Wide Area Bonjour

How to use WAB with Mac OS X 10.6 Server

Writen by Yoann Gini, translated by Laurent Pertois

Summary

Introduction

This article is about Wide Area Bonjour, or how to pass Bonjour (ZeroConf) informations across routers (and VPN) with Mac OS X Server.

If you've been using Mac OS X Server for a long time, you should know that Wide Area Bonjour (WAB) is part of the best technologies, but also one of the most incomprehensible to setup, at first.

On my side, I've been trying to use it since Tiger, but I have to admit that documentation is very poor about it, as a proof of it, the official website dns-sd.org only has four pages…

That said, after long discussions with other administrators, I've been able to collect all useful informations to make it work “out of the box”. I wish to thank Guillaume Gete for giving me all the documentations he had collected himself, they have been very useful.

Before writing this article, I've been able to make this work one saturday evening at 1am. Suffice to say I have not pushed the tests beyond normal. This article is aimed at skilled administrators who have sufficient interest in that technology. I let you test it before going to production.

Static Data

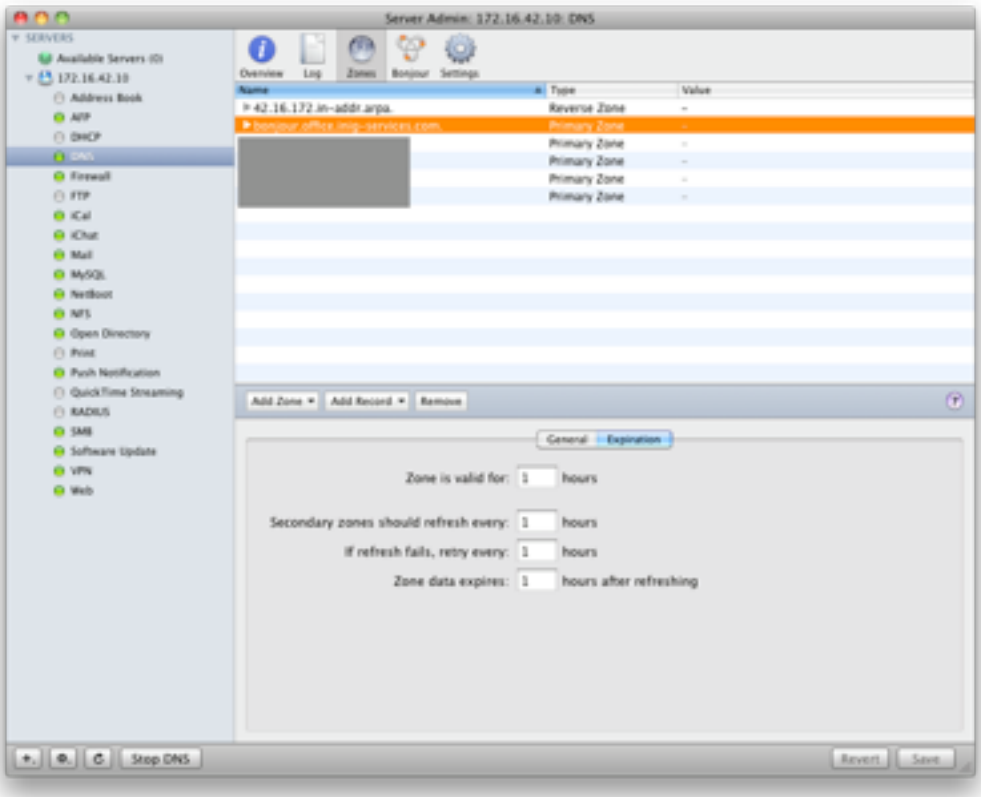
Let's start with setting WAB with static data only. This is the simplest setup, you can consider it reliable and put it in production with no known issue.

The idea is to provide static Bonjour informations, so this will be the DNS administrator who will fill his network informations. This can be useful to publish URLs of some intranet pages.

In order to work we need to configure a specific DNS zone, as for me I have decided to differentiate it from my internal zone. I'm using office.inig-services.com domain for my internal services, so I decided to use bonjour.office.inig-services.com as my Bonjour zone.

First, setup that zone and tell Server Admin this is the WAB zone.

To create the zone, nothing is simpler, add it in Server Admin as for any other zone.



I decided to use 1h validity because it looked good, I'm not certain this would be that necessary, but it seems useful if your data is going to change.

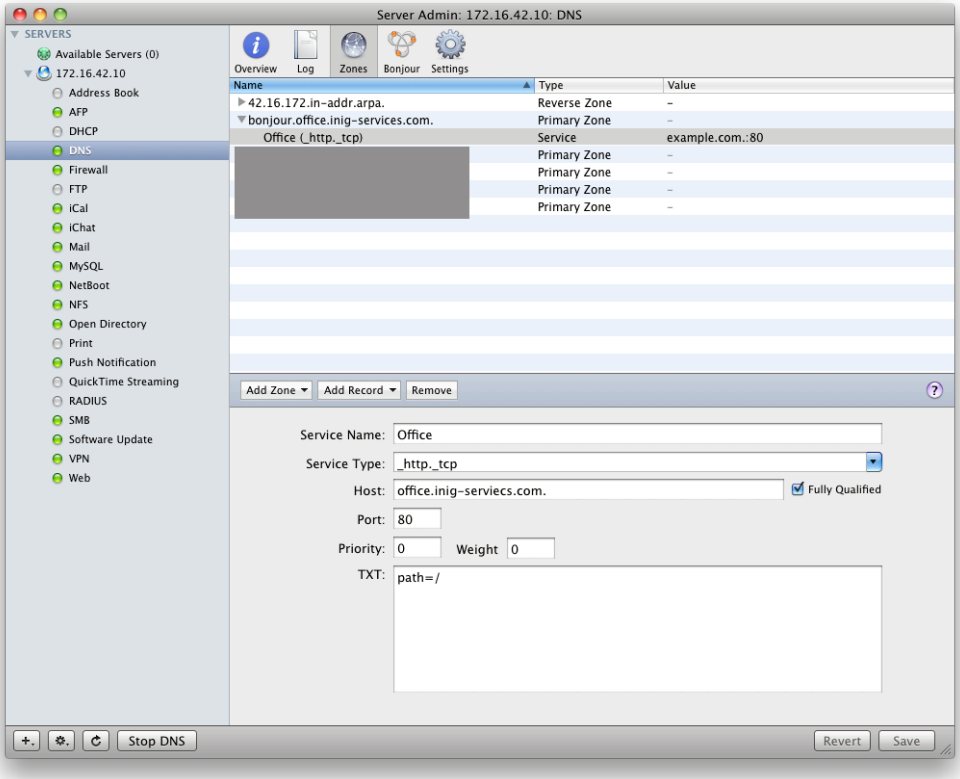
That being done, inform the office.inig-services.com zone that our subdomain is handled by our server. For this, we need to modify the configuration file of the DNS Server from the command line as Server Admin doesn't handle this manipulation.

The file to modify is **/var/named/db.office.inig-services.com**. It only contains few things except the include to the zone file modified by Server Admin, it's here to receive our modifications.

```
;THE FOLLOWING INCLUDE WAS ADDED BY SERVER ADMIN. PLEASE DO NOT REMOVE.
$INCLUDE /var/named/zones/db.office.inig-services.com.zone.apple
bonjour.office.inig-services.com. 86400 IN NS office.inig-services.com.
```

This is the modified file, we only added to the zone informations the fact that the bonjour.office.inig-services.com subdomain is managed by office.inig-services.com server. You can use this manipulation so that the WAB zone is handled by another server, for example.

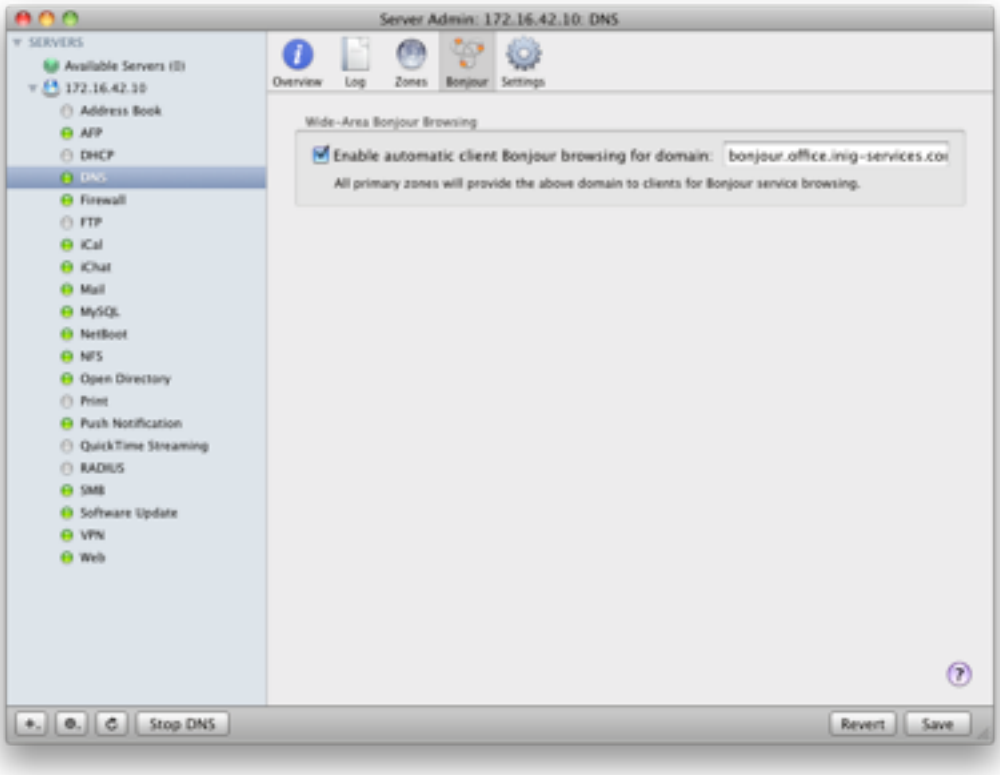
Add these data to this zone



I just added an information for a _http._tcp service, the name of this service is Office, that's the name Bonjour will show. This service is hosted on office.inig-services.com on port 80 (http, in fact) and this is the root of my server.

If my service was webmail, the path would be =/webmail in TXT informations.

Now, we need to do one last thing, use Server Admin to give the WAB zone name. For this, go in Server Admin Bonjour section and type in the zone name.



This will add these specific lines to each zone file managed by Server Admin.

```
lb._dns-sd._udp IN  PTR bonjour.office.inig-services.com.
b._dns-sd._udp IN  PTR bonjour.office.inig-services.com.
```

These lines tell client computers that WAB informations are in the specific zone called bonjour.office.inig-services.com.

If you have a look at dns-sd documentation, a “b._dns-sd” entry indicates the potential search zone and an “lb._dns-sd” the zone to use in addition to the .local

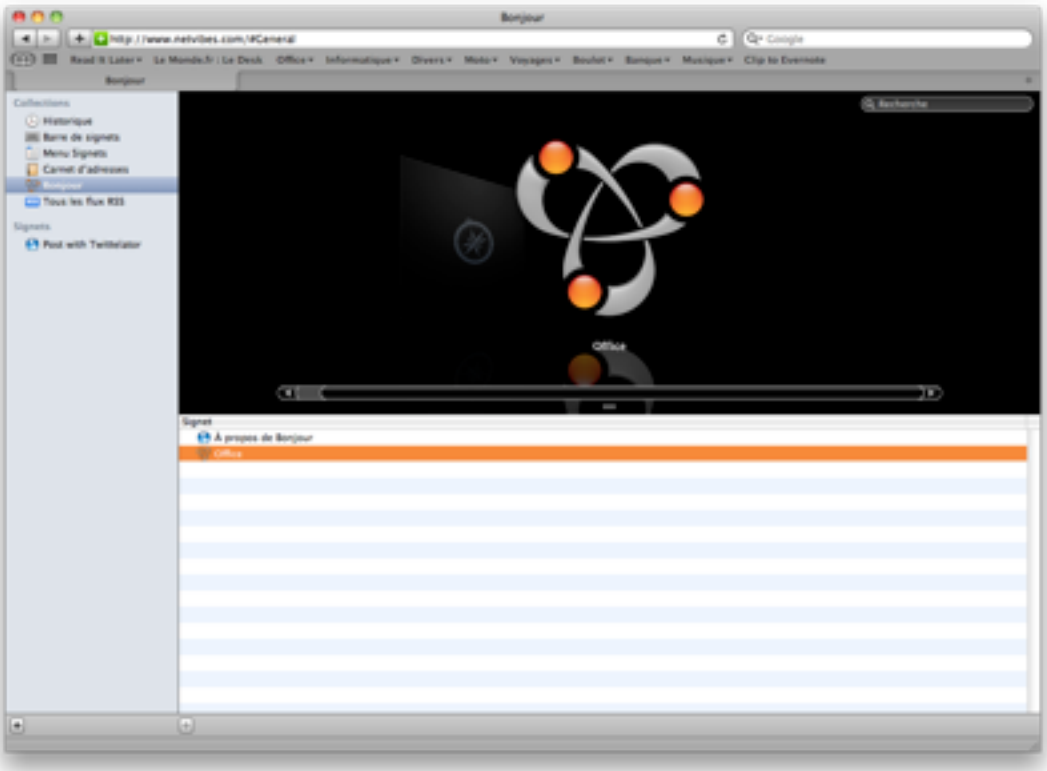
zone depending on developpers choices when they use Bonjour in their applications.

Once this is done you should have a functional read-only WAB zone !

To check this, login on a client computer that is correctly configured for DNS and search domains. This is my **/etc/resolv.conf** file for example :

```
domain office.inig-services.com
nameserver 172.21.42.10
nameserver 8.8.8.8
```

If I launch Safari and goes in its Bonjour research, this is what I get now :



An open zone

Our previous chapter was about a simple setup for a WAB zone with static data. Let's see now how client computers can write informations by recording themselves in our WAB zone and publishing their local Bonjour informations.

These manipulations assume you already have setup your WAB zone with static data as seen before. We will modify that WAB zone to host informations about unauthenticated client computers. This will be an open WAB zone.

Apple helps us a lot nowadays, with a little analysis on Mac OS X Server tools and a lot of intuition, this is how to do. Look at your DNS server parameters from the command line :

```
root@office / 18:30 % serveradmin settings dns
...
dns:views:_array_id:2247116D-446D-4254-
AEB0-8BD7377D4256:primaryZones:_array_id:0AC3AE46-8D87-4679-9EA0-
CCEDB87FF11F:nameservers:_array_index:0:name = "bonjour.office.inig-
services.com."
dns:views:_array_id:2247116D-446D-4254-
AEB0-8BD7377D4256:primaryZones:_array_id:0AC3AE46-8D87-4679-9EA0-
CCEDB87FF11F:bonjourRegistration = "off"
dns:views:_array_id:2247116D-446D-4254-
AEB0-8BD7377D4256:primaryZones:_array_id:0AC3AE46-8D87-4679-9EA0-
CCEDB87FF11F:allow-update = "none;"
...
```

You can see here informations about our bonjour.office.inig-services.com zone stored in a special way : dns:views:_array_id:<id>:primaryZones:_array_id:<id>:

Whatever that means doesn't matter, focus on the good values.

You may have noticed a value which name is bonjourRegistration that is off as of now, we will simply set it to “open” so that Server Admin changes the different tools for us so that the client computers can update the zone.

```
root@office / 18:38 % serveradmin settings dns:views:_array_id:
2247116D-446D-4254-AEB0-8BD7377D4256:primaryZones:_array_id:
0AC3AE46-8D87-4679-9EA0-CCEDB87FF11F:bonjourRegistration = "open"
```

After that particular command you should have a new file in **/etc/dns named dnsextd.conf** :

```
root@office / 18:40 % ls -l /etc/dns
total 32
-rw-r--r--@ 1 root  wheel   204B Jan 17 18:38 dnsextd.conf.apple
-rw-r--r--@ 1 root  wheel   130B Jan 17 18:38 loggingOptions.conf.apple
-rw-r--r--@ 1 root  wheel   324B Jan 17 18:38 options.conf.apple
-rw-r--r--@ 1 root  wheel   1.3K Jan 17 18:38 publicView.conf.apple
```

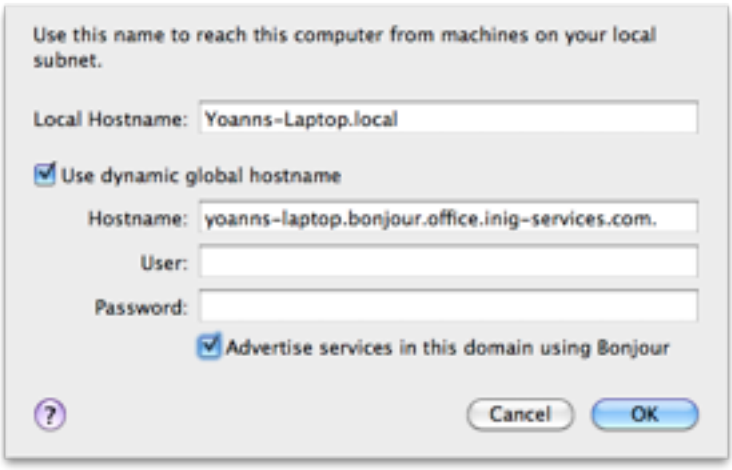
“dnsextd” is the daemon responsible for the communication between client and DNS server.

We can also notice that the other files have been modified, Server Admin also added all needed informations to have a valid WAB setup.

Our server is now ready to receive informations from our client, we just have to tell our machines that they can record, and also tell them which name to use.

To do this, open System Preferences on your client computer, then go to Sharing. In the Computer Name panel, click on the Edit button to modify Bonjour informations.

A new panel appears, select the “Use dynamic global hostname” checkbox, enter the host name of the machine, you don't need any credentials, and finally select “Advertise services in this domain using Bonjour” checkbox.



Once you have validated by clicking “Ok”, your client computer should record to your server (only, of course, if it's using the good DNS server).

This is how to check that everything went fine. From a Mac OS X client computer, launch Terminal and type the following command and compare the results :

```
yoann@Yoanns-Laptop ~ 19:00 % dns-sd -E
Looking for recommended registration domains:
Timestamp     Recommended Registration domain
19:00:26.729  Added     (More)              local
19:00:26.730  Added     (More)              mac.com
                                                          - > members
                                                          - - > yoann
19:00:26.730  Added                         inig-services.com
                                                          - > office
                                                          - - > bonjour
```

This command shows me the Bonjour domains recommended for record, I can find my .local domain (the default one), the MobileMe domain (yes, MobileMe is using WAB to provide Back To My Mac services) and our domain, everything is fine !

Another command (it needs that your recorded client has the AFP service on) :

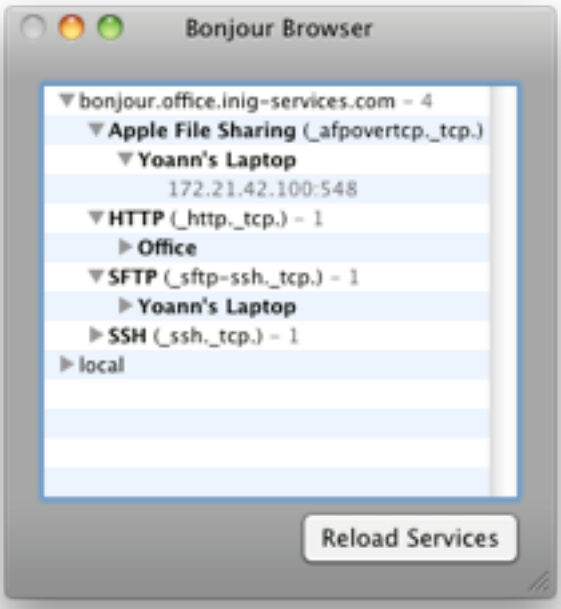
```
yoann@Yoanns-Laptop ~ 19:00 % dns-sd -B _afpovertcp._tcp bonjour.office.inig-
services.com.
Browsing for _afpovertcp._tcp.bonjour.office.inig-services.com.
Timestamp     A/R Flags if Domain                    Service Type
Instance Name
19:03:30.913  Add     2  0 bonjour.office.inig-services.com.
_afpovertcp._tcp.          Yoann's Laptop
```

I can list all _afpovertcp._tcp service record on my bonjour.office.inig-services.com zone.

Now, if I want to get informations for a specific service on a machine, this is all I have to do :

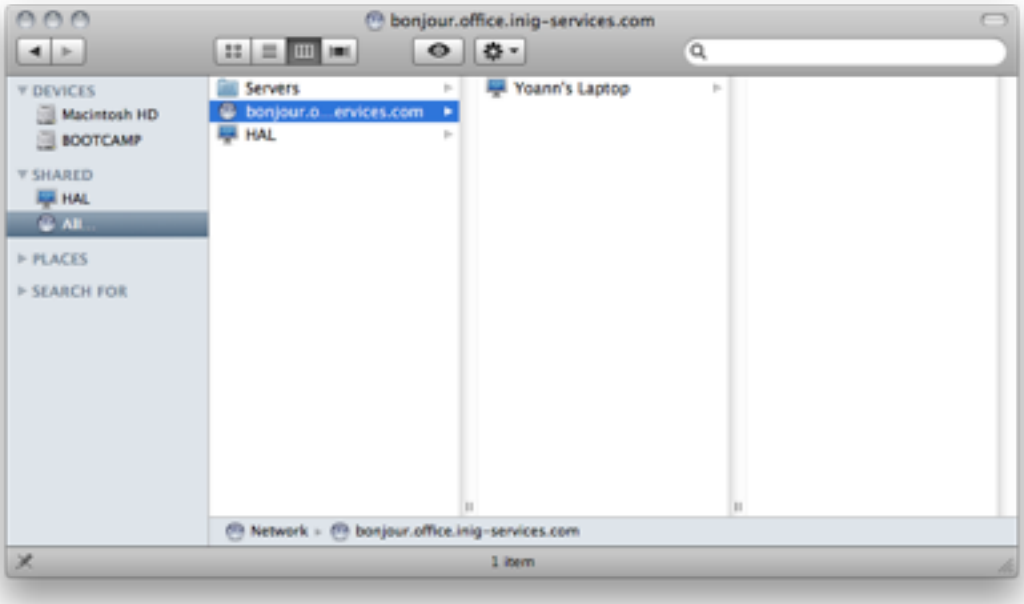
```
yoann@Yoanns-Laptop ~ 19:05 % dns-sd -L "Yoann's Laptop" _afpovertcp._tcp
bonjour.office.inig-services.com.
Lookup Yoann's Laptop._afpovertcp._tcp.bonjour.office.inig-services.com.
19:05:26.225  Yoann's\032Laptop._afpovertcp._tcp.bonjour.office.inig-
services.com. can be reached at yoann-laptop.office.inig-services.com.:548
(interface 0)
```

Another easy way to see published informations on Bonjour domains is to use the excellent Bonjour Browser, here it is launched on another machine :

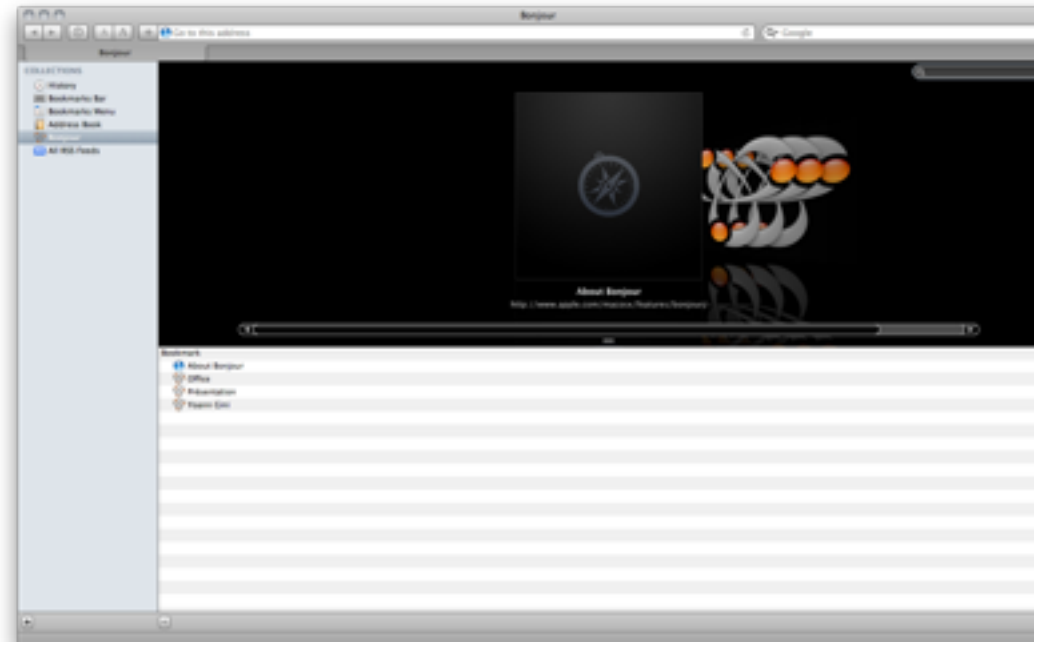


Now our WAB zone is functional. Will only be recorded on that zone client computers with the good options selected in System Preferences. Others will see what is published by the machines configured correctly as long as they are using the good DNS server and the good search domain.

This is what a VPN connected client can see on my server :



And this is from Safari :



A little more about records

We know how to setup a DNS zone for WAB, this little chapter will complete your configuration so that a wide range of services can record on WAB.

To start with, a little explanation about what is Bonjour from a developer point of view (being a Mac/iPhone developer a third of my time, I consider I can talk about this).

When you create a Mac application, using Bonjour network discovery is pretty simple. You just need to give a unique name for the service (and its communication protocol), "_http._tcp" for example and then create a record (or a search) on the domain. The domain can be local, to limit to the local Bonjour, or, as advised by the documentation, an empty string of characters. This last choice, as already chosen by number of developers, lets the system choose what is the best zone for the Bonjour record.

The question is to know how the best zone is chosen. This is very simple, by default this is the local zone, except if another zone is defined as default (in that particular case the record is done on both, the local and the extra one).

Why do you need to know that ? If, as I do, you have softwares (I won't say which ones) that work only with Bonjour, or if you are not able to record your server manually (which are, in my opinion, bad developments), you will be in trouble in a large network or over VPN.

The idea then is to make sure a majority of these software (those which let the system choose the zone) will use our WAB zone. To say, only some services will record on the "secondary" zones.

Reopen the Terminal on your server to add a few lines in your static search zone configuration files, in my example it was **/var/db/db.office.inig-services.com**.

We have already made some modifications to that file to specify the zone delegation for WAB, we will write 3 lines to get this :

```
;THE FOLLOWING INCLUDE WAS ADDED BY SERVER ADMIN. PLEASE DO NOT REMOVE.
$INCLUDE /var/named/zones/db.office.inig-services.com.zone.apple

db._dns-sd._udp IN  PTR bonjour.office.inig-services.com.
r._dns-sd._udp IN  PTR bonjour.office.inig-services.com.
dr._dns-sd._udp IN  PTR bonjour.office.inig-services.com.

bonjour.office.inig-services.com. 86400 IN NS office.inig-services.com.
```

Have a look at dns-sd.org documentation :

- "db._dns-sd" defines our domain as a default search domain for Bonjour
- "r._dns-sd" defines our domain as a potential record domain
- "dr._dns-sd" defines our domain as a default record domain

By the way, activating WAB in Server Admin, as we did in the first article, added these entries to all your domains :

- "b._dns-sd" to indicate a potential search domain
- "lb._dns-sd" to tell client computers to use your domain in addition to the local domain (and so to force applications to read its content).

That being done, you only have to restart Bonjour enabled services.

And now, a majority of the softwares you are using will be accessible over VPN.

Shared secret authentication

In previous chapters, we discovered how to setup a read-only WAB zone, then how to make that zone read and write so that client computers could record their services and finally little tips to make our zone as rich as possible.

It's time to see how to ensure write access to the zone is protected using a shared secret.

If you remember, in the second chapter we used command line to set the bonjourRegistration key to “open”. Now, we are going to modify this value to “secure”.

```
root@office / 18:17 % serveradmin settings dns:views:_array_id:
2247116D-446D-4254-AEB0-8BD7377D4256:primaryZones:_array_id:
0AC3AE46-8D87-4679-9EA0-CCEDB87FF11F:bonjourRegistration = "secure"
```

This command will change the **/etc/dns/publicView.conf.apple** which contains domains definitions. Look at your WAB zone, it should be like this :

```
zone "bonjour.office.inig-services.com." {
       type master;
       file "db.bonjour.office.inig-services.com.";
       allow-transfer {none;};
       allow-update {key com.apple.ServerAdmin.DNS.bonjour.sharedSecret;};
};
```

The interesting point is the “allow-update” line which is now set by Server Admin to only use the “*com.apple.ServerAdmin.DNS.bonjour.sharedSecret”* key. We need, now, to define that key and transmit it to our client computers.

Defining that key is done with “*rndc-confgen”* command line tool, we will need to indicate where to store the key, I have placed it in **/etc/dns/bonjour.key** :

```
root@office / 18:27 % rndc-confgen -a -c /etc/dns/bonjour.key -k
com.apple.ServerAdmin.DNS.bonjour.sharedSecret
```

If you look at the content of this file, this is what you should see :

```
key "com.apple.ServerAdmin.DNS.bonjour.sharedSecret" {
       algorithm hmac-md5;
       secret "lasZZ9TN+AILCl+TpNgUiw==";
};
```

Notice the secret that is between quotes, you will need it on client computers.

That key being generated, tell BIND where to find by modifying the **/etc/named.conf** file like this :

```
//
// Include keys file
//
include "/etc/rndc.key";
include "/etc/dns/bonjour.key";

// ...
```

Now restart the DNS service :

```
root@office / 18:33 % serveradmin stop dns && serveradmin start dns
```

Last thing, configure client computers going in Sharing in System Preferences to change the WAB record, the user name will be "*com.apple.ServerAdmin.DNS.bonjour.sharedSecret"* and the password "*lasZZ9TN+AILCl+TpNgUiw==*" (the one we saw before in the **/etc/dns/bonjour.key**).

If you wish to test your zone is working perfectly, Bonjour Browser is your friend :-)

More about the authors

This documentation was originatly written in french by Yoann Gini on blog.inig-services.com an translated in english by Laurent Pertois.

Yoann Gini is a french freelance who works on IT Apple product for business. He has been an Apple Certified Trainer for ACSP & ACTC courses since Mac OS X Tiger and works also for Apple Authorized Trainer Centers, ApaxxDesigns and Terkane.

Laurent Pertois is a french trainer and consultant of Agnosys, the oldest Apple Authorized Training Center on IT in France. He has been Apple Certified Trainer and Apple Certifies System Administrator since Mac OS X 10.2.

Yoann Gini: yoann.gini@inig-services.com

Laurent Pertois: laurent@it42.fr