



Outils DNS

Serveur Linux CentOS

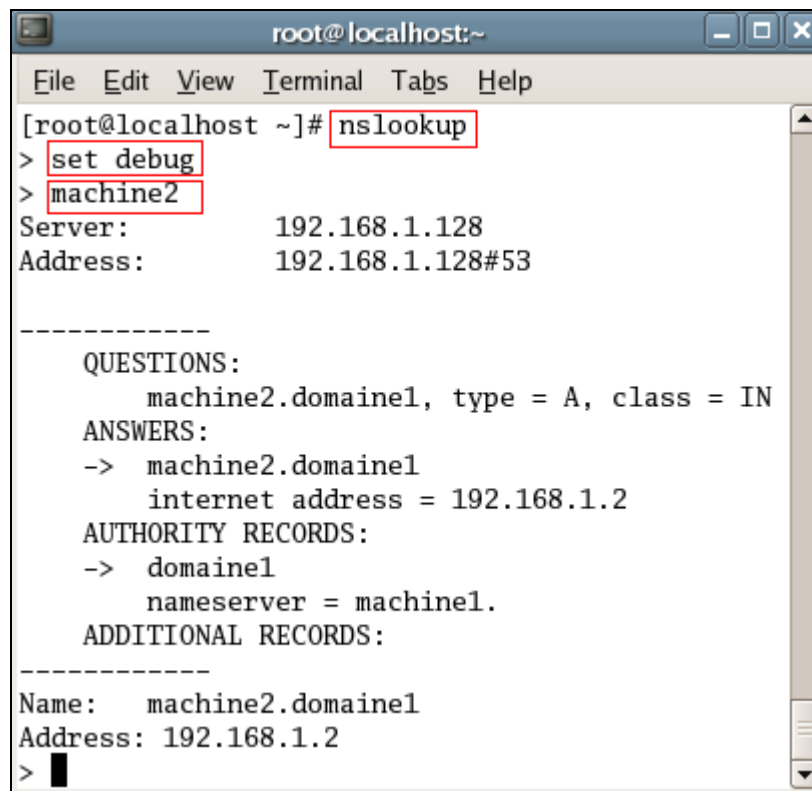
Table des matières

1	DÉBUGUER UN DNS	3
2	DNS ET SÉCURITÉ.....	4
3	OUTILS	5
3.1	rndc	5
3.2	nslookup.....	7
3.3	host.....	8
3.4	dig	8

1 DÉBUGUER UN DNS

Il est admis que l'écriture des fichiers de configuration d'un DNS est difficile. En plus de cela, il faut faire très attention à ce que l'on écrit, un espace ou un point oublié peuvent tout changer, et pour trouver l'erreur, on peut y passer des heures ! Cette section présente quelques trucs et sources d'erreurs possibles.

- Consulter le fichier **/var/log/messages** après chaque lancement de **named**. Les erreurs apparaîtront avec le nom du fichier et la ligne incriminée ;
- Vérifier les noms des hôtes dans les fichiers de configuration. Ne pas oublier qu'un nom est relatif à la zone s'il ne se termine pas par un point ;
- Ne pas oublier d'incrémenter le numéro de série dans les fichiers de configuration du DNS primaire pour qu'il soit pris en compte par DNS secondaire.
- Ne pas oublier que si un champ est facultatif, il faut quand même laisser un espace (IN MX 10 machine et MX 10 machine sont équivalents, mais il doit y avoir un espace avant MX) ;
- Si une zone extérieure semble ne pas être atteignable, utiliser l'option **debug** de **nslookup** :

A screenshot of a terminal window titled 'root@localhost:~'. The terminal shows the execution of 'nslookup' followed by 'set debug' and 'machine2'. The output displays the server address (192.168.1.128) and the lookup results for 'machine2.domaine1', showing an internet address of 192.168.1.2 and a nameserver of machine1. The terminal text is as follows:

```
root@localhost:~# nslookup
> set debug
> machine2
Server:          192.168.1.128
Address:         192.168.1.128#53

-----
      QUESTIONS:
        machine2.domaine1, type = A, class = IN
      ANSWERS:
-> machine2.domaine1
    internet address = 192.168.1.2
  AUTHORITY RECORDS:
-> domaine1
    nameserver = machine1.
  ADDITIONAL RECORDS:

-----
Name:   machine2.domaine1
Address: 192.168.1.2
>
```

2 DNS ET SÉCURITÉ

Il est souhaitable de sécuriser son DNS local. Voici quelques recettes. Dans le fichier **/etc/named.conf**, on peut spécifier les DNS autorisés à demander un transfert de zone à l'aide de l'option **allow-transfer** :

```
/*
 * Seul le DNS d'adresse 192.168.2.1 a le droit de
 * récupérer les informations à partir de ce DNS.
 */

zone "orabec.ca" {
    type master;
    file "domaine1";
    allow-transfer { 192.168.2.1 ; };
};
```

Les transferts de zones étant utilisés par les **spammers** et les **spoofers** d'IP, il est recommandé de spécifier cette option. Si on n'a pas de DNS secondaire, on peut mettre l'adresse **loopback (127.0.0.1)**. On peut préciser plusieurs adresses, séparées par un point-virgule ;

Autoriser les requêtes au DNS de la part des hôtes d'un domaine particulier, les autres n'y étant pas autorisés. Par exemple, pour que seuls les hôtes du domaine local **192.168.1.0** soient autorisés à interroger le DNS, insérer dans le fichier **/etc/named.conf** l'option **allow-query** :

```
/*
 * Seuls les hôtes du domaine 192.168.1.0/24
 * sont autorisés à interroger ce DNS local.
 */

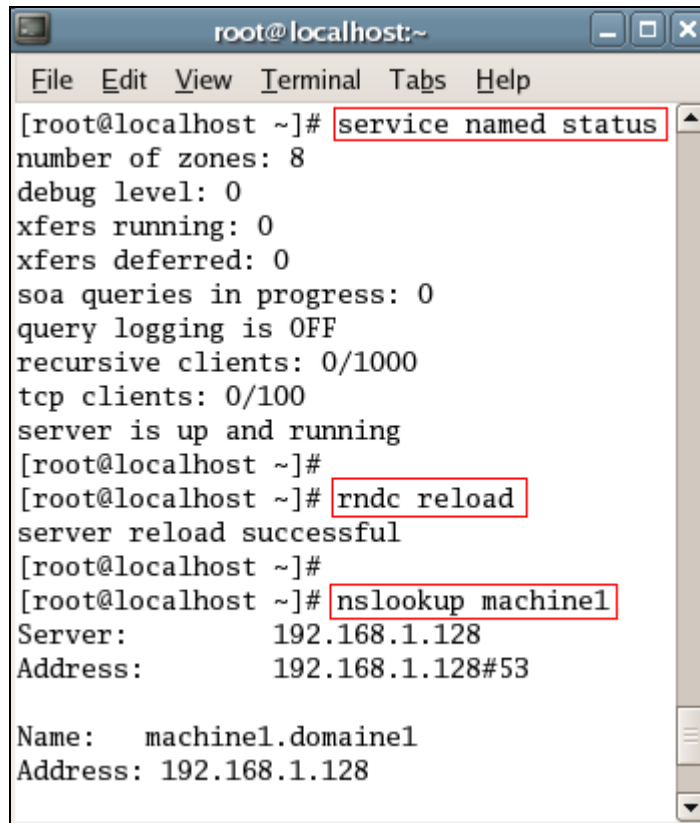
zone "orabec.ca" {
    type master;
    file "orabec.ca";
    allow-transfer { 192.168.2.1 ; };
    allow-query {192.168.1.0/24 ; };
};
```

L'adresse **192.168.1.0/24** signifie "toutes les adresses dont les **24** premiers bits commencent par **192.168.1.0**". Comme on a une adresse de classe C avec un masque de réseau correspondant à une adresse de classe C, cela revient à dire tous les hôtes du réseau **192.168.1.0** ;

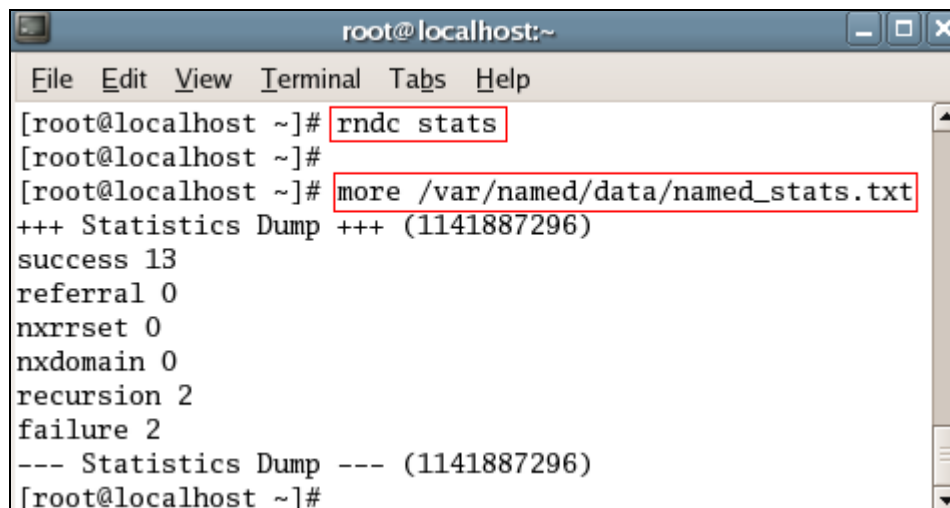
Ne pas mettre de **RR** de type **HINFO**. Les informations associées donnant des informations sur la machine sur laquelle tourne le DNS, on peut plus facilement trouver les failles de sécurité.

3 OUTILS

3.1 rndc



```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# service named status  
number of zones: 8  
debug level: 0  
xfers running: 0  
xfers deferred: 0  
soa queries in progress: 0  
query logging is OFF  
recursive clients: 0/1000  
tcp clients: 0/100  
server is up and running  
[root@localhost ~]#  
[root@localhost ~]# rndc reload  
server reload successful  
[root@localhost ~]#  
[root@localhost ~]# nslookup machine1  
Server:          192.168.1.128  
Address:         192.168.1.128#53  
  
Name:   machine1.domain1  
Address: 192.168.1.128
```



```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# rndc stats  
[root@localhost ~]#  
[root@localhost ~]# more /var/named/data/named_stats.txt  
+++ Statistics Dump +++ (1141887296)  
success 13  
referral 0  
nxrrset 0  
nxdomain 0  
recursion 2  
failure 2  
--- Statistics Dump --- (1141887296)  
[root@localhost ~]#
```

```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# rndc querylog  
[root@localhost ~]#  
[root@localhost ~]# tail -f -n 1 /var/log/messages  
Mar 9 02:04:58 localhost named[4595]: query logging is now on
```

```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# nslookup machine2  
Server: 192.168.1.128  
Address: 192.168.1.128#53  
  
Name: machine2.domain1  
Address: 192.168.1.2  
  
[root@localhost ~]# tail -f -n 2 /var/log/messages  
Mar 9 02:04:58 localhost named[4595]: query logging is now on  
Mar 9 02:11:06 localhost named[4595]: client 192.168.1.128#32789: query: machine2.domain1 IN A +
```

```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# rndc querylog  
[root@localhost ~]#  
[root@localhost ~]# tail -f -n 1 /var/log/messages  
Mar 9 02:12:48 localhost named[4595]: query logging is now off
```

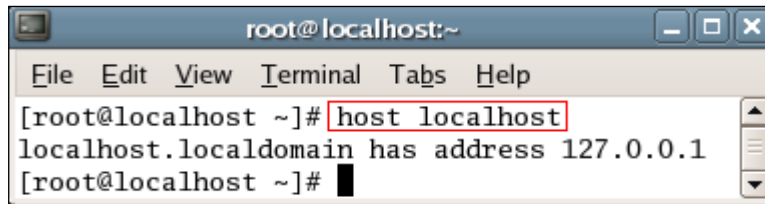
```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# rndc dumpdb  
[root@localhost ~]#  
[root@localhost ~]# more /var/named/data/cache_dump.db  
;  
; Start view _default  
;  
;  
; Cache dump of view '_default'  
;  
$DATE 20060309075816  
;  
; Start view _default  
;  
;  
; Address database dump  
;  
;  
; Unassociated entries  
;  
;  
; Start view _bind  
;  
;  
; Cache dump of view '_bind'
```

```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# rndc flush  
[root@localhost ~]#  
[root@localhost ~]# rndc trace  
[root@localhost ~]#  
[root@localhost ~]# rndc trace 4  
[root@localhost ~]#
```

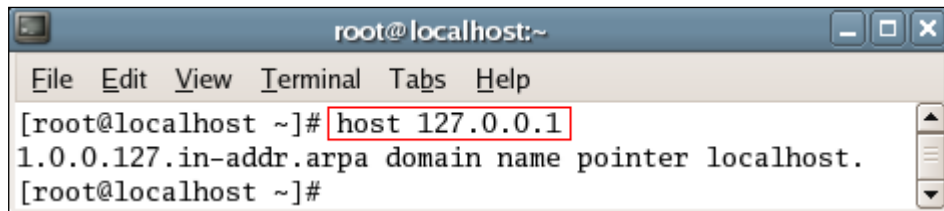
3.2 nslookup

```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# nslookup machine1  
Server:      192.168.1.128  
Address:     192.168.1.128#53  
  
Name:   machine1.domain1  
Address: 192.168.1.128  
[root@localhost ~]#
```

3.3 host

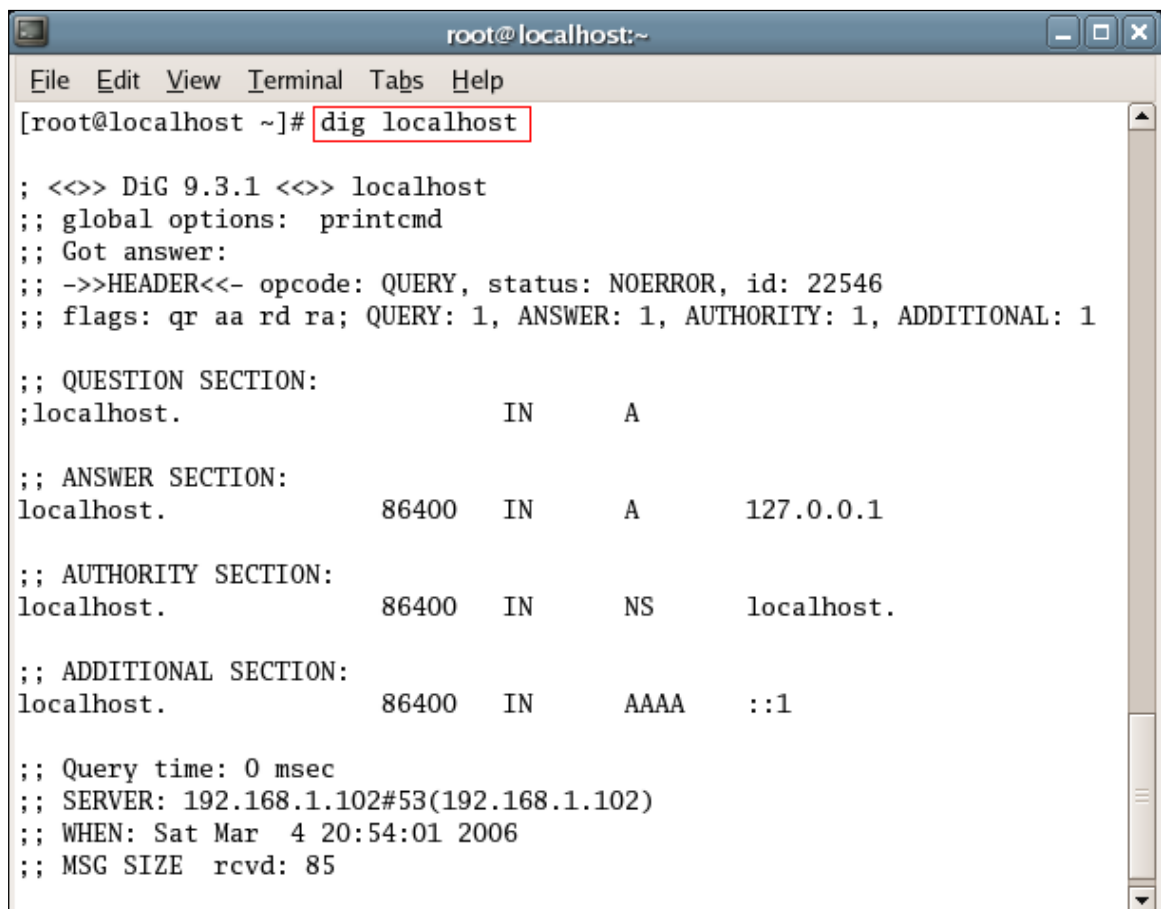


```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# host localhost  
localhost.localdomain has address 127.0.0.1  
[root@localhost ~]#
```



```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# host 127.0.0.1  
1.0.0.127.in-addr.arpa domain name pointer localhost.  
[root@localhost ~]#
```

3.4 dig



```
root@localhost:~  
File Edit View Terminal Tabs Help  
[root@localhost ~]# dig localhost  
  
; <>> DiG 9.3.1 <>> localhost  
;; global options: printcmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22546  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1  
  
;; QUESTION SECTION:  
localhost. IN A  
  
;; ANSWER SECTION:  
localhost. 86400 IN A 127.0.0.1  
  
;; AUTHORITY SECTION:  
localhost. 86400 IN NS localhost.  
  
;; ADDITIONAL SECTION:  
localhost. 86400 IN AAAA ::1  
  
;; Query time: 0 msec  
;; SERVER: 192.168.1.102#53(192.168.1.102)  
;; WHEN: Sat Mar 4 20:54:01 2006  
;; MSG SIZE rcvd: 85
```