Serveur DNS Maître / Esclave

Théorie & Sécurisation

Objectifs de la Présentation

Comprendre Maître / Esclave

Démystifier les rôles et le fonctionnement de base du DNS.

Fonctionnement SOA + NOTIFY

Saisir les mécanismes de synchronisation des zones DNS.

Types de Transferts

Identifier les différentes méthodes de réplication de données DNS.

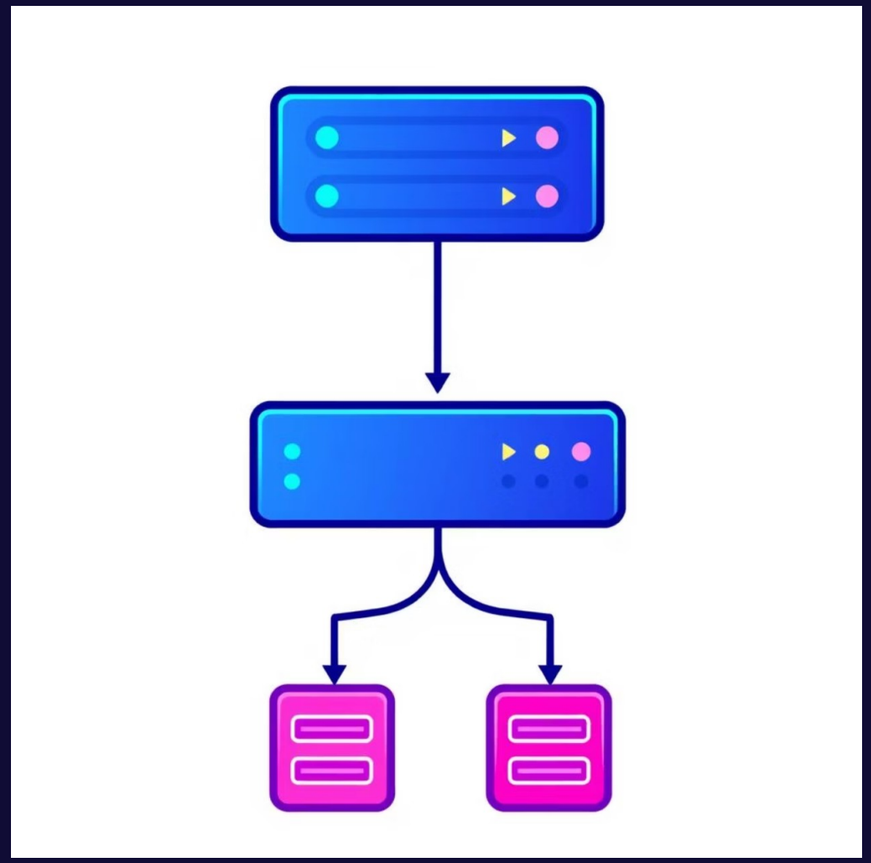
Sécurisation via ACL

Appréhender les méthodes pour sécuriser les transferts de zones.

Pourquoi un Serveur DNS Esclave ?

Un serveur DNS esclave est essentiel pour garantir la robustesse et la fiabilité de votre infrastructure DNS. Il assure une présence constante, même en cas de défaillance du maître.

- **Haute disponibilité :** Les requêtes DNS peuvent toujours être résolues même si le serveur maître est hors service.
- **Redondance :** Une copie complète des données de zone est disponible sur un serveur distinct, protégeant contre la perte de données.
- **Continuité de service :** Minimise les interruptions, assurant que les services et applications restent accessibles aux utilisateurs.
- **Distribution de charge :** Permet de répartir les requêtes DNS, réduisant la charge sur le serveur maître.



Rôle du Maître & Rôle de l'Esclave

1

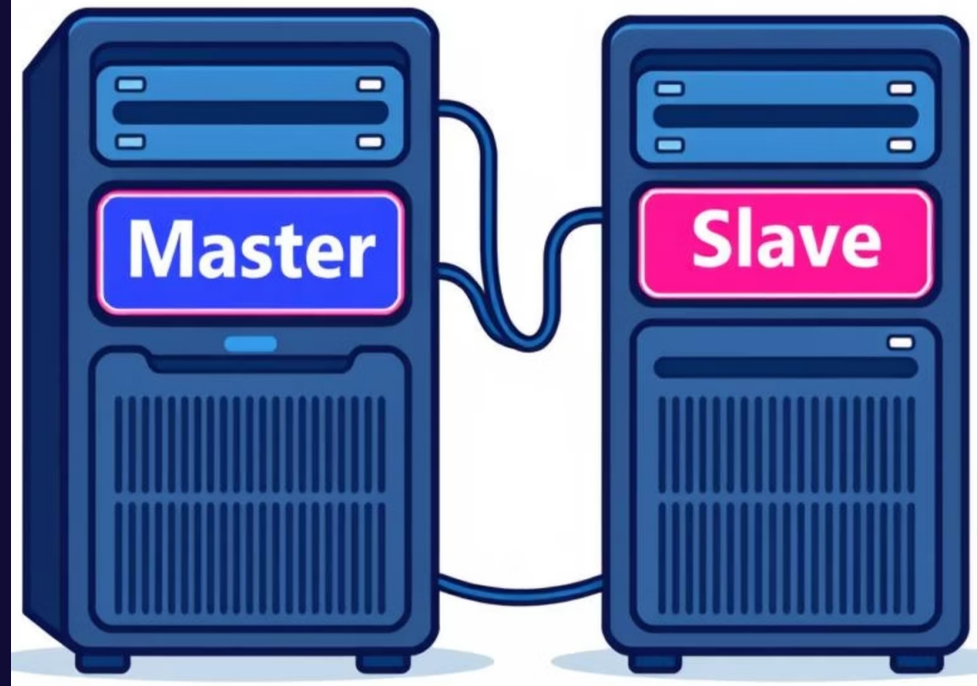
Le Serveur DNS Maître

Le serveur maître détient la version **officielle et faisant autorité** de la zone DNS. Toutes les modifications (ajouts, suppressions, mises à jour d'enregistrements) sont effectuées sur ce serveur. Il est la source primaire des données.

2

Le Serveur DNS Esclave

Le serveur esclave maintient une **copie synchronisée** de la zone. Il ne permet pas de modifications directes, mais il répond aux requêtes DNS des clients. Son rôle est de décharger le maître et d'assurer la résilience.

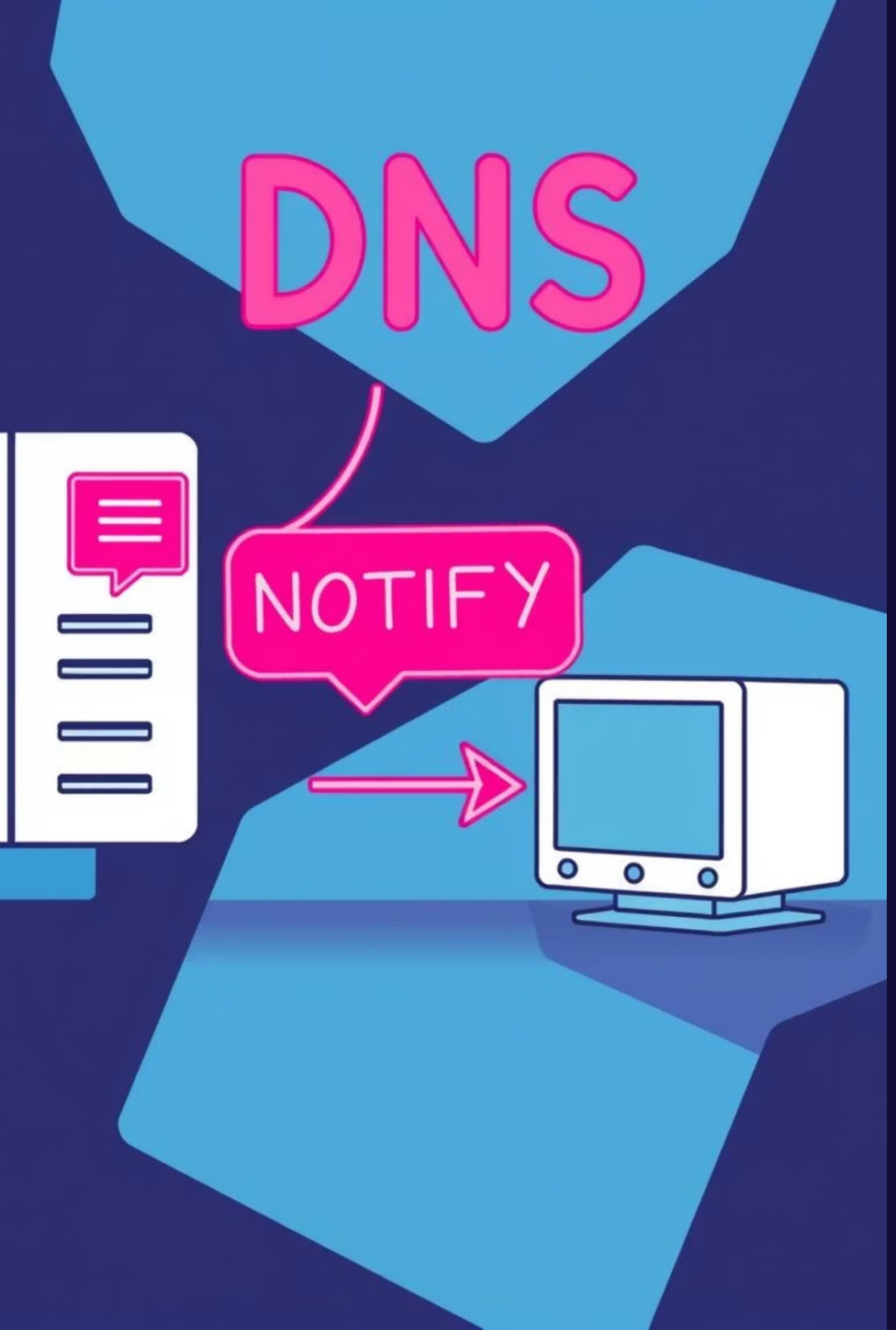


Fichier SOA et Numéro de Série

L'enregistrement `SOA` (Start of Authority) est fondamental pour la gestion des zones DNS. Il contient des informations cruciales sur la zone, y compris le **numéro de série**.

- Le numéro de série indique la **version actuelle** de la zone. C'est un entier qui doit être incrémenté à chaque modification apportée à la zone DNS.
- Les serveurs esclaves utilisent ce numéro pour déterminer si leur copie de la zone est **obsolète** et si un transfert est nécessaire.
- Un numéro de série non incrémenté après une modification peut entraîner une **désynchronisation** entre le maître et les esclaves.


```
$TTL 86400
@ IN SOA ns1.example.com. hostmaster.example.com. (
 2023102701 ; Serial
 3600 ; Refresh
 1800 ; Retry
 604800 ; Expire
 86400 ; Minimum TTL
)
```



NOTIFY : Le Mécanisme de Notification

Détection par le Maître

Le serveur maître détecte qu'une modification a été faite dans la zone, ce qui entraîne l'incrémentation du numéro de série SOA.

Envoi du NOTIFY

Le serveur maître envoie un message `NOTIFY` aux serveurs esclaves configurés, les informant qu'une nouvelle version de la zone est disponible.

Réception et Comparaison par l'Esclave

L'esclave reçoit le NOTIFY, vérifie le numéro de série SOA de la zone reçue et le compare avec sa propre version locale.

Demande de Transfert

Si le numéro de série du maître est supérieur, l'esclave initie une demande de transfert de zone (`AXFR` ou `IXFR`) pour se mettre à jour.

Types de Transfert de Zone

AXFR (Full Zone Transfer)

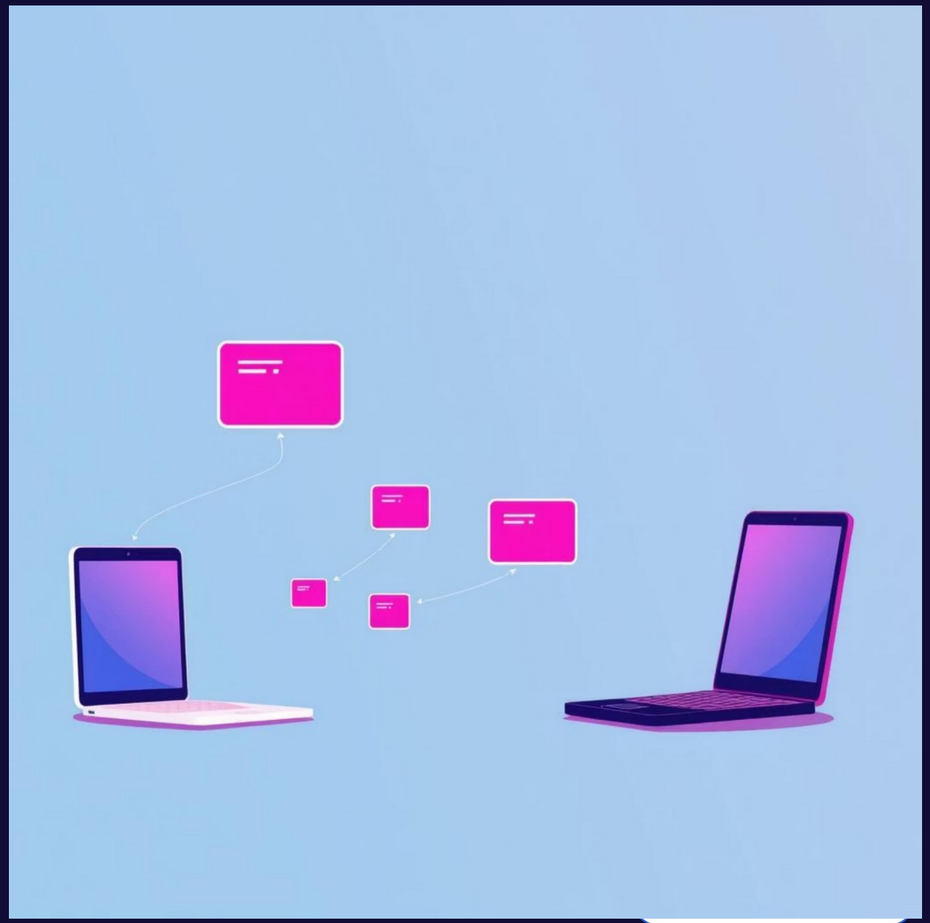
Le transfert de zone complet est la méthode la plus simple, où le serveur esclave demande et reçoit une **copie complète** de la zone du serveur maître.

- Utilisé historiquement pour tous les transferts.
- Peut être **inefficace** pour les zones volumineuses ou fréquemment mises à jour, car il transfère l'intégralité des données à chaque fois.
- Généralement utilisé lors de la configuration initiale d'un esclave ou en cas de problème avec l'IXFR.

IXFR (Incremental Zone Transfer)

Le transfert de zone incrémental permet aux serveurs esclaves de ne demander et recevoir que les **modifications** apportées à la zone depuis le dernier transfert.

- **Plus rapide et moins gourmand** en bande passante que l'AXFR.
- Requiert que le maître conserve un historique des modifications de la zone.
- C'est la méthode **préférée** pour les mises à jour régulières, assurant une synchronisation efficace.



Sécurisation : Listes de Contrôle d'Accès (ACL)

> "La sécurité DNS est primordiale pour la stabilité et la confiance de votre infrastructure réseau."

Pour prévenir les transferts de zone non autorisés, qui pourraient révéler des informations sensibles sur votre réseau, il est crucial de configurer des ACL (Access Control Lists) sur votre serveur DNS maître.

Limiter les Transferts de Zone

L'option `allow-transfer` dans la configuration de votre serveur DNS (par exemple, BIND) permet de spécifier quelles adresses IP sont autorisées à demander un transfert de zone.

```
zone "example.com" {
  type master;
  file "db.example.com";
  allow-transfer { 192.168.1.5; 192.168.1.6; };
  also-notify { 192.168.1.5; 192.168.1.6; };
};
```

Notifications Ciblées

L'option `also-notify` assure que les messages `NOTIFY` sont envoyés uniquement aux serveurs esclaves légitimes, renforçant la sécurité du processus de synchronisation.

Ces mesures sont la **première ligne de défense** contre les attaques par énumération de zone.

Option Additionnelle : TSIG (Transaction Signature)

Alors que les ACL offrent un niveau de sécurité de base, les signatures de transaction (TSIG) apportent une couche de protection cryptographique essentielle pour les transferts de zone DNS.

Signature Cryptographique

TSIG utilise des clés secrètes partagées pour signer numériquement les messages DNS, y compris les requêtes de transfert de zone. Cela garantit l'authenticité et l'intégrité des messages.

Évite le Spoofing IP

En vérifiant la signature, les serveurs DNS peuvent s'assurer que les requêtes proviennent bien d'une source autorisée, empêchant ainsi le "spoofing" d'adresses IP.

Sécurité Renforcée

Bien que non utilisé dans ce TP, l'implémentation de TSIG est **fortement recommandée** dans un environnement de production pour une sécurité maximale des transferts de zone.

Le TSIG n'est pas seulement pour les transferts ; il peut aussi sécuriser les mises à jour dynamiques DNS.

Résumé de la Partie Théorie

Les Fondamentaux du DNS Maître/Esclave

SOA

L'enregistrement **SOA** (Start of Authority) contient le **numéro de série** qui indique la version actuelle de la zone DNS. Il est crucial pour la détection des mises à jour.

ACL

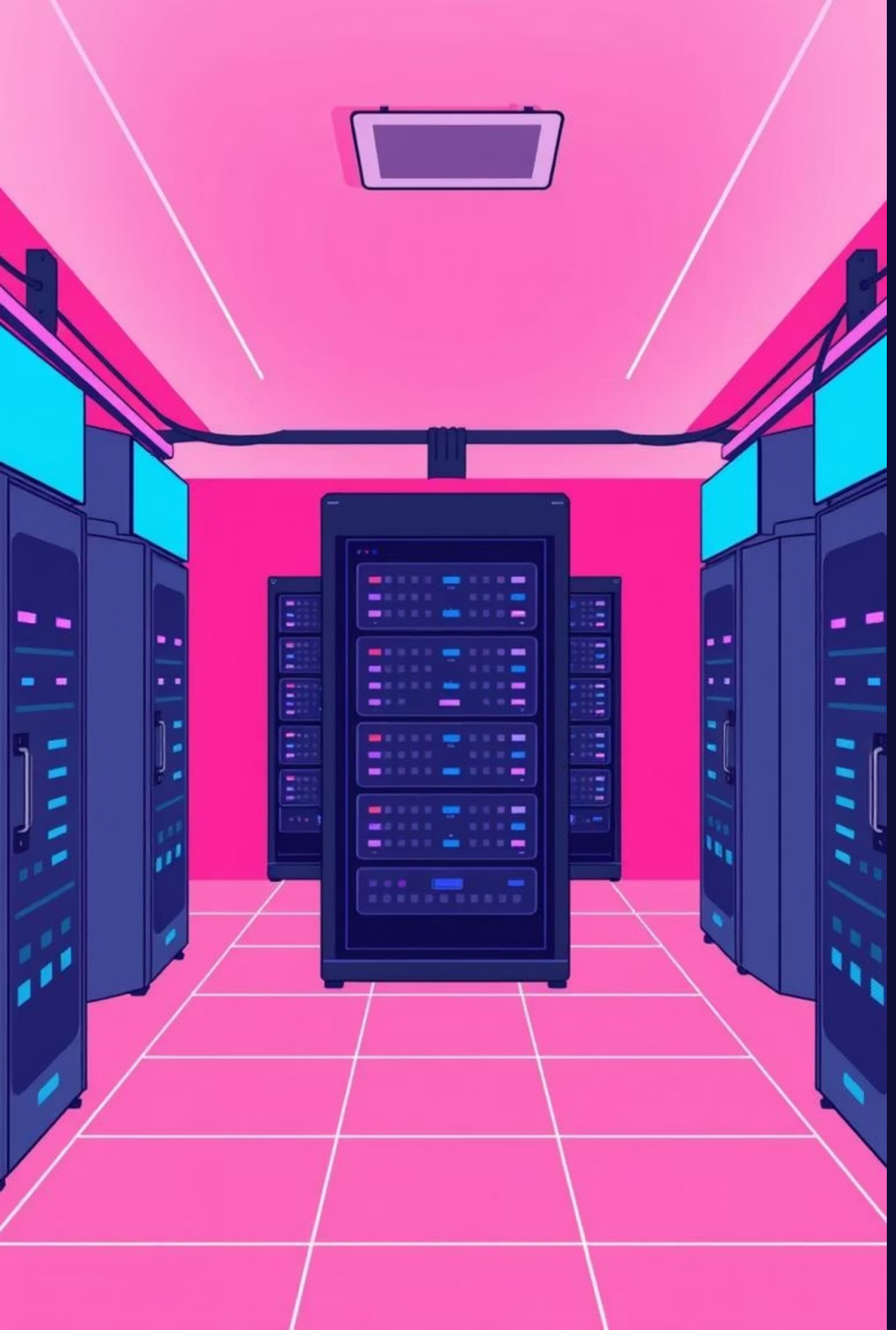
Les **ACL** (Access Control Lists) fournissent une **sécurité minimale** en contrôlant quelles adresses IP sont autorisées à demander des transferts de zone, protégeant contre l'accès non autorisé.

NOTIFY

Le mécanisme **NOTIFY** est utilisé par le serveur maître pour alerter proactivement les serveurs esclaves d'une nouvelle version de la zone, déclenchant ainsi le processus de réplication.

AXFR/IXFR

Ces sont les **méthodes de synchronisation** : **AXFR** pour un transfert complet de la zone (utilisé pour la configuration initiale ou en cas de problèmes), et **IXFR** pour un transfert incrémental des seules modifications (plus efficace).



Mise en place d'un DNS Esclave et Sécurisation ACL

Ce TP détaille la configuration d'un serveur DNS maître et esclave, incluant la réplication de zones et la sécurisation par listes de contrôle d'accès (ACL). Préparez-vous à plonger dans le cœur de la résolution de noms !

Objectifs du TP : Maîtriser la Haute Disponibilité DNS

01

Configuration du Maître

Mettre en place le serveur DNS primaire et définir les zones autoritaires.

02

Configuration de l'Esclave

Déployer le serveur DNS secondaire et le préparer pour la réplication.

03

Activation de la Réplication

S'assurer que les données de zone se synchronisent automatiquement et en toute sécurité.

04

Test et Validation

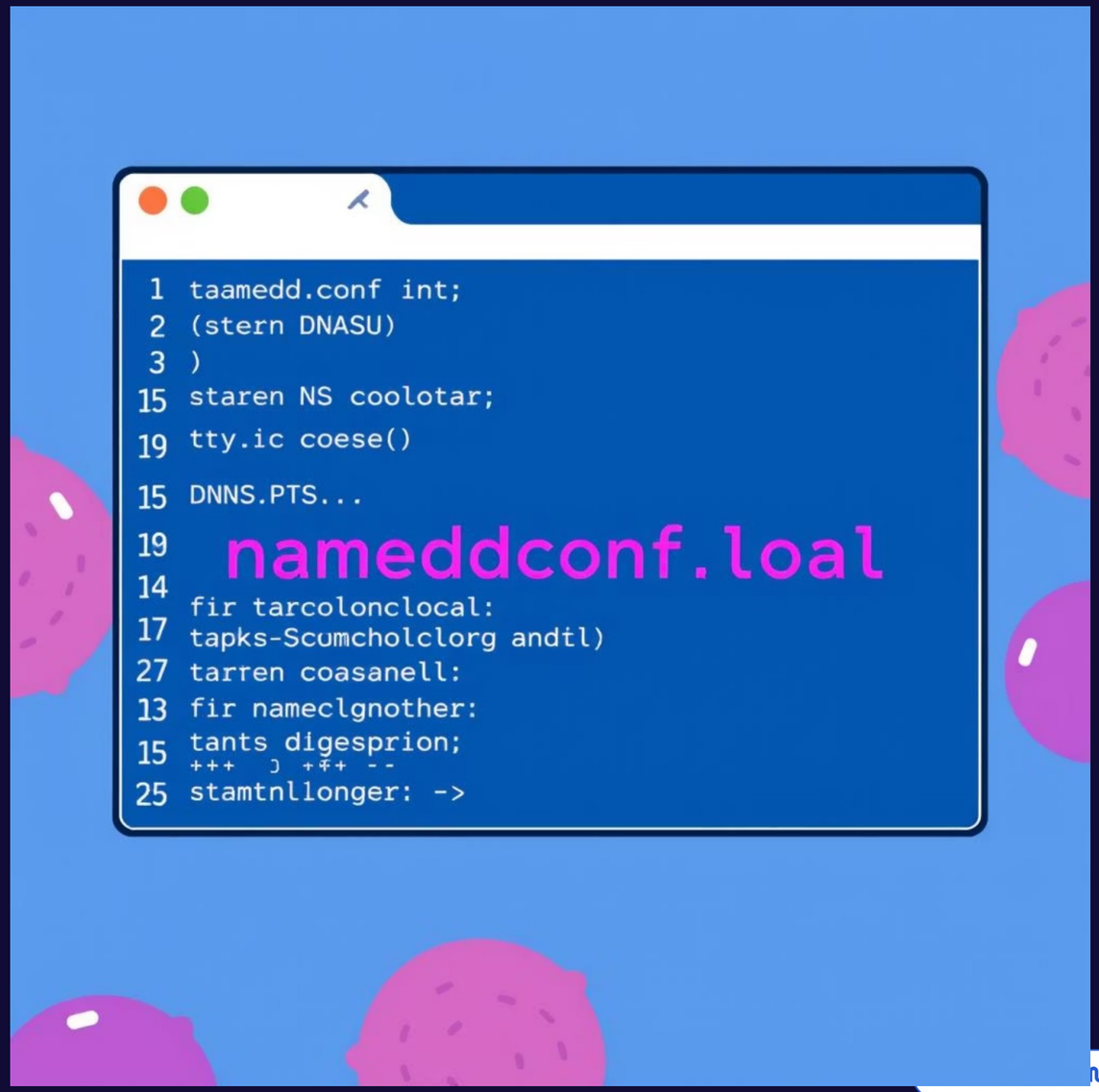
Vérifier le bon fonctionnement de l'ensemble du système DNS maître-esclave.

Étape 1 : Configuration Initiale du Serveur DNS Maître

Modification de `named.conf.local`

La première étape consiste à éditer le fichier de configuration local de Bind9 sur votre serveur maître. C'est ici que nous déclarons les zones DNS gérées par ce serveur et que nous définissons les paramètres de sécurité.

- Accédez au fichier de configuration principal de Bind9.
- Déclarez la zone et son type (maître).
- Spécifiez le chemin du fichier de zone.



rachid@srv-dns01: ~ | rachid@srv-dns02: ~ | Windows PowerShell

```
 GNU nano 8.4                    /etc/bind/named.conf.local *
// Zone directe
zone "ing-infra.lan" IN {
    type master;
    file "/etc/bind/db.ing-infra.lan";
    allow-transfer { 192.168.1.5; };   // Autoriser l'esclave
    also-notify   { 192.168.1.5; };   // Envoyer NOTIFY
};

// Zone inverse
zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/bind/db.192";
    allow-transfer { 192.168.1.5; };
    also-notify   { 192.168.1.5; };
};
// Zone de recherche directe pour le domaine principal ing-infra.lan
// You may choose to use db.ing-infra.lan to combine all records,
// or keep them separate if you intend to use View/Policy.
zone "ing-infra.lan" IN {
    type master;

^G Aide      ^O Écrire     ^F Chercher   ^K Couper     ^T Exécuter   ^C Emplacement
^X Quitter   ^R Lire fich. ^\ Remplacer  ^U Coller     ^J Justifier  ^/ Aller l
```

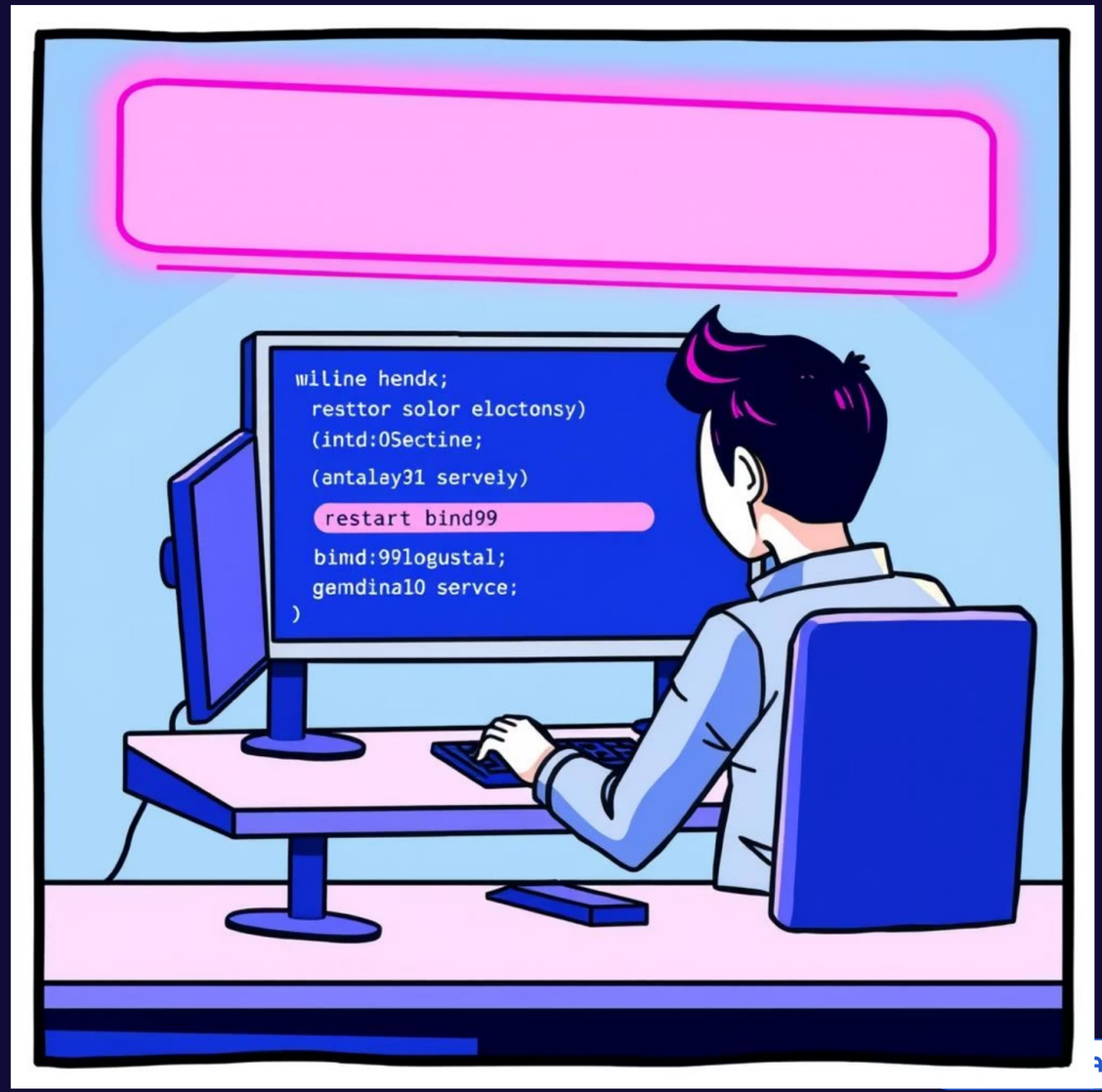
Redémarrage du Service DNS Maître

Appliquer les Modifications

Après avoir modifié le fichier `named.conf.local`, il est impératif de redémarrer le service `bind9` pour que les nouvelles configurations soient prises en compte par le serveur maître.

```
sudo systemctl restart bind9
```

- Cette commande assure que les directives ACL et `also-notify` sont activées.
- Une absence de message d'erreur indique généralement un redémarrage réussi.
- En cas de problème, vérifiez les journaux du service (`journalctl -u bind9`).



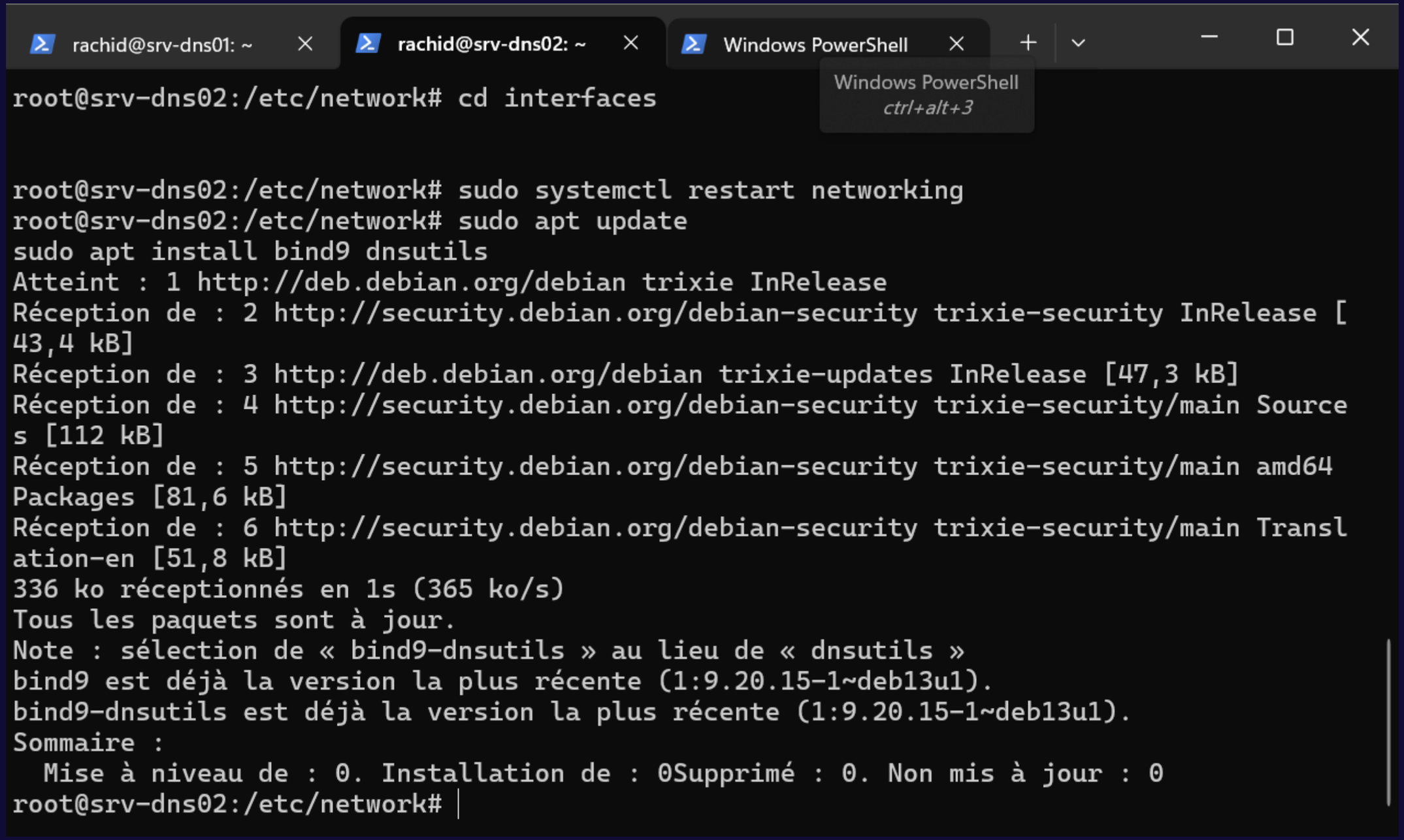
Étape 2 : Configuration du Serveur DNS Esclave

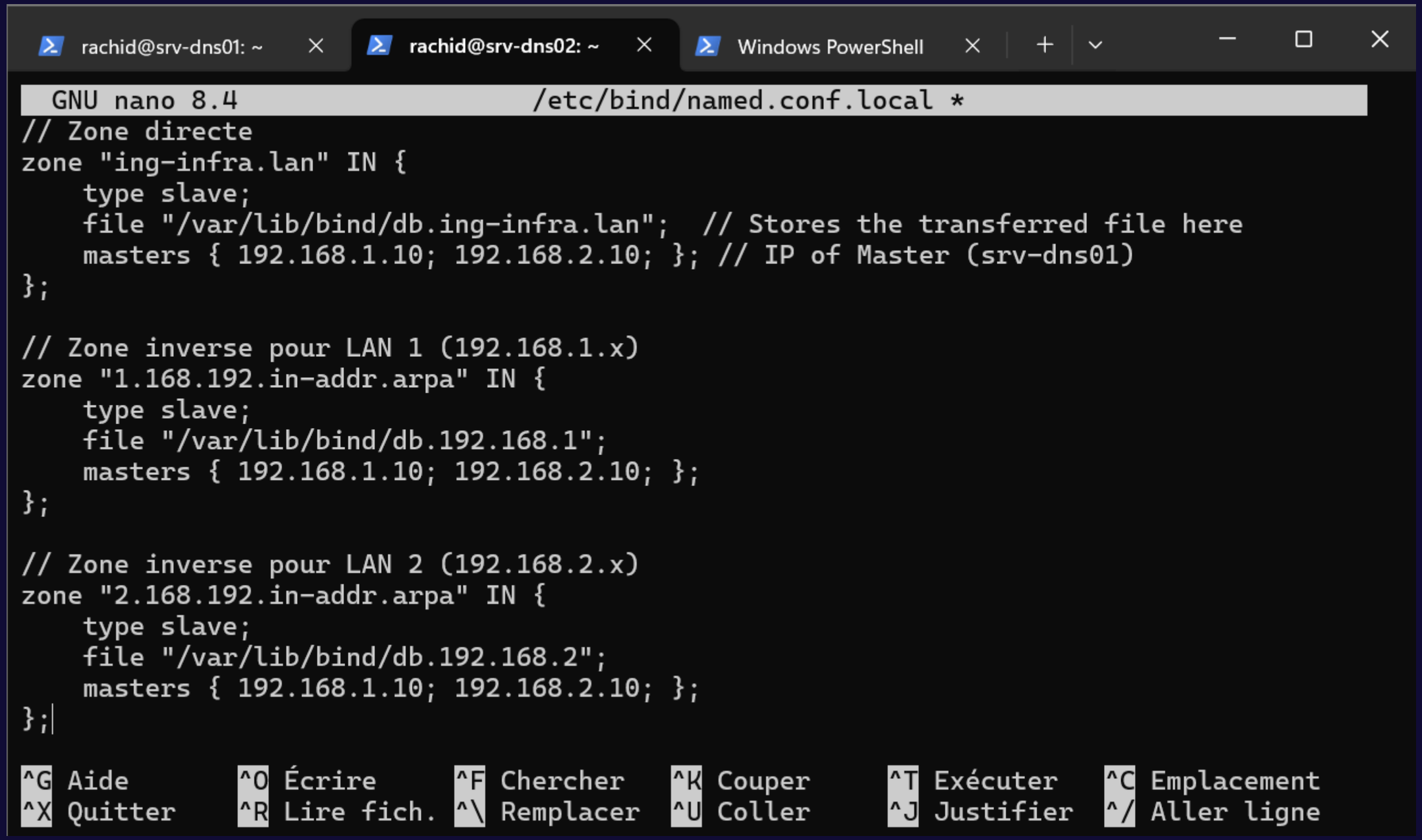
Déclaration des Zones en Mode Esclave

Sur le serveur esclave, nous devons également modifier le fichier `named.conf.local`. Cette fois, nous déclarons les zones comme étant de type `slave` et spécifions l'adresse IP du serveur maître à partir duquel l'esclave doit récupérer les données.

```
zone "inq-infra.lan" {
    type slave;
    file "/var/cache/bind/db.ing-infra.lan";
    masters { 192.168.1.10; };
};
```

- `type slave;` : Indique que ce serveur est un esclave pour cette zone.
- `file "/var/cache/bind/db.ing-infra.lan";` : Chemin où l'esclave stockera la copie locale du fichier de zone.
- `masters { 192.168.1.10; };` : Adresse IP du serveur DNS maître.


rachid@srv-dns01: ~
rachid@srv-dns02: ~
Windows PowerShell
Windows PowerShell
ctrl+alt+3
root@srv-dns02:/etc/network# cd interfaces
root@srv-dns02:/etc/network# sudo systemctl restart networking
root@srv-dns02:/etc/network# sudo apt update
sudo apt install bind9 dnsutils
Atteint : 1 http://deb.debian.org/debian trixie InRelease
Réception de : 2 http://security.debian.org/debian-security trixie-security InRelease [
43,4 kB]
Réception de : 3 http://deb.debian.org/debian trixie-updates InRelease [47,3 kB]
Réception de : 4 http://security.debian.org/debian-security trixie-security/main Source
s [112 kB]
Réception de : 5 http://security.debian.org/debian-security trixie-security/main amd64
Packages [81,6 kB]
Réception de : 6 http://security.debian.org/debian-security trixie-security/main Transl
ation-en [51,8 kB]
336 ko réceptionnés en 1s (365 ko/s)
Tous les paquets sont à jour.
Note : sélection de « bind9-dnsutils » au lieu de « dnsutils »
bind9 est déjà la version la plus récente (1:9.20.15-1~deb13u1).
bind9-dnsutils est déjà la version la plus récente (1:9.20.15-1~deb13u1).
Sommaire :
  Mise à niveau de : 0. Installation de : 0Supprimé : 0. Non mis à jour : 0
root@srv-dns02:/etc/network#


rachid@srv-dns01: ~
rachid@srv-dns02: ~
Windows PowerShell
GNU nano 8.4 /etc/bind/named.conf.local *
// Zone directe
zone "ing-infra.lan" IN {
type slave;
file "/var/lib/bind/db.ing-infra.lan"; // Stores the transferred file here
masters { 192.168.1.10; 192.168.2.10; }; // IP of Master (srv-dns01)
};
// Zone inverse pour LAN 1 (192.168.1.x)
zone "1.168.192.in-addr.arpa" IN {
type slave;
file "/var/lib/bind/db.192.168.1";
masters { 192.168.1.10; 192.168.2.10; };
};
// Zone inverse pour LAN 2 (192.168.2.x)
zone "2.168.192.in-addr.arpa" IN {
type slave;
file "/var/lib/bind/db.192.168.2";
masters { 192.168.1.10; 192.168.2.10; };
};
^G Aide ^O Écrire ^F Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne

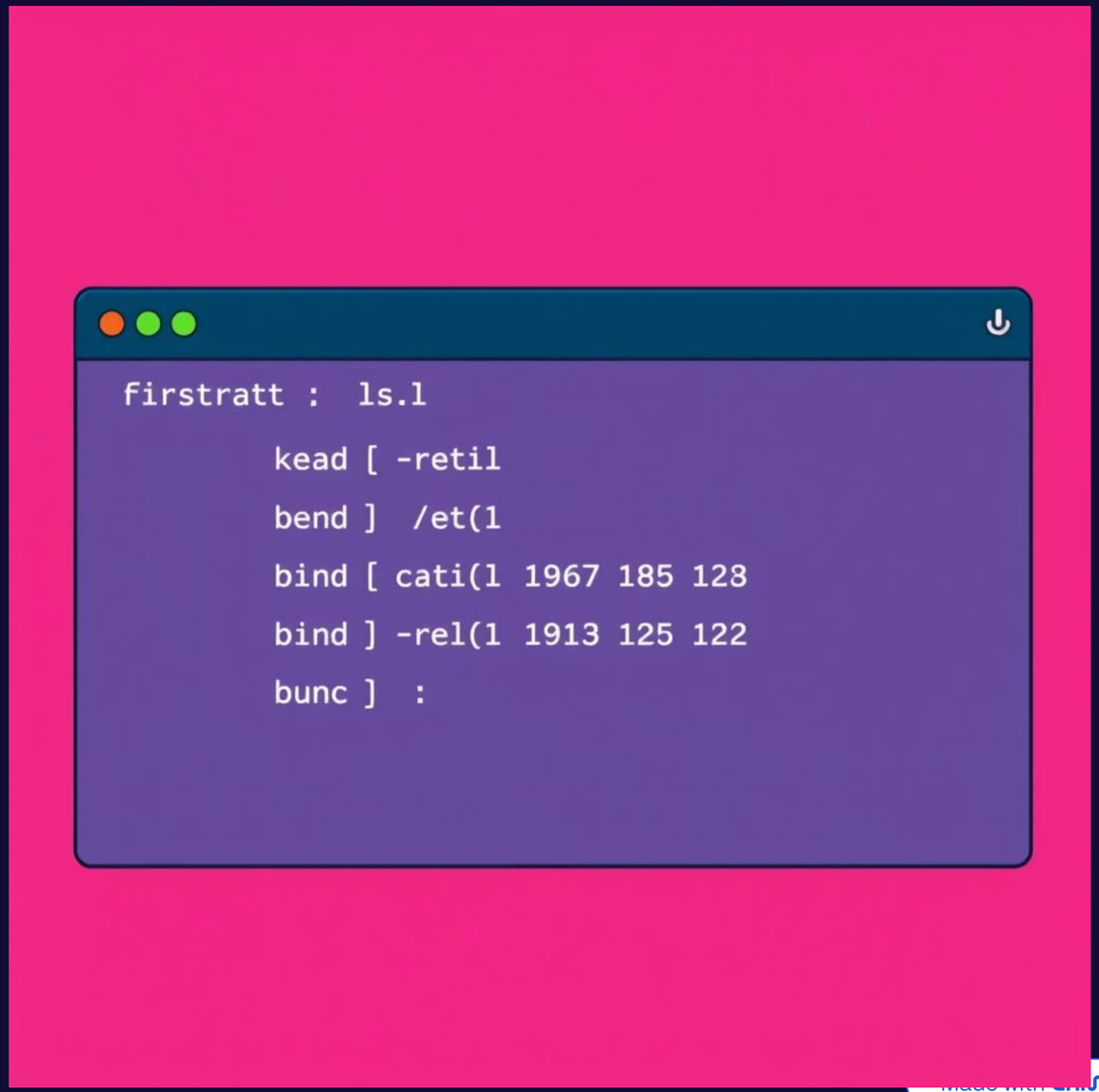
Redémarrage de l'Esclave et Vérification des Fichiers de Zone

Activation du Service et Confirmation de la Réplication

Après la configuration du fichier `named.conf.local` sur l'esclave, redémarrez le service `bind9`. L'esclave tentera alors de contacter le maître pour le transfert de zone. Utilisez `ls -l /var/cache/bind/` pour vérifier la création du fichier de zone.

```
sudo systemctl restart bind9
ls -l /var/cache/bind/
```

La présence du fichier `db.ing-infra.lan` dans `/var/cache/bind/` confirme que le transfert de zone a eu lieu avec succès.



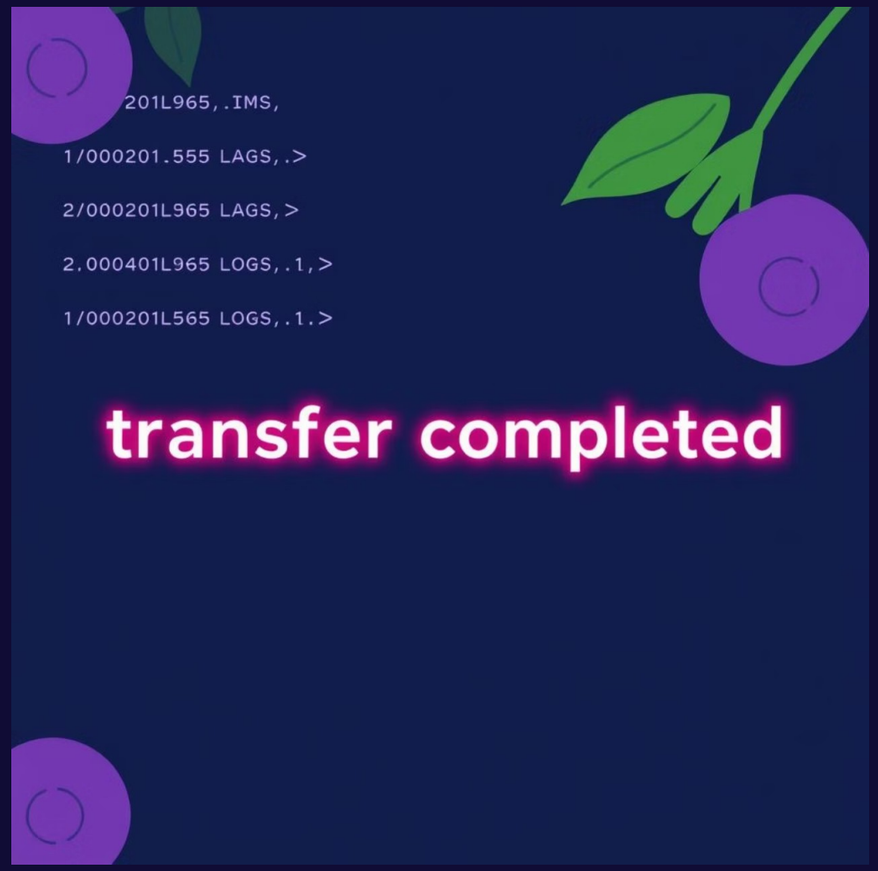
Étape 3 : Vérification des Logs pour un Transfert Réussi

Confirmation du Transfert de Zone

Pour s'assurer que la réplication a fonctionné comme prévu, il est essentiel de consulter les journaux du service `bind9` sur le serveur esclave. Nous recherchons des messages spécifiques qui indiquent un transfert de zone réussi.

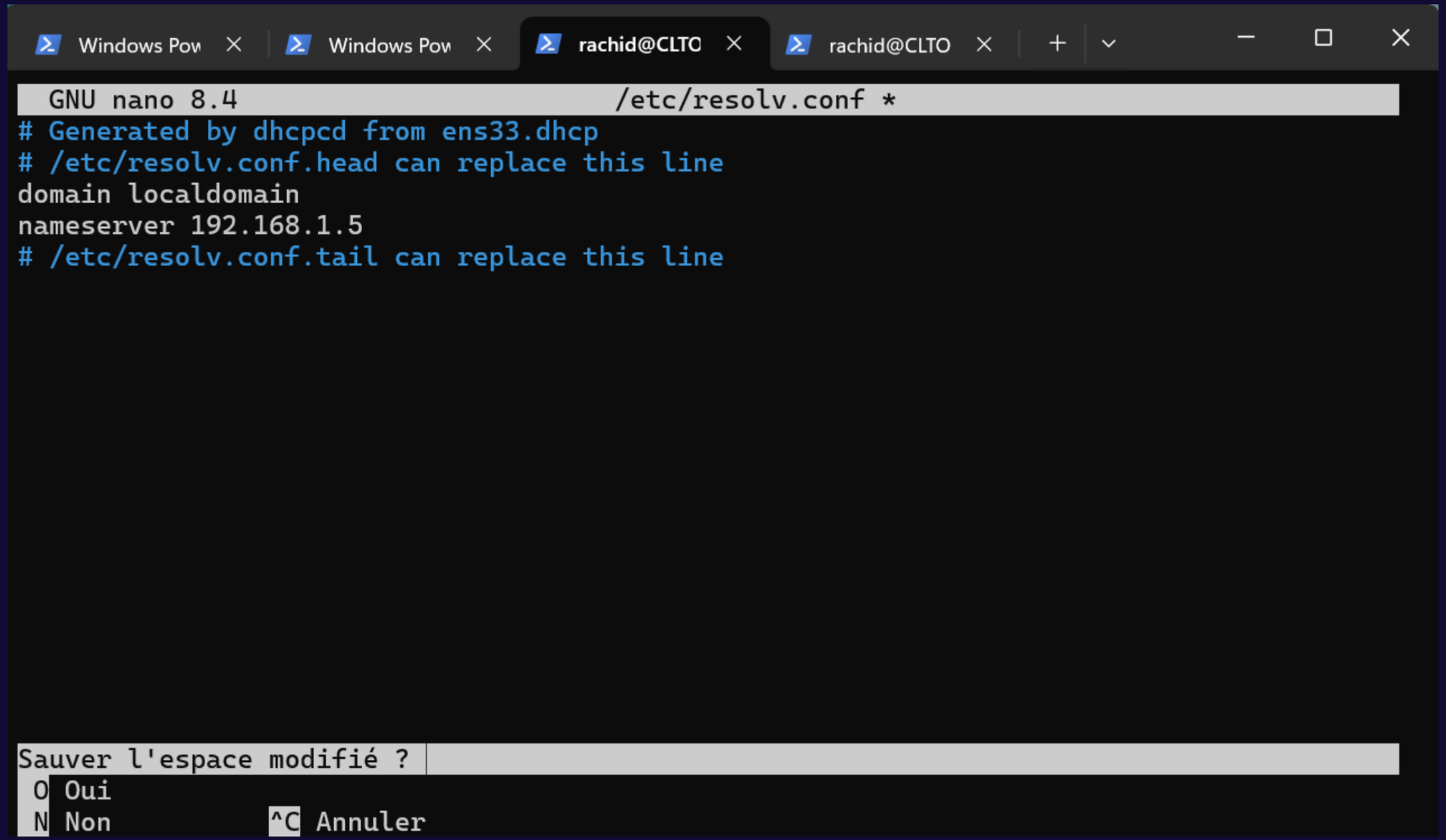
```
sudo journalctl -u bind9 -f
```

Recherchez la ligne contenant **"Transfer completed"**. Cette entrée confirme que le serveur esclave a bien reçu et appliqué la zone du maître.



```
déc. 07 22:00:01 srv-dns02 named[1258]: client @0x7f2e03b7ac00 192.168.2.10#60094: received notify for zone '2.168.192.in-addr.arpa'
déc. 07 22:00:01 srv-dns02 named[1258]: zone 2.168.192.in-addr.arpa/IN: refused notify from non-primary: 192.168.2.10#60094
déc. 07 22:00:01 srv-dns02 named[1258]: client @0x7f2e03b7e400 192.168.2.10#55165: received notify for zone '1.168.192.in-addr.arpa'
déc. 07 22:00:01 srv-dns02 named[1258]: zone 1.168.192.in-addr.arpa/IN: refused notify from non-primary: 192.168.2.10#55165
déc. 07 22:00:01 srv-dns02 named[1258]: client @0x7f2e060fec00 192.168.1.10#34200: received notify for zone '1.168.192.in-addr.arpa'
déc. 07 22:00:01 srv-dns02 named[1258]: zone 1.168.192.in-addr.arpa/IN: notify from 192.168.1.10#34200: zone is up to date
déc. 07 22:00:01 srv-dns02 named[1258]: client @0x7f2e060fd000 192.168.2.10#38259: received notify for zone 'ing-infra.lan'
déc. 07 22:00:01 srv-dns02 named[1258]: zone ing-infra.lan/IN: refused notify from non-primary: 192.168.2.10#38259
déc. 07 22:00:01 srv-dns02 named[1258]: zone ing-infra.lan/IN: Transfer started.
déc. 07 22:00:01 srv-dns02 named[1258]: 0x7f2e03a38000: transfer of 'ing-infra.lan/IN' from 192.168.1.10#53: connected using 192.168.1.10#53
déc. 07 22:00:01 srv-dns02 named[1258]: zone ing-infra.lan/IN: transferred serial 2025120702
déc. 07 22:00:01 srv-dns02 named[1258]: 0x7f2e03a38000: transfer of 'ing-infra.lan/IN' from 192.168.1.10#53: Transfer status: success
déc. 07 22:00:01 srv-dns02 named[1258]: 0x7f2e03a38000: transfer of 'ing-infra.lan/IN' from 192.168.1.10#53: Transfer completed: 1 messages, 7
0 bytes/sec) (serial 2025120702)
déc. 07 22:00:01 srv-dns02 named[1258]: zone ing-infra.lan/IN: sending notifies (serial 2025120702)
```

```
ved notify for zone 'ing-infra.lan'
déc. 07 22:00:01 srv-dns02 named[1258]: zone ing-infra.lan/IN: refused notify from non-p
rimary: 192.168.2.10#38259
déc. 07 22:00:01 srv-dns02 named[1258]: zone ing-infra.lan/IN: Transfer started.
déc. 07 22:00:01 srv-dns02 named[1258]: 0x7f2e03a38000: transfer of 'ing-infra.lan/IN' f
rom 192.168.1.10#53: connected using 192.168.1.10#53
déc. 07 22:00:01 srv-dns02 named[1258]: zone ing-infra.lan/IN: transferred serial 202512
0702
déc. 07 22:00:01 srv-dns02 named[1258]: 0x7f2e03a38000: transfer of 'ing-infra.lan/IN' f
rom 192.168.1.10#53: Transfer status: success
déc. 07 22:00:01 srv-dns02 named[1258]: 0x7f2e03a38000: transfer of 'ing-infra.lan/IN' f
rom 192.168.1.10#53: Transfer completed: 1 messages, 7 records, 221 bytes, 0.004 secs (5
5250 bytes/sec) (serial 2025120702)
déc. 07 22:00:01 srv-dns02 named[1258]: zone ing-infra.lan/IN: sending notifies (serial
2025120702)
^C
root@srv-dns02:/etc/bind# ls -l /var/cache/bind/
total 20
-rw-r--r-- 1 bind bind  381  7 déc.  21:53 db.192.168.1
-rw-r--r-- 1 bind bind  381  7 déc.  21:53 db.192.168.2
-rw-r--r-- 1 bind bind  364  7 déc.  22:00 db.ing-infra.lan
-rw-r--r-- 1 bind bind 1411  7 déc.  21:54 managed-keys.bind
-rw-r--r-- 1 bind bind 1766  7 déc.  21:54 managed-keys.bind.jnl
root@srv-dns02:/etc/bind#
```


Windows Pow
Windows Pow
rachid@CLTO
rachid@CLTO
GNU nano 8.4 /etc/resolv.conf *
Generated by dhcpcd from ens33.dhcp
/etc/resolv.conf.head can replace this line
domain localdomain
nameserver 192.168.1.5
/etc/resolv.conf.tail can replace this line
Sauver l'espace modifié ?
O Oui
N Non
^C Annuler

```
; <<>> DiG 9.20.15-1~deb13u1-Debian <<>> srv-web01.ing-infra.lan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 30376
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b1dd1173d278fffc010000006935eba6e3fa58df4f523687 (good)
;; QUESTION SECTION:
;srv-web01.ing-infra.lan.       IN      A

;; AUTHORITY SECTION:
ing-infra.lan.          604800  IN      SOA     srv-dns01.ing-infra.lan. admin.ing-infra
.lan. 2025120702 604800 86400 2419200 604800

;; Query time: 4 msec
;; SERVER: 192.168.1.5#53(192.168.1.5) (UDP)
;; WHEN: Sun Dec 07 22:03:34 CET 2025
;; MSG SIZE  rcvd: 132

root@CLTO1:/home/rachid#
```

Étape 4 : Test de Résolution DNS depuis un Client

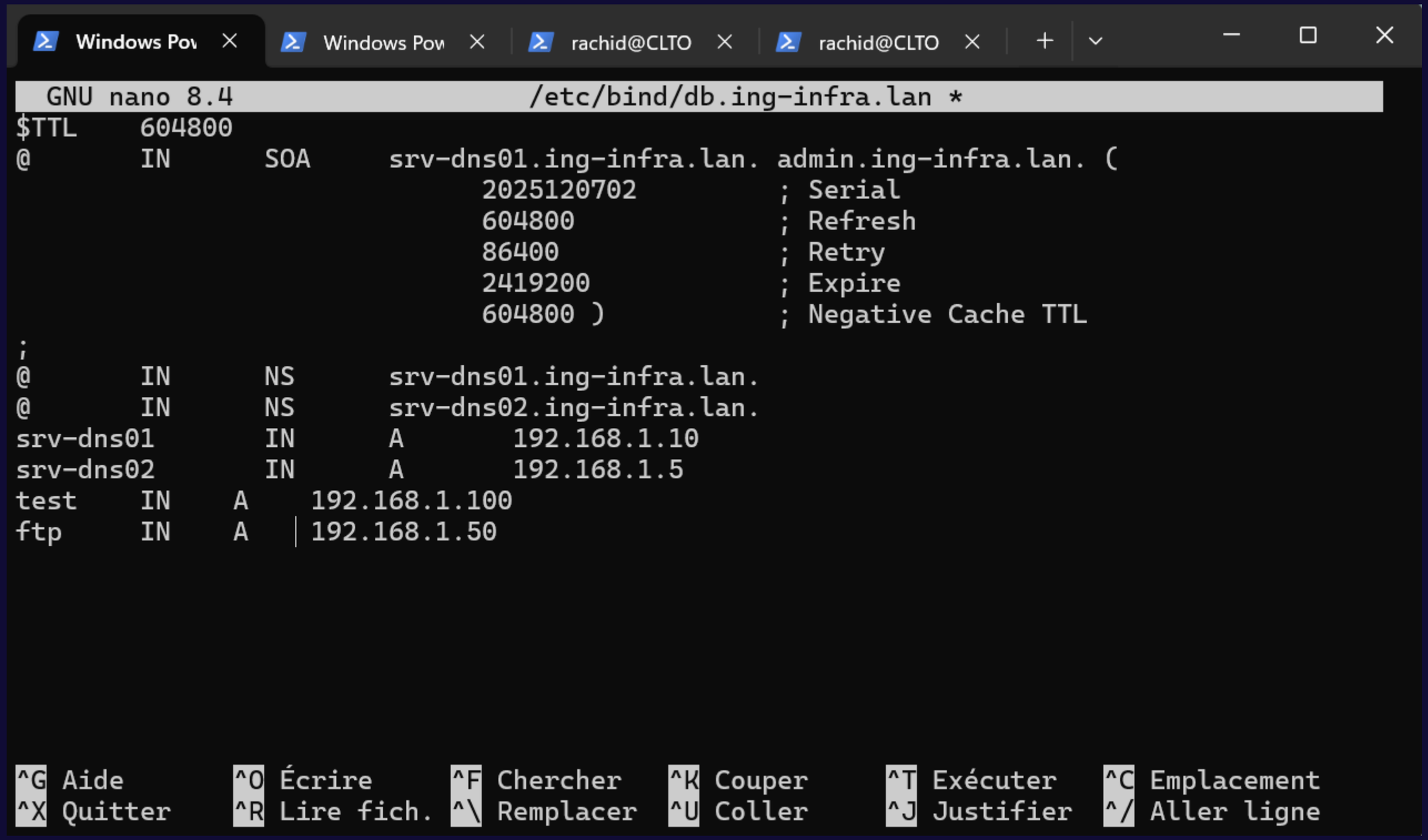
Validation de la Résolution de Noms via l'Esclave

Après toutes les étapes de configuration et de vérification des logs, il est temps de tester la résolution de noms à partir d'un poste client, en ciblant spécifiquement le serveur DNS esclave.

```
dig @192.168.1.5 ftp.ing-infra.lan
```

Un résultat positif, affichant l'adresse IP correcte pour `ftp.ing-infra.lan`, confirme que :

- Le serveur esclave est opérationnel.
- La réplication de zone est fonctionnelle.
- La sécurisation ACL n'a pas empêché le transfert de zone autorisé.


Windows Pov
Windows Pow
rachid@CLTO
rachid@CLTO
GNU nano 8.4 /etc/bind/db.ing-infra.lan *
$TTL 604800
@ IN SOA srv-dns01.ing-infra.lan. admin.ing-infra.lan. (
2025120702 ; Serial
604800 ; Refresh
86400 ; Retry
2419200 ; Expire
604800) ; Negative Cache TTL
;
@ IN NS srv-dns01.ing-infra.lan.
@ IN NS srv-dns02.ing-infra.lan.
srv-dns01 IN A 192.168.1.10
srv-dns02 IN A 192.168.1.5
test IN A 192.168.1.100
ftp IN A 192.168.1.50
^G Aide ^O Écrire ^F Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^\ Remplacer ^U Coller ^J Justifier ^/ Aller ligne

Windows Pow | Windows Pow | rachid@CLTO | rachid@CLTO

```
; <<>> DiG 9.20.15-1~deb13u1-Debian <<>> @192.168.1.5 ftp.ing-infra.lan
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23866
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4c6462bce9c99991010000006935eca908ec2889ddacaab3 (good)
;; QUESTION SECTION:
;ftp.ing-infra.lan.             IN      A

;; ANSWER SECTION:
ftp.ing-infra.lan.      604800  IN      A       192.168.1.50

;; Query time: 4 msec
;; SERVER: 192.168.1.5#53(192.168.1.5) (UDP)
;; WHEN: Sun Dec 07 22:07:53 CET 2025
;; MSG SIZE  rcvd: 90

root@CLTO1:/home/rachid#
```

Conclusion du TP : DNS Esclave Opérationnel et Sécurisé

Félicitations ! Vous avez successfully configuré un environnement DNS maître-esclave sécurisé. Ce travail est fondamental pour la haute disponibilité et la robustesse de votre infrastructure réseau.

Réplication Automatique OK

Les mises à jour de zone sont transférées efficacement du maître à l'esclave.

Sécurisation via ACL OK

Les transferts de zone sont contrôlés, empêchant tout accès non autorisé.

Esclave Opérationnel et Synchronisé

Votre serveur esclave est prêt à prendre le relais en cas de défaillance du maître.

```
root@srv-dns01:~# nano /etc/bind/db.ing-infra.lan
root@srv-dns01:~# sudo journalctl -u bind9 -f
^Xsudo journalctl -u bind9 -f^C
root@srv-dns01:~# sudo systemctl restart bind9
root@srv-dns01:~# nano /etc/bind/db.ing-infra.lan
root@srv-dns01:~# sudo systemctl restart bind9
root@srv-dns01:~# dnssec-keygen -a RSASHA256 -b 2048 -n ZONE ing-infra.lan
Generating key pair..+.........+.......+....+...+...+..++++++++++++++++++++++++++++++
+++++++*.+.....+.....+.......+.........++++++++++++++++++++++++++++++++++++++++*.....
+.........+.+...+..............+....+......+.....+........+......+...........+..+.
+..........+...+.....+....+........+......+..........+...+..............+........+
.+.....+....+..+.+..+...++++++ ....+....+..+...+++++++++++++++++++++++++++++++++++*.
+.......+...+...+.....+.........++++++++++++++++++++++++++++++++++*.......+........
....+...+....+...+.....+..........+..+...+.......+.....+....+.........+..............
..................+.+..+....+........+.+.........+...+.........+...+..+....+.....+......
+......+.......+...+.....+..........+...+.....+......+..............+..........+...+...
+.....................+.+........+...+....+.....+.+..+...+....+................+....
..+......+...+........+....+...+........+...+....+.....+.+......+......+.....+.........+
.........+....+..+....+..+...+....+..+.+...+......+.....+..........+.........+..+.......
+...+...+...........+.........+.+.....................+.....+...+....+...+..+....+..
...+....+.....+..............+....+..+....+............+..+.+.....+....+...+..+...+...+
..................+..+...+...+....+...+.....++++++
King-infra.lan.+008+21898
root@srv-dns01:~#
```