Cache DNS

Ce tutoriel développe la mise en place d'un serveur cache DNS (BIND).
Il facilitera la résolution des noms de domaine pour votre serveur proxy, mail, ... par exemple.

Installation des packages

Mandrake	debian
bind-9.3.0-3.1.101mdk.i586.rpm bind-utils-9.3.0-3.1.101mdk.i586.rpm caching-nameserver-9.2-2mdk.noarch.rpm	bind-9_9.2.3+9.2.4-rc2-1_i386.deb bind9-host_9.2.3+9.2.4-rc2-1_i386.deb dnsutils_9.2.3+9.2.4-rc2-1_i386.deb libdns11_9.2.3+9.2.4-rc2-1_i386.deb

Génération de la clef TSIG (Transaction SIGnatures)

BIND utilise une signature par clef cryptée pour authentifier les transactions le concernant.

La commande suivante génère une paire de clefs HMAC-MD5 à 128 bits intitulé mykey

```
[root@pc user]# dnssec-keygen -a HMAC-MD5 -b 128 -n USER mykey
[root@pc user]# ls
Kmykey.+157+12345.key     Kmykey.+157+12345.private
[root@pc user]#
```

Ouvrez le fichier Kmykey.+157+12345.private pour extraire la clef

```
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: vwMIK07Iqm5+LjnKaiOvsg==
```

Copiez cette clef dans le fichier

Mandrake	debian
/etc/rndc.key (chmod 600) sous cette forme :	**/etc/bind/rndc.key** (chmod 600) sous cette forme :

```
key mykey {
        algorithm       hmac-md5;
        secret "vwMIK07Iqm5+LjnKaiOvsg==";
};
```

Configuration de BIND (cache DNS)

Mandrake

Modifier le fichier **/etc/named.conf**

```
// Déclaration de la clef en incluant directement le fichier clef.
include "/etc/rndc.key";

// Autorise une mise à jour avec la clef.
controls {
inet 127.0.0.1 allow { any; } keys { "mykey"; };
};

// Définit les options du serveur dans son ensemble.
options {
directory "/var/named";
pid-file "/var/run/named/named.pid";

// Permet de masquer la version de BIND.
version "SECRET";

// Indique que le port 53 est le port d'échange DNS.
// Recommandé lorsqu'il y a un Firewall.
query-source address * port 53;

// Définit les zones root et locales.
zone "." {
type hint;
file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
};
```

debian

Modifiez le fichier **/etc/bind/named.conf**

```
// Déclaration de la clef en incluant directement le fichier clef.
include "/etc/bind/rndc.key";

// Autorise une mise à jour avec la clef.
controls {
inet 127.0.0.1 allow { any; } keys { "mykey"; };
};

include "/etc/bind/named.conf.options";

// prime the server with knowledge of the root servers
zone "." {
type hint;
file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
type master;
file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
type master;
file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
type master;
file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
type master;
file "/etc/bind/db.255";
};
```

debian

Modifiez le fichier **/etc/bind/named.conf.options**

```
options {
directory "/var/cache/bind";

// If there is a firewall between you and nameservers you want
// to talk to, you might need to uncomment the query-source
// directive below. Previous versions of BIND always asked
// questions using port 53, but BIND 8.1 and later use an unprivileged
// port by default.

query-source address * port 53;

// Permet de masquer la version de BIND.
version "SECRET";

// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

// forwarders {
// 0.0.0.0;
// };

//auth-nxdomain no; # conform to RFC1035

};
```

Mandrake	debian

Modifiez le fichier **/etc/rndc.conf**
 	
`options {`
`default-server 127.0.0.1;`
`default-key "mykey";`
`};`
 	
`server localhost {`
`key "mykey";`
`};`
 	
`include "/etc/rndc.key";`
	Modifiez le fichier **/etc/bind/rndc.conf**
	
	`options {`
	`default-server 127.0.0.1;`
	`default-key "mykey";`
	`};`
	
	`server localhost {`
	`key "mykey";`
	`};`
	
	`include "/etc/bind/rndc.key";`

Modifiez le fichier **/etc/resolv.conf**pour que votre machine utilise le serveur cache DNS local en premier. Si vous avez d'autres serveurs DNS dans votre réseau mettez les à la suite.

```
nameserver 127.0.0.1
#nameserver 192.168.0.1
#nameserver 192.168.0.5
```

Vérifiez que le fichier **/etc/nsswitch.conf**contient la ligne :
`hosts: files dns`

et que **/etc/host.conf**:
```
order hosts,bind
multi on
```

Document mis à jour : 03/05/05