissi di ricerca".
  - *<inserire il nome host da risolvere>* seguito da INVIO.
  - Selezionare il primo server DNS della lista dei DNS autoritativi per il nome richiesto ed impostarlo come server di default tramite il comando seguente:

    server <nome server DNS autoritativo scelto>
  - Ripetere la query iniziale: *<inserire il nome host da risolvere>* seguito da INVIO.
  - Continuare fino ad arrivare all'ultimo server DNS autoritativo per l'hostname ricercato il quale, finalmente, risolverà la query iniziale.
- Forzare un'operazione di *Full Zone Transfer*:

  Dopo aver identificato il server DNS autoritativo per il dominio/zona in questione (e.g.:), è possibile eseguire il seguente comando:

  > *ls –d <FQDN-Dominio/Zona>*

  È da notare che l'esito del suddetto comando dipende dalla configurazione della zona DNS. Infatti, esso richiede l'autorizzazione allo *Zone Transfer* verso un prefissato insieme di indirizzi IP oppure verso tutti gli host (deprecabile a livello di sicurezza).
- Determinare la versione di BIND utilizzata su un server UNIX/Linux remoto, tramite delle query *nslookup*. Dal prompt di *nslookup* (modalità interattiva) inserire la seguente sequenza di comandi (attenzione: il risultato non sempre è garantito, in quanto il RR corrispondente può essere stato anche modificato dall'amministratore del DNS BIND remoto).

  > *server 193.205.245.5*

  > *set class=chaos*

```
> set type=txt
> version.bind
Risposta:
version.bind    text =
"9.3.1"
version.bind    nameserver = version.bind
>
```

Query DNS "qualificate" e "non-qualificate"

Utilizzando *nslookup* come client DNS per simulare l'invio di query ad uno o più DNS server, è possibile notare dei comportamenti diversi a seconda della configurazione del client/resolver (e.g.: lista dei domini DNS da accodare ad un nome host in fase di risoluzione (*search list*)) e, soprattutto, del tipo di nome utilizzato:

- Nome host (e.g.: panarea).
- Nome FQDN "non-qualificato" o "non-ben-formato", ovvero non terminato dal dominio root indicato dal carattere "." (e.g.: panarea.isoleeolie.org).
- Nome FQDN "qualificato o ben-formato" o "completo", ovvero terminato dal dominio root (e.g.: panarea.isoleeolie.org.) come nel caso del *path assoluto* di un file all'interno di un *File System* (e.g.: /etc/services oppure c:\windows\system32\drivers\etc\services).

A tal proposito è possibile verificare quanto detto, utilizzando *nslookup* e inviando due query, una con FQDN non qualificato ed una con FQDN qualificato. Negli esempi sotto riportati, la lista di ricerca impostata per il client DNS è costituita da isoleeolie2003.org.

Esempio di query con FQDN incompleto (non terminato dal punto finale)

```
C:\>nslookup -ds www.nic.it

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 1, rcode = NOERROR
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 0,  additional = 0

    QUESTIONS:
        201.0.168.192.in-addr.arpa, type = PTR, class = IN
    ANSWERS:
    ->  201.0.168.192.in-addr.arpa
        name = calajunco-2k3.isoleeolie2003.org
        ttl = 1200 (20 mins)
```

```
------------
Server:  calajunco-2k3.isoleeolie2003.org
Address:  192.168.0.201

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NXDOMAIN
        header flags:  response, auth. answer, want recursion, recursion avail.
        questions = 1,  answers = 0,  authority records = 1,  additional = 0

    QUESTIONS:
        www.nic.it.isoleeolie2003.org, type = A, class = IN
    AUTHORITY RECORDS:
    ->  isoleeolie2003.org
        ttl = 3600 (1 hour)
        primary name server = calajunco-2k3.isoleeolie2003.org
        responsible mail addr = leoner.isoleeolie2003.org
        serial  = 36
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)

------------
------------
Got answer:
    HEADER:
        opcode = QUERY, id = 3, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 4,  additional = 5

    QUESTIONS:
        www.nic.it, type = A, class = IN
    ANSWERS:
    ->  www.nic.it
        internet address = 193.205.245.13
        ttl = 120 (2 mins)
    AUTHORITY RECORDS:
    ->  nic.it
        nameserver = itgeo.mix-it.net
        ttl = 78899 (21 hours 54 mins 59 secs)
    ->  nic.it
        nameserver = nameserver.cnr.it
        ttl = 78899 (21 hours 54 mins 59 secs)
```

```
   ->  nic.it
       nameserver = DNS.nic.it
       ttl = 78899 (21 hours 54 mins 59 secs)
   ->  nic.it
       nameserver = dns2.nic.it
       ttl = 78899 (21 hours 54 mins 59 secs)
   ADDITIONAL RECORDS:
   ->  DNS.nic.it
       internet address = 193.205.245.5
       ttl = 78899 (21 hours 54 mins 59 secs)
   ->  DNS.nic.it
       AAAA IPv6 address = 2001:760:4000:1f5::5
       ttl = 11596 (3 hours 13 mins 16 secs)
   ->  dns2.nic.it
       internet address = 193.205.245.8
       ttl = 78895 (21 hours 54 mins 55 secs)
   ->  itgeo.mix-it.net
       internet address = 217.29.76.5
       ttl = 78902 (21 hours 55 mins 2 secs)
   ->  nameserver.cnr.it
       internet address = 194.119.192.34
       ttl = 78893 (21 hours 54 mins 53 secs)

------------
Non-authoritative answer:
Name:    www.nic.it
Address:  193.205.245.13
```

Esempio di query con FQDN completo (i.e.: terminato con il punto finale)

```
Got answer:
   HEADER:
       opcode = QUERY, id = 1, rcode = NOERROR
       header flags:  response, auth. answer, want recursion, recursion avail.
       questions = 1,  answers = 1,  authority records = 0,  additional = 0

   QUESTIONS:
       201.0.168.192.in-addr.arpa, type = PTR, class = IN
   ANSWERS:
   ->  201.0.168.192.in-addr.arpa
       name = calajunco-2k3.isoleeolie2003.org
       ttl = 1200 (20 mins)
```

```
------------
Server:  calajunco-2k3.isoleeolie2003.org
Address:  192.168.0.201

------------
Got answer:
    HEADER:
        opcode = QUERY, id = 2, rcode = NOERROR
        header flags:  response, want recursion, recursion avail.
        questions = 1,  answers = 1,  authority records = 4,  additional = 5

    QUESTIONS:
        www.nic.it, type = A, class = IN
    ANSWERS:
    ->  www.nic.it
        internet address = 193.205.245.13
        ttl = 120 (2 mins)
    AUTHORITY RECORDS:
    ->  nic.it
        nameserver = nameserver.cnr.it
        ttl = 76074 (21 hours 7 mins 54 secs)
    ->  nic.it
        nameserver = DNS.nic.it
        ttl = 76074 (21 hours 7 mins 54 secs)
    ->  nic.it
        nameserver = dns2.nic.it
        ttl = 76074 (21 hours 7 mins 54 secs)
    ->  nic.it
        nameserver = itgeo.mix-it.net
        ttl = 76074 (21 hours 7 mins 54 secs)
    ADDITIONAL RECORDS:
    ->  DNS.nic.it
        internet address = 193.205.245.5
        ttl = 76074 (21 hours 7 mins 54 secs)
    ->  DNS.nic.it
        AAAA IPv6 address = 2001:760:4000:1f5::5
        ttl = 8771 (2 hours 26 mins 11 secs)
    ->  dns2.nic.it
        internet address = 193.205.245.8
        ttl = 76070 (21 hours 7 mins 50 secs)
    ->  itgeo.mix-it.net
        internet address = 217.29.76.5
        ttl = 76077 (21 hours 7 mins 57 secs)
    ->  nameserver.cnr.it
        internet address = 194.119.192.34
        ttl = 76068 (21 hours 7 mins 48 secs)
```

Come si può notare, nel primo caso *nslookup* esegue un tentativo di ricerca componendo un FQDN completo, composto dal FQDN "non-ben-formato" passato come argomento e completato di volta in volta con uno dei domini che compongono la lista dei suffissi DNS di ricerca configurati sul computer utilizzato. Viceversa, nel secondo caso, essendo il nome da ricercare già in formato FQDN completo, il client nslookup invia una sola query.

Troubleshooting nslookup

- Lanciando *nslookup* in modalità interattiva, viene visualizzato il seguente messaggio:

  Default Server: localhost

  Address: 127.0.0.1

  >

  Oppure quest'altro:

  *** Default servers are not available

  Default Server: UnKnown

  Address: 127.0.0.1

  >

  Causa: nel primo caso è stato indicato (probabilmente forzato dal sistema operativo) come indirizzo IP del server DNS quello di loopback o localhosts (127.0.0.1). Nel secondo caso, invece, è probabile che il computer non sia ancora stato configurato con nessun indirizzo IP, nè proprio nè del server DNS. Ciò può verificarsi per un computer configurato come DHCP client, in attesa di ricevere un indirizzo IP dal DHCP server.
- Lanciando *nslookup* in modalità interattiva, viene visualizzato il seguente messaggio di errore:

  *** Can't find server name for address 192.168.1.200: Non-existent domain

  *** Default servers are not available

  Default Server: UnKnown

  Address: 192.168.1.200

  Causa: in fase di avvio il comando *nslookup* invia una query di tipo reverse al proprio server DNS locale, allo scopo di risalire dall'indirizzo IP del server, indicato nella configurazione IP del computer, al nome.

  Probabili cause del problema possono essere:

  - Non è stata creata la zona di reverse per la subnet IP di cui fa parte il server DNS (e.g.: 1.168.192.in-addr.arpa).
  - La zona di reverse è stata creata, ma non esiste il RR PTR corrispondente al server DNS locale.
- Lanciando *nslookup* in modalità interattiva, viene visualizzato il seguente messaggio in seguito all'inserimento di un comando *set* (e.g.: per configurare delle query di tipo MX o visualizzare le opzioni di configurazione):

  *** Can't find address for server TYPE=MX: Timed out

  oppure:

  *** Can't find address for server ALL: Timed out

  Causa: il comando è stato inserito in maiuscolo mentre nslookup accetta solo comandi in minuscolo.

Dig

Dig (il cui nome deriva dal verbo inglese *to dig*, scavare, scoprire o investigare) è una *utility* presente in qualsiasi sistema operativo all'interno del quale è installato l'ambiente DNS BIND; pertanto essa è disponibile nativamente in ambiente Linux/Unix. Contrariamente a *nslookup*, *dig* non contempla una modalità interattiva, ma è disponibile solamente in modalità non interattiva o batch.

Utilizzare dig e host in ambito Windows

Per disporre in ambito Windows delle utility dig e host è necessario scaricare dal sito http://www.isc.org il package BIND (e.g.: http://ftp.isc.org/isc/bind/contrib/ntbind-9.3.2/BIND9.3.2.zip) e procedere con l'estrazione dei file in una directory (e.g.: c:\bind9.3.2).

Alcuni esempi di utilizzo della utility *dig* sono mostrati di seguito.

Alcuni esempi di utilizzo dell'utility dig

- Help (sintassi del comando *dig*):

  dig –h

  Esempio:

  c:\etc\dig -h

```
Usage:  dig [@global-server] [domain] [q-type] [q-class] {q-opt}
        {global-d-opt} host [@local-server] {local-d-opt}
        [ host [@local-server] {local-d-opt} [...]]
Where:  domain              is in the Domain Name System
    q-class                 is one of (in,hs,ch,...) [default: in]
    q-type                  is one of (a,any,mx,ns,soa,hinfo,axfr,txt,...) [default:a]
        (Use ixfr=version for type ixfr)
    q-opt                   is one of:
        -x dot-notation     (shortcut for in-addr lookups)
        -i                  (IP6.INT reverse IPv6 lookups)
        -f filename         (batch mode)
        -b address[#port]   (bind to source address/port)
        -p port             (specify port number)
        -t type             (specify query type)
        -c class            (specify query class)
        -k keyfile          (specify tsig key file)
        -y name:key         (specify named base64 tsig key)
        -4                  (use IPv4 query transport only)
        -6                  (use IPv6 query transport only)
    d-opt                   is of the form +keyword[=value], where keyword is:
```

+[no]vc	*(TCP mode)*
+[no]tcp	*(TCP mode, alternate syntax)*
+time=###	*(Set query timeout) [5]*
+tries=###	*(Set number of UDP attempts) [3]*
+retry=###	*(Set number of UDP retries) [2]*
+domain=###	*(Set default domainname)*
+bufsize=###	*(Set EDNS0 Max UDP packet size)*
+ndots=###	*(Set NDOTS value)*
+[no]search	*(Set whether to use searchlist)*
+[no]defname	*(Ditto)*
+[no]recurse	*(Recursive mode)*
+[no]ignore	*(Don't revert to TCP for TC responses.)*
+[no]fail	*(Don't try next server on SERVFAIL)*
+[no]besteffort	*(Try to parse even illegal messages)*
+[no]aaonly	*(Set AA flag in query (+[no]aaflag))*
+[no]adflag	*(Set AD flag in query)*
+[no]cdflag	*(Set CD flag in query)*
+[no]cl	*(Control display of class in records)*
+[no]cmd	*(Control display of command line)*
+[no]comments	*(Control display of comment lines)*
+[no]question	*(Control display of question)*
+[no]answer	*(Control display of answer)*
+[no]authority	*(Control display of authority)*
+[no]additional	*(Control display of additional)*
+[no]stats	*(Control display of statistics)*
+[no]short	*(Disable everything except short form of answer)*
+[no]ttlid	*(Control display of ttls in records)*
+[no]all	*(Set or clear all display flags)*
+[no]qr	*(Print question before sending)*
+[no]nssearch	*(Search all authoritative nameservers)*
+[no]identify	*(ID responders in short answers)*
+[no]trace	*(Trace delegation down from root)*
+[no]dnssec	*(Request DNSSEC records)*
+[no]multiline	*(Print records in an expanded format)*
global d-opts and servers	*(before host name) affect all queries.*
local d-opts and servers	*(after host name) affect only that lookup.*
-h	*(print help and exit)*
-v	*(print versi*on and exit)

- Numero di versione della utility *dig*:
  dig –v
  Esempio:
  c:\etc\dig -v
  DiG 9.3.2

- Come determinare la versione di un server DNS BIND (naturalmente, come già detto a proposito del comando *nslookup*, l'esito di questo comando dipende dalla configurazione del server BIND e dalla possibilità che l'amministratore abbia o meno filtrato tale risposta):
  dig @<indirizzo-IP-server-DNS> txt chaos version.bind
  Esempio:
  - c:\etc\dig @193.205.245.5 chaos txt version.bind
  Oppure:
  - c:\etc\dig @193.205.245.5 txt chaos version.bind

  ; <<>> DiG 9.3.2 <<>> @193.205.245.5 txt chaos version.bind
  ; (1 server found)
  ;; global options: printcmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1003
  ;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 0

  ;; QUESTION SECTION:
  ;version.bind. CH TXT

  ;; ANSWER SECTION:
  version.bind. 0 CH TXT "9.3.1"

  ;; AUTHORITY SECTION:
  version.bind. 0 CH NS version.bind.

  ;; Query time: 15 msec
  ;; SERVER: 193.205.245.5#53(193.205.245.5)
  ;; WHEN: Sun Feb 05 15:03:51 2006
  ;; MSG SIZE rcvd: 62

- Query di reverse (i.e.: a partire da un indirizzo IP risalire al nome di un host):
  dig @<indirizzo-IP-server-DNS> -x <indirizzo-IP-oggetto-della-query>
  Esempio:
  c:\etc\ dig @dns.nic.it -x 193.205.245.15
  ; <<>> DiG 9.3.2 <<>> @dns.nic.it -x 193.205.245.15

; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1537
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;15.245.205.193.in-addr.arpa. IN PTR

;; ANSWER SECTION:
15.245.205.193.in-addr.arpa. 3600 IN PTR hp4550.nic.it.

;; AUTHORITY SECTION:
245.205.193.in-addr.arpa. 432000 IN NS dns.nic.it.
245.205.193.in-addr.arpa. 432000 IN NS nameserver.cnr.it.

;; ADDITIONAL SECTION:
dns.nic.it. 86400 IN A 193.205.245.5
dns.nic.it. 86400 IN AAAA 2001:760:4000:1f5::5
nameserver.cnr.it. 72368 IN A 194.119.192.34

;; Query time: 187 msec
;; SERVER: 193.205.245.5#53(193.205.245.5)
;; WHEN: Sun Feb 05 19:11:33 2006
;; MSG SIZE rcvd: 179

- Query multiple: elencare tutti i RR contenuti in due zone/domini gestite da un server DNS/BIND:
  dig @<indirizzo-IP-server-DNS> <FQDN-dominio> -t <any> <FQDN-dominio> -t <any>
  Esempio:
  C:\dig>dig @212.25.160.10 learning-solutions.it -t any silmarconsulting.it -t any
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1776
  ;; flags: qr aa rd; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 15

  ;; QUESTION SECTION:
  ;learning-solutions.it. IN ANY

  ;; ANSWER SECTION:
  learning-solutions.it. 172800 IN SOA dns.seeweb.it. hostmaster.seeweb.it. 2005030300 86400 7200 2592000 86400

```
learning-solutions.it.  172800  IN     NS     dns2.seeweb.it.
learning-solutions.it.  172800  IN     NS     dns.seeweb.it.
learning-solutions.it.  172800  IN     MX     10 wnx-5b.seeweb.it.
learning-solutions.it.  172800  IN     MX     20 smtp-f1.seeweb.it.
learning-solutions.it.  172800  IN     MX     20 smtp-f2.seeweb.it.
learning-solutions.it.  172800  IN     MX     20 smtp-f3.seeweb.it.
learning-solutions.it.  172800  IN     MX     20 smtp-f4.seeweb.it.

;; ADDITIONAL SECTION:
dns.seeweb.it.        172800  IN     A      212.25.160.10
dns2.seeweb.it.       172800  IN     A      217.64.196.10
wnx-5b.seeweb.it.     172800  IN     A      212.25.179.6
smtp-f1.seeweb.it.    172800  IN     A      212.25.179.65
smtp-f1.seeweb.it.    172800  IN     A      212.25.179.69
smtp-f1.seeweb.it.    172800  IN     A      212.25.179.73
smtp-f2.seeweb.it.    172800  IN     A      212.25.179.74
smtp-f2.seeweb.it.    172800  IN     A      212.25.179.66
smtp-f2.seeweb.it.    172800  IN     A      212.25.179.70
smtp-f3.seeweb.it.    172800  IN     A      212.25.179.71
smtp-f3.seeweb.it.    172800  IN     A      212.25.179.75
smtp-f3.seeweb.it.    172800  IN     A      212.25.179.67
smtp-f4.seeweb.it.    172800  IN     A      212.25.179.76
smtp-f4.seeweb.it.    172800  IN     A      212.25.179.68
smtp-f4.seeweb.it.    172800  IN     A      212.25.179.72

;; Query time: 406 msec
;; SERVER: 212.25.160.10#53(212.25.160.10)
;; WHEN: Sun Feb 05 15:49:41 2006
;; MSG SIZE  rcvd: 489

; <<>> DiG 9.3.2 <<>> @212.25.160.10 learning-solutions.it -t any silmarconsulting.it -t any
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1563
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;silmarconsulting.it.          IN     ANY
```

;; ANSWER SECTION:

silmarconsulting.it. 172800 IN SOA dns.seeweb.it. hostmaster.seeweb.it. 2002112100 86400 7200 2592000 86400

silmarconsulting.it. 172800 IN NS dns.seeweb.it.

silmarconsulting.it. 172800 IN NS dns2.nic.it.

silmarconsulting.it. 172800 IN MX 10 mail.silmarconsulting.it.

;; ADDITIONAL SECTION:

dns.seeweb.it. 172800 IN A 212.25.160.10

mail.silmarconsulting.it. 172800 IN A 212.25.170.113

;; Query time: 250 msec

;; SERVER: 212.25.160.10#53(212.25.160.10)

;; WHEN: Sun Feb 05 15:49:41 2006

;; MSG SIZE rcvd: 185

■ Interpretazione dell'*output* del comando *dig*:

Il formato dell'*output* del comando *dig* prevede cinque parti o sezioni:

- Sezioni *Flags* e *Status*:

  In questa prima parte dell'*output* sono visualizzate alcune informazioni riguardanti i *flag* e lo *status* relativo al tipo di risposta ottenuta.

  Alcuni parametri utilizzati dal comando *dig* sono i seguenti:

  - *Flags*: qr (*Query/Response*); aa (*Authoritative Answer*); rd (*Recursion Desidered*); ra (*Recursion Available*); ad (*Authenticated Data*); cd (*Checking Disabled*); ds (*DNSSEC OK*).
  - *Status*: NOERR (*No Error Condition*); FORMERR (*Format Error*: il server DNS non è stato in grado di interpretare la query a causa di un errore nel suo formato); SERVFAIL (*Server Failure*: il server DNS non è stato in grado di interpretare la query; ciò può accadere o per problemi con il server o perché il nome richiesto non è un FQDN "ben-formato" (e.g.: è stato inviato solamente il nome host senza nessun suffisso DNS) oppure a causa di funzionalità non disponibili (e.g.: una query ricorsiva rivolta ad un server sul quale questo tipo di query sono state disabilitate); NXDOMAIN (*Non eXistent Domain*: segnala che il nome DNS o il suffisso specificato nella query è ineesistente); NOTIMP (*Not Implemented* (per le versioni BIND precedenti alla 9.3 il codice di errore potrebbe essere NOTIMPL): il server DNS non supporta l'operazione richiesta); REFUSED (il server DNS rifiuta le operazioni richieste (e.g.: una richiesta di *Full Zone Transfer* (AXFR))); YXDOMAIN (il server DNS segnala che il nome di dominio esiste quando invece non dovrebbe (cf. RFC 2136)); YXRRSet (il server DNS segnala che il RR esiste quando invece non dovrebbe (cf. RFC 2136)); NXRRSet (il server DNS segnala che il RR che dovrebbe esistere invece non è stato trovato (cf. RFC 2136)); NotAuth (il server DNS non è autoritativo per la zona in questione (cf. RFC 2136)); NotZone (il server DNS segnala che il nome cercato non appartiene alla zona in questione (cf. RFC 2136)).

Per ulteriori informazioni sui suddetti codici di errore si rimanda il lettore al Capitolo 5, sezione "Struttura della sezione *Header*" di una PDU DNS (cf. anche la tabella 5.14, sempre nel Capitolo 5).

- Sezione *Question* (*query* o interrogazione): contiene la richiesta inoltrata al server DNS.
- Sezione *Answer* (risposta): contiene le risposte alla query.
- Sezione *Authority* (risposta): contiene la lista dei server DNS autoritativi per la zona/dominio considerato.
- Sezione *Additional* (risposta): contiene eventuali informazioni addizionali importanti per completare la risoluzione desiderata (e.g.: i RR A relativi ad altri server DNS autoritativi per i RR richiesti). Ciò accade, ad esempio, nel caso di invio della query *dig @193.205.245.5 learning-solutions.it any*. Infatti, non essendo il server DNS 193.205.245.5 autoritativo per la zona *learning-solutions.it*, il comando *dig* fornisce i FQDN ed i relativi RR A per identificare univocamente i server DNS autoritativi per il dominio *learning-solutions.it*.
- Sezione *Question* (*query* o interrogazione): contiene la richiesta inoltrata al server DNS.

■ Forzare un'operazione di *Full Zone Transfer*:

dig @<indirizzo-IP-server-DNS> <FQDN-dominio> axfr

Esempio:

C:\dig>dig @192.168.0.201 isoleeolie2003.org. axfr

; <<>> DiG 9.3.2 <<>> @192.168.0.201 isoleeolie2003.org. axfr

; (1 server found)

;; global options: printcmd

isoleeolie2003.org. 3600 IN SOA calajunco-2k3.isoleeolie2003.org. leoner.isoleeolie2003.org. 47 900 600 86400 3600

isoleeolie2003.org. 600 IN A 192.168.0.230

isoleeolie2003.org. 3600 IN NS calajunco-2k3.isoleeolie2003.org.

_kerberos._tcp.default-first-site-name._sites.dc._msdcs.isoleeolie2003.org. 600 IN SRV 0 100 88 ie-mi-dc-01.isoleeolie2003.org.

_ldap._tcp.default-first-site-name._sites.dc._msdcs.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

_kerberos._tcp.dc._msdcs.isoleeolie2003.org. 600 IN SRV 0 100 88 ie-mi-dc-01.isoleeolie2003.org.

_ldap._tcp.dc._msdcs.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

_ldap._tcp.56a8a918-d321-46bc-881d-cc58bf0e6f9b.domains._msdcs.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

e886b836-966c-4e26-8eb6-bdec708da42b._msdcs.isoleeolie2003.org. 600 IN CNAME ie-mi-dc-01.isoleeolie2003.org.

gc._msdcs.isoleeolie2003.org. 600 IN A 192.168.0.230

_ldap._tcp.default-first-site-name._sites.gc._msdcs.isoleeolie2003.org. 600 IN SRV 0 100 3268 ie-mi-dc-01.isoleeolie2003.org.

_ldap._tcp.gc._msdcs.isoleeolie2003.org. 600 IN SRV 0 100 3268 ie-mi-dc-01.isoleeolie2003.org.

_ldap._tcp.pdc._msdcs.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

_gc._tcp.default-first-site-name._sites.isoleeolie2003.org. 600 IN SRV 0 100 3268 ie-mi-dc-01.isoleeolie2003.org.

_kerberos._tcp.default-first-site-name._sites.isoleeolie2003.org. 600 IN SRV 0 100 88 ie-mi-dc-01.isoleeolie2003.org.

_ldap._tcp.default-first-site-name._sites.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

_gc._tcp.isoleeolie2003.org. 600 IN SRV 0 100 3268 ie-mi-dc-01.isoleeolie2003.org.

_kerberos._tcp.isoleeolie2003.org. 600 IN SRV 0 100 88 ie-mi-dc-01.isoleeolie2003.org.

_kpasswd._tcp.isoleeolie2003.org. 600 IN SRV 0 100 464 ie-mi-dc-01.isoleeolie2003.org.

_ldap._tcp.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

_kerberos._udp.isoleeolie2003.org. 600 IN SRV 0 100 88 ie-mi-dc-01.isoleeolie2003.org.

_kpasswd._udp.isoleeolie2003.org. 600 IN SRV 0 100 464 ie-mi-dc-01.isoleeolie2003.org.

calajunco-2k3.isoleeolie2003.org. 3600 IN A 192.168.193.1

calajunco-2k3.isoleeolie2003.org. 3600 IN A 192.168.93.1

calajunco-2k3.isoleeolie2003.org. 3600 IN A 192.168.0.201

domaindnszones.isoleeolie2003.org. 600 IN A 192.168.0.230

_ldap._tcp.default-first-site-name._sites.domaindnszones.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

_ldap._tcp.domaindnszones.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

forestdnszones.isoleeolie2003.org. 600 IN A 192.168.0.230

_ldap._tcp.default-first-site-name._sites.forestdnszones.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

_ldap._tcp.forestdnszones.isoleeolie2003.org. 600 IN SRV 0 100 389 ie-mi-dc-01.isoleeolie2003.org.

ftp.isoleeolie2003.org. 3600 IN CNAME www.isoleeolie2003.org.

www.isoleeolie2003.org. 3600 IN A 192.168.0.200

isoleeolie2003.org. 3600 IN SOA calajunco-2k3.isoleeolie2003.org. leoner.isoleeolie2003.org. 47 900 600 86400 3600

;; Query time: 515 msec

;; SERVER: 192.168.0.201#53(192.168.0.201)

;; WHEN: Sun Feb 05 19:23:24 2006

;; XFR size: 34 records (messages 34)

È da notare che l'esito del suddetto comando dipende dalla configurazione della zona DNS. Infatti, esso richiede l'autorizzazione allo *Zone Transfer* verso un prefissato insieme di indirizzi IP oppure verso tutti gli host (deprecabile a livello di sicurezza).

- Forzare un'operazione di *Full Zone Transfer* in presenza di un'implementazione TSIG per la crittografia delle operazioni di *Zone Transfer*:
  dig @192.168.0.201 guidadns.it AXFR –k Kdns1-dns2.+157+19475.private
  dove *Kdns1-dns2.+157+19475.private* rappresenta il file che contiene la chiave condivisa utilizzata per la crittografia.
- Rilevare i RR MX (i.e.: i server SMTP) per un determinato dominio:
  dig @<indirizzo-IP-server-DNS> <FQDN-dominio> -t mx
  Esempio:
  C:\dig>dig @212.25.160.10 silmarconsulting.it -t mx

  ; <<>> DiG 9.3.2 <<>> @212.25.160.10 silmarconsulting.it -t mx
  ; (1 server found)
  ;; global options: printcmd
  ;; Got answer:
  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1369
  ;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

  ;; QUESTION SECTION:
  ;silmarconsulting.it. IN MX

  ;; ANSWER SECTION:
  silmarconsulting.it. 172800 IN MX 10 mail.silmarconsulting.it.

  ;; AUTHORITY SECTION:
  silmarconsulting.it. 172800 IN NS dns.seeweb.it.
  silmarconsulting.it. 172800 IN NS dns2.nic.it.

  ;; ADDITIONAL SECTION:
  mail.silmarconsulting.it. 172800 IN A 212.25.170.113
  dns.seeweb.it. 172800 IN A 212.25.160.10

  ;; Query time: 281 msec
  ;; SERVER: 212.25.160.10#53(212.25.160.10)
  ;; WHEN: Sun Feb 05 15:55:53 2006
  ;; MSG SIZE rcvd: 138
- Identificare il server DNS primario per una data zona/dominio, tramite rilevazione del RR SOA:
  dig @<indirizzo-IP-server-DNS> <FQDN-dominio> -t soa

Esempio:

```
C:\dig>dig @193.205.245.66 nic.it soa

; <<>> DiG 9.3.2 <<>> @193.205.245.66 nic.it soa
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 148
;; flags: qr rd; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 2

;; QUESTION SECTION:
;nic.it.                        IN      SOA

;; ANSWER SECTION:
nic.it.         84078   IN      SOA     dns.nic.it. hostmaster.nic.it. 2006011900 86400 1800
604800 86400

;; AUTHORITY SECTION:
nic.it.         84298   IN      NS      dns2.nic.it.
nic.it.         84298   IN      NS      itgeo.mix-it.net.
nic.it.         84298   IN      NS      nameserver.cnr.it.
nic.it.         84298   IN      NS      dns.nic.it.

;; ADDITIONAL SECTION:
itgeo.mix-it.net.       521     IN      A       217.29.76.5
nameserver.cnr.it.      86400   IN      A       194.119.192.34

;; Query time: 265 msec
;; SERVER: 193.205.245.66#53(193.205.245.66)
;; WHEN: Tue Feb 07 11:16:33 2006
;; MSG SIZE  rcvd: 199
```

http://www.DNSstuff.com: un concentrato di strumenti diagnostici

DNSstuff è un sito contenente una grande varietà di strumenti utili per scopi diagnostici, analisi e test. Essi sono organizzati in quattro categorie:

- *Domain Name Test: DNS Report, DNS Timing, WHOIS Lookup, Abuse Lookup, Domain Info.*
- *IP Test: Spam database lookup, Reverse DNS lookup, IPWHOIS Lookup, City From IP.*
- *Hostname Test: DNS lookup, Traceroute, Ping, ISP cached DNS lookup.*

- *Other Tests: URL deobfuscator, Free E-mail Lookup, CIDR/Netmask, E-mail Test, CSE HTML Validator, Decimal IPs.*

Alla URL seguente: https://addons.mozilla.org/extensions/moreinfo.php?application=firefox&id=827 è disponibile anche l'add-on per Firefox (DNSStuff Toolbar – Firefox Extension).

Verificare la congruenza tra le informazioni relative ai server DNS registrate nel database Whois ed i server DNS presenti nella zona delegata

È importante accertarsi che vi sia sempre corrispondenza tra le coordinate dei server DNS autoritativi per un dato nome a dominio (e.g.: guidadns.it), che risultano registrati nel database Whois del Registro competente (e.g.: whois.nic.it, per il ccTLD ".it.") ed i server DNS presenti nella zona delegata corrispondente al dominio stesso.

Nel caso del Registro italiano del ccTLD ".it." è possibile effettuare un "controllo di integrità referenziale" tramite il servizio messo a disposizione alla URL seguente: http://www.nic.it/PM/nscheck.html.