



# DOCUMENTATION TECHNIQUE

Configuration BIND9 pour la Haute Disponibilité avec  
Keepalived

---

Système : DNS BIND9 + Keepalived

Version : 1.0

Date : Mars 2025

Statut : Document de référence



## Table des matières

Table des matières .....	3
1. Introduction .....	4
2. Prérequis .....	<b>Erreur ! Signet non défini.</b>
3. Étapes de Configuration.....	4
3.1 Création du fichier de zone inverse – db.10.11.10.13 .....	4
3.2 Création du fichier de zone directe – db.saveol.coop.....	5
3.3 Déclaration des fichiers de zone dans named.conf.....	5
4. Suppression des Anciennes Configurations .....	6
4.1 Vérification des fichiers existants.....	6
4.2 Création du dossier d'archivage – old_file .....	6
4.3 Déplacement des anciens fichiers de configuration .....	7
5. Résultats et Vérifications.....	7
5.1 Résultat de l'organisation des fichiers.....	7
5.2 État du service BIND9 .....	7
5.3 Tests de résolution DNS.....	<b>Erreur ! Signet non défini.</b>
5.4 Vérification de la haute disponibilité.....	<b>Erreur ! Signet non défini.</b>
5.5 Configuration Keepalived – Bascule automatique.....	10
5.6 Partage NFS – Accès au contenu du site web .....	12
6. Commandes de Référence .....	13
7. Dépannage .....	<b>Erreur ! Signet non défini.</b>
8. Conclusion .....	<b>Erreur ! Signet non défini.</b>

## 1. Introduction

Ce document décrit les étapes de modification de notre serveur DNS BIND9 dans un environnement de haute disponibilité (HA) utilisant Keepalived. L'objectif est de garantir la continuité de service DNS en cas de défaillance d'un des serveurs ou applications, via l'utilisation d'une adresse IP virtuelle partagée entre plusieurs serveurs.

Composant	Description
<b>BIND9</b>	Serveur DNS open-source – résolution de noms de domaine
<b>Keepalived</b>	Démon VRRP assurant la bascule automatique de l'IP virtuelle
<b>IP virtuelle</b>	Adresse IP partagée garantissant la continuité de service
<b>Zone DNS</b>	Fichiers de zone définissant les enregistrements de résolution

## 3. Étapes de Configuration

Les étapes ci-dessous décrivent la procédure complète de modification de BIND9 pour intégrer la haute disponibilité. Chaque étape est illustrée par une capture d'écran de la commande exécutée.

### 3.1 Création du fichier de zone inverse – db.10.11.10.13

**1**

#### Fichier de zone inverse

Création du fichier de zone DNS inverse pour la résolution PTR de l'adresse 10.11.10.13

La première étape consiste à créer le fichier de zone inverse correspondant à l'adresse IP 10.11.10.13. Ce fichier permettra la résolution inverse (PTR record) dans BIND9.

Commande exécutée :

```
nano db.10.11.10.13
```

```
GNU nano 7.2 db.10.11.10.13
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.saveol.coop. admin.saveol.coop. (
; Serial
          1         ; Refresh
          604800    ; Retry
          86400     ; Expire
          2419200   ; Negative Cache TTL
          604800 )
;
@         IN      NS       ns.saveol.coop.
13.10    IN      PTR      www.saveol.coop.
```

Figure 1 – Création et édition du fichier de zone inverse db.10.11.10.13

## 3.2 Création du fichier de zone directe – db.saveol.coop

### 2

#### Fichier de zone directe

Création du fichier de zone DNS directe pour le domaine saveol.coop

Cette étape crée le fichier de zone directe qui contiendra les enregistrements A, MX, NS et autres pour le domaine saveol.coop.

Commande exécutée :

```
nano db.saveol.coop
```

```
GNU nano 7.2 db.saveol.coop
$TTL 604800
@      IN      SOA      ns.saveol.coop. admin.saveol.coop. (
                        2          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@      IN      NS       ns.saveol.coop.
@      IN      A        10.11.10.13
www    IN      A        10.11.10.13
ns     IN      A        10.11.10.13
```

Figure 2 – Création et édition du fichier de zone directe db.saveol.coop

## 3.3 Déclaration des fichiers de zone dans named.conf

### 3

#### Déclaration des zones

Référencement des fichiers de zone dans la configuration principale de BIND9

Une fois les fichiers de zone créés, il est nécessaire de les déclarer dans le fichier de configuration de BIND9 (named.conf.local) pour que le serveur DNS puisse les charger au démarrage.

```
GNU nano 7.2 named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "saveol.coop" {
    type master;
    file "/etc/bind/db.saveol.coop";
};

zone "10.13.in-addr.arpa" {
    type master;
    file "/etc/bind/db.10.11.10.13";
};
```

Figure 3 – Déclaration des nouvelles zones dans named.conf

## 4. Suppression des Anciennes Configurations

Après l'intégration des nouveaux fichiers de zone, il est indispensable d'archiver les anciennes configurations pour éviter toute confusion.

### 4.1 Vérification des fichiers existants

#### 4

#### Vérification

Listage des fichiers de configuration présents avant nettoyage

Avant toute suppression, il convient de lister les fichiers existants afin d'identifier ceux à archiver (db.10.11.10.11.old, db.saveol.coop.old).

```
root@srvweb:/etc/bind# ls
bind.keys  db.10.11.10.11.old  db.127  db.empty  db.saveol.coop  named.conf
named.conf.local  rndc.key
db.0  db.10.11.10.13  db.255  db.local  db.saveol.coop.old  named.conf.default-zones
named.conf.options  zones.rfc1918
root@srvweb:/etc/bind#
```

Figure 4 – Vérification des fichiers de configuration existants

### 4.2 Création du dossier d'archivage – old\_file

#### 5

#### Création du dossier archive

Création d'un répertoire dédié pour sauvegarder les anciens fichiers

Un dossier `old_file` est créé pour stocker les anciens fichiers de configuration, permettant une restauration rapide en cas de besoin ou d'erreur.

```
root@srvweb:/etc/bind# mkdir old_file
root@srvweb:/etc/bind# ls
bind.keys  db.10.11.10.11.old  db.127  db.empty  db.saveol.coop  named.conf  named.conf.local  old_file  zones.rfc1918
db.0      db.10.11.10.13    db.255  db.local  db.saveol.coop.old  named.conf.default-zones  named.conf.options  rndc.key
```

Figure 5 – Création du répertoire `old_file`

## 4.3 Déplacement des anciens fichiers de configuration

### 6

#### Archivage

Déplacement des anciens fichiers vers le répertoire d'archive

Les anciens fichiers de zone sont déplacés dans le dossier `old_file`. Cette opération préserve les données tout en améliorant la visibilité de la configuration.

```
root@srvweb:/etc/bind# mv db.10.11.10.11.old old_file/
root@srvweb:/etc/bind# mv db.saveol.coop.old old_file/
root@srvweb:/etc/bind# ls
bind.keys  db.10.11.10.13  db.255  db.local  named.conf  named.conf.local  old_file  zones.rfc1918
db.0      db.127          db.empty  db.saveol.coop  named.conf.default-zones  named.conf.options  rndc.key
```

Figure 6 – Déplacement des anciens fichiers de configuration vers `old_file`

## 5. Résultats et Vérifications

Après avoir effectué toutes les modifications, il est essentiel de vérifier le bon fonctionnement de la configuration BIND9. Cette section présente les captures d'écran des résultats obtenus lors des vérifications.

### 5.1 Résultat de l'organisation des fichiers

```
root@srvweb:/home/srv_web# cd /etc/bind
root@srvweb:/etc/bind# ls
bind.keys  db.127  db.local  named.conf.default-zones  old_file
db.0      db.255  db.saveol.coop  named.conf.local  rndc.key
db.10.11.10.13  db.empty  named.conf  named.conf.options  zones.rfc1918
root@srvweb:/etc/bind#
```

Figure 7 – Vue de l'organisation des fichiers après nettoyage

### 5.2 État du service BIND9

Redémarrage et vérification du statut du service `named` après application des modifications.

```
valtd _ttl forever preferred_ttl forever
root@srvweb:/home/srv_web# systemctl restart bind9
root@srvweb:/home/srv_web# systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
   Active: active (running) since Fri 2026-03-13 07:52:46 UTC; 31s ago
     Docs: man:named(8)
   Main PID: 115833 (named)
    Status: "running"
     Tasks: 8 (limit: 4608)
    Memory: 22.9M (peak: 23.3M)
       CPU: 100ms
    CGroup: /system.slice/named.service
           └─115833 /usr/sbin/named -f -u bind
```

### 5.3 Configuration de la redirection DNS sur l'AD

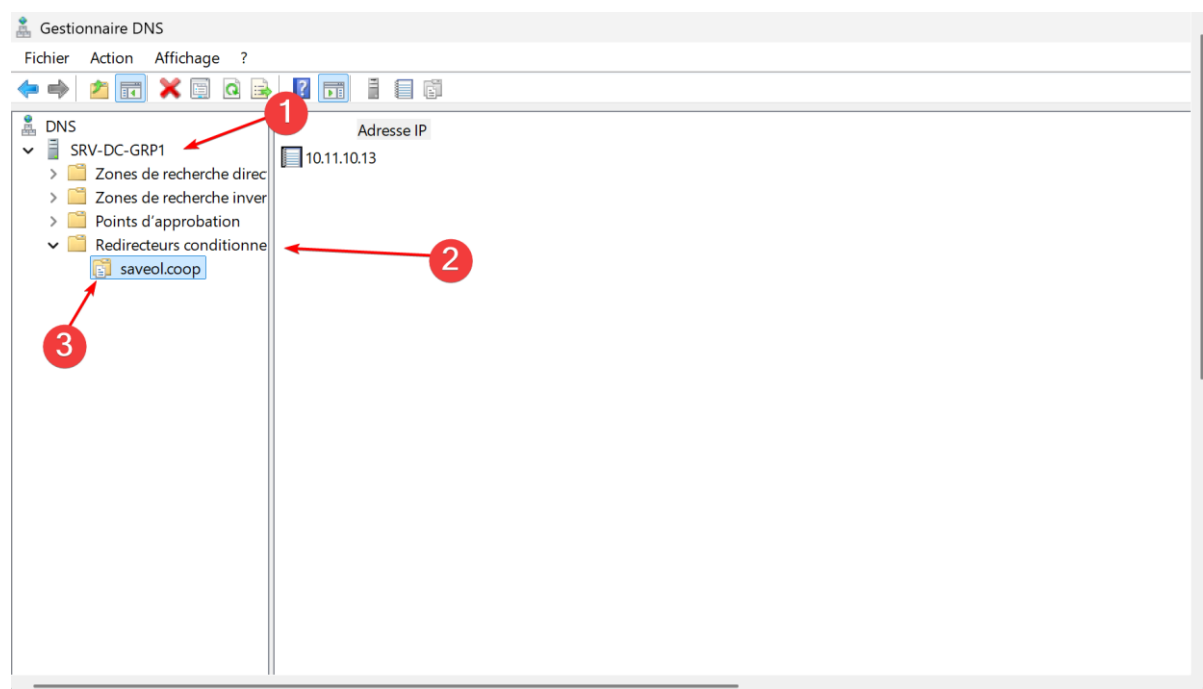


Figure 8 – Statut du service BIND9 (named) après redémarrage

Modifier l'ancienne adresse du redirecteur

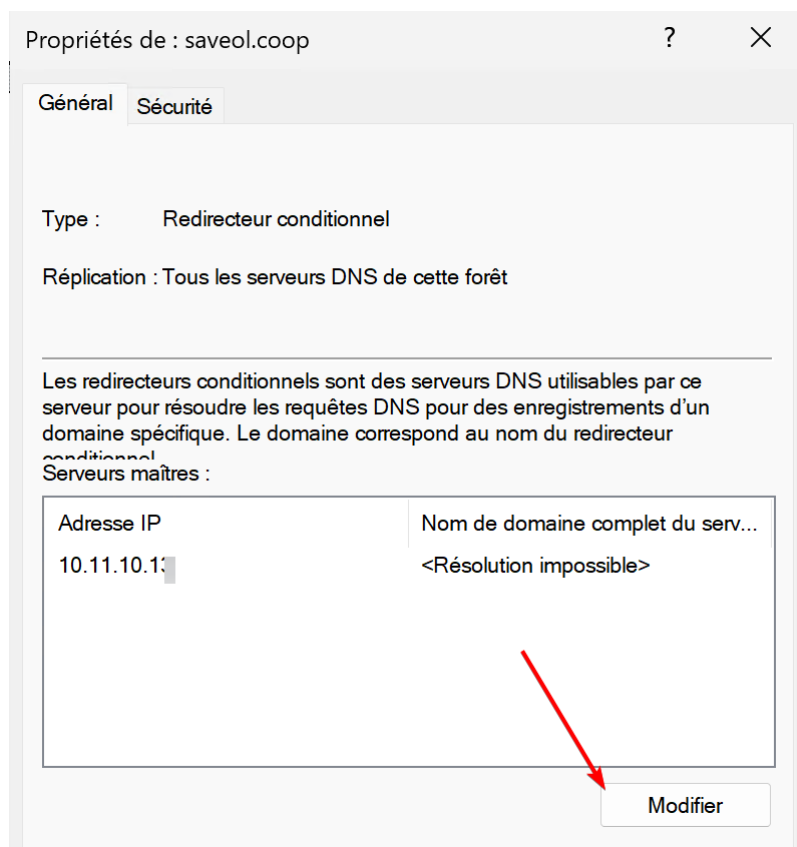


Figure 9 – Tests de résolution DNS (zones directe et inverse)

Ajouter l'adresse IP virtuelle 10.11.10.13

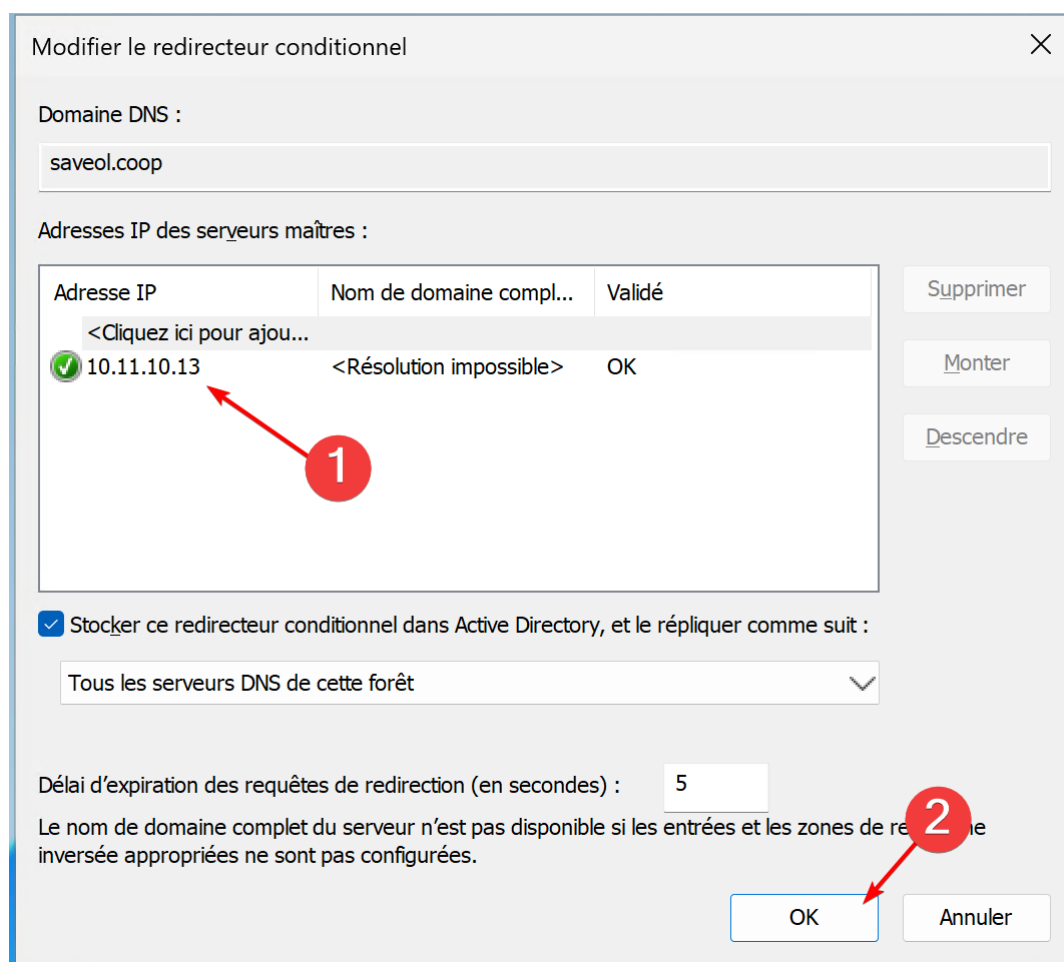


Figure 10 – Vérification du mécanisme de haute disponibilité Keepalived

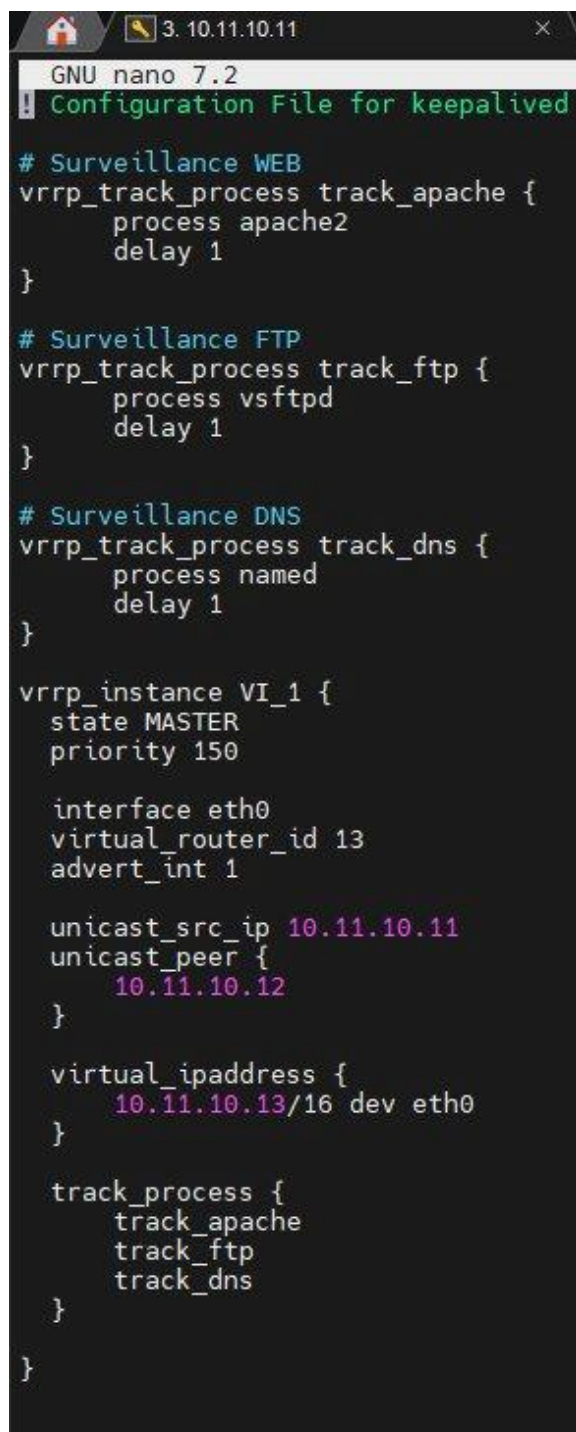
## 5.5 Configuration Keepalived – Bascule automatique

Afin de garantir la haute disponibilité du service web, Keepalived est configuré pour effectuer une bascule automatique vers le serveur de secours dans les cas suivants :

- Arrêt ou indisponibilité du serveur web physique principal
- Chute du service Apache2 (serveur web)
- Chute du service vsftpd (FTP)
- Chute du service named (DNS)

La surveillance de chaque service est définie via des blocs `vrrp_track_process` dans le fichier de configuration Keepalived. Le serveur MASTER possède la priorité 150 et le serveur BACKUP la priorité 149. L'option `nopreempt` sur le BACKUP empêche une reprise prématurée du rôle MASTER lors du redémarrage du serveur principal.

### Configuration du serveur MASTER (10.11.10.11)



```
GNU nano 7.2
! Configuration File for keepalived

# Surveillance WEB
vrrp_track_process track_apache {
    process apache2
    delay 1
}

# Surveillance FTP
vrrp_track_process track_ftp {
    process vsftpd
    delay 1
}

# Surveillance DNS
vrrp_track_process track_dns {
    process named
    delay 1
}

vrrp_instance VI_1 {
    state MASTER
    priority 150

    interface eth0
    virtual_router_id 13
    advert_int 1

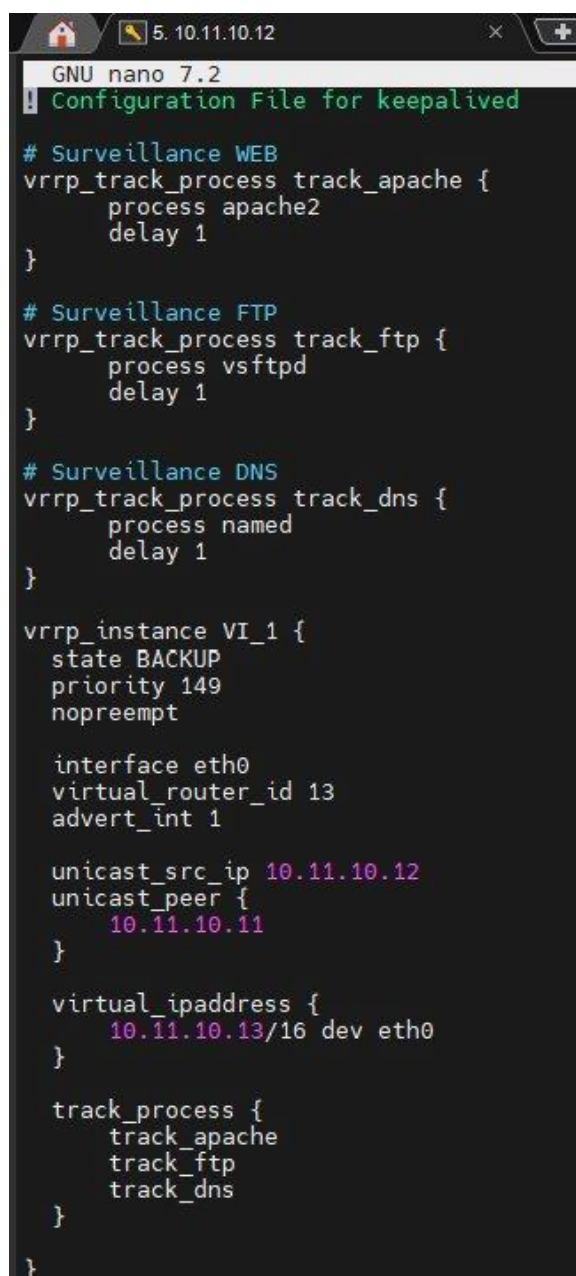
    unicast_src_ip 10.11.10.11
    unicast_peer {
        10.11.10.12
    }

    virtual_ipaddress {
        10.11.10.13/16 dev eth0
    }

    track_process {
        track_apache
        track_ftp
        track_dns
    }
}
}
```

Figure 11 – Configuration Keepalived – Serveur MASTER (10.11.10.11), priorité 150

### Configuration du serveur BACKUP (10.11.10.12)



```
GNU nano 7.2
! Configuration File for keepalived

# Surveillance WEB
vrrp_track_process track_apache {
    process apache2
    delay 1
}

# Surveillance FTP
vrrp_track_process track_ftp {
    process vsftpd
    delay 1
}

# Surveillance DNS
vrrp_track_process track_dns {
    process named
    delay 1
}

vrrp_instance VI_1 {
    state BACKUP
    priority 149
    noreempt

    interface eth0
    virtual_router_id 13
    advert_int 1

    unicast_src_ip 10.11.10.12
    unicast_peer {
        10.11.10.11
    }

    virtual_ipaddress {
        10.11.10.13/16 dev eth0
    }

    track_process {
        track_apache
        track_ftp
        track_dns
    }
}
}
```

Figure 12 – Configuration Keepalived – Serveur BACKUP (10.11.10.12), priorité 149 avec noreempt

## 5.6 Partage NFS – Accès au contenu du site web

Le contenu du site web (répertoire `/var/www/html`) est hébergé sur le serveur de base de données `10.12.10.31` et est exposé via NFS. Les deux serveurs web (MASTER et BACKUP) montent ce partage afin d'accéder aux mêmes fichiers du site en permanence, y compris lors d'une bascule.

Le fichier `/etc/exports` sur le serveur `10.12.10.31` autorise explicitement les deux serveurs web à monter le répertoire en lecture/écriture :

```

GNU nano 7.2 /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes gss/krb5i(rw,sync,no_subtree_check)
#
/var/www/html 10.11.10.11(rw,sync,no_root_squash,no_subtree_check)
/var/www/html 10.11.10.12(rw,sync,no_root_squash,no_subtree_check)

```

Figure 13 – Contenu de /etc/exports sur le serveur 10.12.10.31 – Autorisation des deux serveurs web

Les options `rw`, `sync`, `no_root_squash`, `no_subtree_check` permettent un accès en lecture/écriture synchrone, avec conservation des privilèges root, ce qui est nécessaire pour qu'Apache puisse écrire dans le répertoire web partagé. Ce partage est monté au démarrage sur les deux serveurs via `/etc/fstab` afin de garantir la disponibilité du contenu même après redémarrage.

## 6. Commandes de Référence

Récapitulatif des commandes utilisées lors de cette procédure :

Commande	Description
<code>nano db.10.11.10.13</code>	Création/édition du fichier de zone inverse
<code>nano db.saveol.coop</code>	Création/édition du fichier de zone directe
<code>nano /etc/bind/named.conf.local</code>	Déclaration des zones dans BIND9
<code>ls -la /etc/bind/</code>	Vérification des fichiers de configuration
<code>mkdir old_file</code>	Création du répertoire d'archivage
<code>mv &lt;ancien_fichier&gt; old_file/</code>	Déplacement des anciens fichiers
<code>systemctl restart named</code>	Redémarrage du service BIND9
<code>systemctl status named</code>	Vérification du statut du service
<code>named-checkconf</code>	Validation de la syntaxe de la configuration
<code>named-checkzone saveol.coop db.saveol.coop</code>	Vérification du fichier de zone directe
<code>dig @localhost saveol.coop</code>	Test de résolution DNS directe
<code>systemctl status keepalived</code>	Vérification du statut Keepalived