

Appendice C

Client Whois per sistema operativo Windows

Descrizione

Il client Whois per Windows è un'implementazione del protocollo Whois standard RFC 3912, “*Whois Protocol Specification*” (e precedenti RFC 812 e 954, “*NICNAME/WHOIS*”), da utilizzare a riga di comando. Da notare che per l'ambiente Windows, contrariamente ai sistemi operativi Unix/Linux, non è disponibile nativamente un client Whois.

Essa è stata realizzata con l'eccezionale contributo dell'amico e collega Alessandro Pilotti in ambiente Visual Studio 2005 e richiede il run-time del *Framework 2.0 .NET* di Microsoft, scaricabile gratuitamente dal sito Microsoft alla URL sotto indicata:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0856eacb-4362-4b0d-8edd-aab15c5e04f5&DisplayLang=en> (per la versione in inglese).

L'utilizzo del client Whois richiede la disponibilità delle porte TCP/43 e UDP/43, anche se di default viene preferita una connessione di tipo TCP.



Verificare la disponibilità dell'accesso ai server Whois (porta 43 TCP/UDP)

Per testare l'accessibilità ad un server Whois (e.g.: whois.nic.it), in caso di connessione a Internet mediata da un Proxy o NAT e/o filtrata da un Firewall, è sufficiente utilizzare il comando telnet verso il server Whois specificando la porta 43:

```
telnet whois.nic.it 43
```

A questo punto è possibile anche inviare una query di test (e.g.: learning-solutions.it) sempre attraverso l'interfaccia telnet.

Da notare che non tutti i server Whois sono capaci di restituire un output correttamente formattato e leggibile in seguito ad una query eseguita tramite una connessione telnet. Viceversa, un server Whois che restituisce l'output correttamente visualizzato è quello del NIC della Lituania: whois.domreg.lt.

In questo caso, dopo aver effettuato la connessione al server Whois tramite il comando:

```
telnet whois.domreg.lt 43
```

e, non appena compare il cursore lampeggiante in alto a sinistra, digitare la query; ad esempio:
domreg.lt

seguita da un INVIO.

Da notare che in assenza di echo locale i caratteri digitati non saranno visibili. Pertanto, dopo aver inserito il comando precedente, il server Whois risponde con i dati relativi alla query; nel nostro esempio (domreg.lt) l'output è il seguente:

% Hello, this is the DOMREG whois service.
% Please visit <http://www.domreg.lt/whois> for more information.
% Rights restricted by copyright.
% See <http://www.domreg.lt/whois/copyright.html>

domain: domreg.lt
holder/descr: ccTLD .lt registry
holder/descr: -----
holder/descr: Kaunas University of Technology
holder/descr: Information Technology Development Institute
holder/descr: Studentu 48a - 111
holder/descr: LT-51367 Kaunas,
holder/descr: Lithuania
admin-c: DT78-LT
tech-c: TM6174-LT
zone-c: LH274-LT
nserver: nemunas.sc-uni.ktu.lt
nserver: slave.dns.lt
changed: hostmaster@litnet.lt 20050330
source: DOMREG

person: Daiva Tamulioniene
e-mail: daiva@litnet.lt
nic-hdl: DT78-LT
changed: steinar.haug@runit.sintef.no 19940411
changed: milda@litnet.lt 20000601
changed: hostmaster@litnet.lt 20010619
changed: hostmaster@litnet.lt 20040910
source: DOMREG

person: Tomas Mackus
e-mail: tomas@litnet.lt
nic-hdl: TM6174-LT
changed: tomas@litnet.lt 20000703
changed: tomas@litnet.lt 20040910
source: DOMREG

person: LT Hostmaster
e-mail: hostmaster@litnet.lt
nic-hdl: LH274-LT
changed: milda@litnet.lt 20000601

```
changed: aurelija@litnet.lt 20020307
source: DOMREG
```

Connection to host lost.

Altrimenti avendo a disposizione la utility portqry.exe (preferibile la versione 2) di Microsoft – scaricabile dal sito Microsoft alla URL “<http://www.microsoft.com/downloads/details.aspx?FamilyID=89811747-C74B-4638-A2D5-AC828BDC6983&displaylang=en>” o disponibile nel kit Support Tools di Windows Server 2003, e descritta nell’articolo Knowledge Base 832919 – è possibile utilizzare il seguente comando, operando in ambiente Microsoft dalla console Command Prompt:

```
portqry -n <FQDN-Server-Whois> -e 43
```

Installazione

Dopo aver scaricato il file “WhoisClientApp_bin_10.zip” dalla URL <http://www.guidadns.it/whois> oppure <http://www.alessandropilotti.com/whois>, è sufficiente estrarre il contenuto in una directory (e.g.: c:\etc). Esso è costituito dai seguenti file:

- *WhoisClient.dll*: contiene le funzioni invocate dall’eseguibile whois.exe.
- *whois.exe*: comando/utility client Whois.
- *whois.xml*: file XML contenente i server Whois organizzati per gTLD/ccTLD e per blocchi di indirizzi IP (i.e.: server Whois dei *Regional Internet Registry* (RIR)). Nel caso in cui il client *Whois.exe* viene eseguito senza indicare nessun server Whois (opzione -r), esso utilizza il file *whois.xml* per dedurre il server Whois “competente” in base al suffisso TLD del dominio indicato nella query; viceversa, se l’argomento della query è un indirizzo IP, viene utilizzato il server Whois di un *Regional Internet Registry* (RIR) delegato per l’indirizzo in questione.



Aggiunta di server Whois al file Whois.xml

Per quanto riguarda le informazioni sui domini di tipo ccTLD, la presenza di un server Whois non è sempre garantita (e.g.: per il suffisso “.za” (Sud Africa) o “.ar” (Argentina)).

Per accertarsi di ciò, è consigliato fare riferimento all’archivio dei ccTLD disponibile alla URL <http://www.iana.org/cctld/cctld-whois.htm>.

Nel caso in cui alcuni di questi ccTLD rendano successivamente disponibile il loro server Whois, è possibile aggiungere le relative informazioni all’interno del file Whois.xml, rispettando il formato.

- *whois.xsd*: contiene la definizione dello schema (*XML Schema Definition*) del file XML.

Successivamente, procedere con il *download* e l’installazione del Microsoft.NET Framework 2.0 dal sito Microsoft alla URL seguente: <http://www.microsoft.com/downloads/details.aspx?FamilyID=0856each-4362-4b0d-8edd-aab15c5e04f5&DisplayLang=en> (per la versione in inglese).

Utilizzo del client Whois

Per utilizzare il client Whois è necessario aprire una sessione *Command Prompt* e spostarsi nella directory nella quale sono stati copiati i file (e.g.: c:\etc). È possibile, al fine di poter utilizzare il comando da una qualsiasi directory di lavoro, inserire la suddetta directory di installazione, nel path di sistema, utilizzando il comando `setx.exe` (simile al comando `setenv` del mondo Unix/Linux) nel modo seguente (da notare che esso è disponibile nativamente in ambito Windows Server 2003; viceversa, in ambiente Windows XP è necessario installare il Resource Kit oppure, più semplicemente, copiarlo dalla directory `%SystemRoot%\System32` di un qualsiasi computer equipaggiato con il sistema operativo Windows Server 2003):

```
setx path "c:etc;%PATH%"
```

Nel suddetto comando, si presuppone che i file siano stati copiati nella directory `c:\etc`.

Lo stesso risultato si può ottenere, operando sulle proprietà del sistema: dal Control Panel, dalla scheda *Advanced*, fare clic sul pulsante *Environment Variables* oppure eseguire l'*applet sysdm.cpl* direttamente o dal prompt dei comandi nel modo seguente:

```
rundll32.exe shell32.dll,Control_RunDLL sysdm.cpl
```

Nel caso di logon con uno *User Account* che non possiede i diritti amministrativi, è possibile utilizzare il comando `RunAs` nel modo seguente:

```
%windir%\system32\runas.exe /u:<utente admin> /savecred "rundll32.exe shell32.dll,Control_RunDLL sysdm.cpl"
```

Ad esempio:

```
%windir%\system32\runas.exe /u:leoner /savecred "rundll32.exe shell32.dll,Control_RunDLL sysdm.cpl"
```

Per inviare delle query Whois è sufficiente, dopo aver seguito le precedenti istruzioni di installazione, utilizzare la sintassi seguente:

```
Whois [-h] [-r <Server[:port]>] <query>
```

Dove:

- *-h*: permette di ottenere la sintassi per l'utilizzo del comando.
- *-r <Server[:port]>*: consente di specificare un determinato server Whois e la relativa porta sulla quale il demone/servizio Whois risponde (di default corrisponde alla 43/TCP). Da notare che né il server né la porta sono obbligatori. Nel caso in cui nessun server Whois è indicato, il client utilizza il file *whois.xml* per dedurre il server Whois "competente" in base al suffisso TLD del dominio indicato nella query, oppure il server Whois di un *Regional Internet Registry* (RIR) delegato, per l'indirizzo IP indicato con l'argomento *<query>*.
- *<query>*: contiene l'interrogazione da inviare al server Whois. Essa può indicare: un nome di dominio; un *nic-handle* di un oggetto Whois di tipo *Person*, *Role*, *Maintainer*, ecc.; oppure un indirizzo IP.

Alcuni esempi di utilizzo del client Whois sono di seguito indicati:

- *whois domreg.lt*
- *whois learning-solutions.it*
- *whois -r whois.nic.it contoso.it*
- *whois -r whois.ripe.net 193.205.245.5*
- *whois 193.205*

- `whois -r whois.nic.it LR2916-ITNIC`
- `whois -r whois.nic.it:43 REGISTRY-MNT`

Web Service SOAP Whois e client Web Whois

Le funzionalità del client Whois descritto precedentemente sono disponibili anche mediante un Web service SOAP all'URL <http://www.alessandropilotti.com/Whois/WhoisClientWS.asmx>. In questo modo, è possibile includere le suddette funzionalità in applicazioni scritte da terze parti.

Infine, è possibile richiamare il servizio tramite un browser Web, ottenendo i risultati di una query Whois in formato XML.

Utilizzo del client Whois in ambiente Unix/Linux con Mono

Prima di utilizzare il client Whois in ambiente Unix/Linux è necessario procedere con l'installazione del Framework .NET *Mono*, disponibile alla URL <http://www.mono-project.com/Downloads> per le varie versioni di sistema operativo.

Inoltre, è possibile scaricare anche tutti i file RPM in un unico file .ZIP; ad esempio:

```
wget http://www.go-mono.com/download/fedora-4-i386/mono-1.1.zip
```

Dopo aver scompattato il tutto in una directory e cancellato gli eventuali file RPM non necessari; ad esempio:

```
rm /f Mono-complete.rpm
```

oppure, se si dispone di client di motori di database installati, è possibile cancellare anche i seguenti RPM:

```
Mono-data-firebird.rpm
```

```
Mono-data-sqlite.rpm
```

```
Mono-data-sybase.rpm
```

```
Mono-data-postgresql.rpm
```

```
Mono-data-oracle.rpm
```

Per eseguire l'installazione di *mono*, usare il comando seguente:

```
rpm -Uvh *
```

Infine, creare una directory per copiare i file che compongono il client *Whois*, ed eseguire il comando seguente per scopattare il contenuto del file ZIP:

```
unzip WhoisClientApp_bin_10.zip
```

Per utilizzare il client *Whois*, eseguire il comando seguente:

```
"mono Whois.exe -r whois.internic.net alessandropilotti.com"
```

Esempi di query Whois

Di seguito vengono riportate alcune query che è possibile inviare utilizzando il client Whois per Windows:

- Verificare la registrazione di un nome di dominio all'interno del ccTLD ".it" (e.g.: guidadns.it):

- Esempio 1

```
C:\etc>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 *  
*****
```

No entries found in the IT-NIC database.

- Esempio 2

```
C:\etc>whois learning-solutions.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:        20070204
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
```

- Verificare gli attributi di un oggetto *person* (e.g.: Leone Randazzo) se presente nel database Whois del Registro italiano IT-NIC:

```
C:\etc>whois -r whois.nic.it "leone randazzo"
```

```
*****
```

```
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 *
*
```

```
*****
```

person: Leone Randazzo
address: IT-NIC
address: via Bronzino, 4
address: I-20133 Milano (MI)
nic-hdl: LR784-ITNIC
source: IT-NIC

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

Da notare che specificando solamente il cognome o il nome di una persona, vengono estratte tutte le occorrenze presenti nel database Whois e comprendenti il cognome o il nome passato come argomento. Naturalmente è possibile ridirigere l'output in un file di testo (e.g.: `whois "randazzo" > c:\temp\randazzo.txt`).

È bene ricordare che un uso improprio di queste funzionalità (e.g.: *advertising*/pubblicità, *data-maining*, ecc.) indipendentemente dal Registro detentore del database Whois è deprecato e contrario ai principi delle leggi vigenti.

- Verificare l'assegnatario (ed il Registro di competenza) di un indirizzo IP:

```
C:\etc>whois 193.205.245.5
*****
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 '193.205.245.0 - 193.205.245.255'
```


inetnum: 193.205.245.0 - 193.205.245.255
netname: GARR-NIS
descr: GARR
descr: NIS
country: IT
admin-c: EV182-RIPE
tech-c: GL965-RIPE
tech-c: ST43-RIPE
rev-srv: dns.nic.it
rev-srv: nameserver.cnr.it
status: ASSIGNED PA
remarks: Lan for external access to GARR-NIS servers
remarks: GARR - Italian academic and research network
mnt-by: GARR-LIR
source: RIPE # Filtered

role: GARR LIR
address: Consortium GARR
address: Viale Palmiro Togliatti 1625
address: I-00155 Roma
address: Italy
remarks: trouble: To notify abuse mailto: cert@garr.it
remarks: trouble: Information at http://www.lir.garr.it/
admin-c: EV182-RIPE
tech-c: GP4562-RIPE
tech-c: VP541-RIPE
tech-c: BM2532-RIPE
tech-c: MG473-RIPE
nic-hdl: GL965-RIPE
mnt-by: GARR-LIR
source: RIPE # Filtered
abuse-mailbox: cert@garr.it

person: Enzo Valente
address: Consortium GARR
address: Viale Palmiro Togliatti 1625
address: I-00155 Roma
address: Italy
phone: +39 06 43361441

fax-no: +39 06 43361444
nic-hdl: EV182-RIPE
mnt-by: GARR-LIR
source: RIPE # Filtered

person: Stefano Trumpy
address: Istituto di Informatica e Telematica - CNR
address: Via Giuseppe Moruzzi, 1
address: I-56124 - PISA
address: Italy
phone: +39 050 3152634
fax-no: +39 050 3152593
nic-hdl: ST43-RIPE
source: RIPE # Filtered

% Information related to '193.204.0.0/15AS137'

route: 193.204.0.0/15
descr: GARR routes
origin: AS137
mnt-by: GARR-LIR
source: RIPE # Filtered

Per ulteriori dettagli sul protocollo e sullo schema di un database Whois si rimanda al Capitolo 3, “Gli organismi che governano Internet: chi si occupa di che cosa”.