AN

Hôpital LEIDOSCOPE · BTS SIO SISR · Infrastructure réseau

DOCUMENTATION TECHNIQUE

Haute Disponibilité avec Keepalived

Adrien Notfell	Mars 2026	Debian 12	Hyper-V

Clonage VM · VRRP · Nginx · vsftpd · BIND · NAT · DNS

1. CONTEXTE ET OBJECTIFS

Ce document décrit la mise en place d'une infrastructure de haute disponibilité (HA) basée sur Keepalived et le protocole VRRP pour l'hôpital LEIDOSCOPE. L'objectif est de garantir la continuité de service des applications critiques (web, FTP, DNS) même en cas de panne d'un serveur. Une VIP (Virtual IP) flottante 10.51.10.67 est partagée entre les deux nœuds : le MASTER la détient en temps normal, le BACKUP la récupère automatiquement en cas de défaillance.

Services déployés

Service	Statut	Rôle
nginx	☑ Actif	Serveur web / reverse proxy
vsftpd	☑ Actif	Serveur FTP — stockage dossiers patients
named (BIND)	☑ Actif	Serveur DNS autoritaire — zone leidoscope.com
php8.2-fpm	☑ Actif	Moteur PHP pour Nginx
keepalived	☑ Actif	Gestion VIP / failover VRRP
snmpd	☑ Actif	Supervision SNMP (LibreNMS)
ssh	☑ Actif	Accès administration sécurisé

2. ARCHITECTURE RÉSEAU

2.1 Plan d'adressage IP

Hôte	Rôle Keepalived	Adresse IP	Interface
VM1 — web (Original)	MASTER	**10.51.10.11**	eth0
VM2 — web2 (Clone)	BACKUP	**10.51.10.12**	eth0

VIP (flottante)	VRRP Virtual IP	**10.51.10.67**	eth0 (logique)
Passerelle Rnet1	—	**192.168.4.51**	—
Passerelle Rnet92i	—	**172.18.55.51**	—
Réseau	—	**10.51.0.0/16**	—

2.2 Logique de failover VRRP

Évènement	Comportement	VIP détenue par
Démarrage normal	MASTER prend la VIP, BACKUP en veille	VM1 — 10.51.10.11
MASTER down / service mort	BACKUP → état MASTER, récupère la VIP automatiquement	VM2 — 10.51.10.12
MASTER revient	Preemption : VIP rebascule sur VM1 (priorité 100 > 90)	VM1 — 10.51.10.11
Service nginx/vsftpd/named mort	Priorité réduite par weight=2, failover si seuil atteint	VM2 (si seuil atteint)

3. CLONAGE DE LA VM (HYPER-V)

> ⚠ Après un clonage, deux problèmes critiques doivent être résolus : conflit de machine-id et adresse IP identique entre source et clone.

3.1 Étapes dans Hyper-V

- Exporter la VM source depuis le Gestionnaire Hyper-V
- Importer la VM exportée (option « Copier » pour créer un nouvel ID)
- Attribuer une nouvelle adresse MAC à la carte réseau du clone
- Démarrer le clone et se connecter en console

3.2 Correction du machine-id

Chaque VM Debian doit avoir un identifiant système unique :

```
sudo rm /etc/machine-id
sudo systemd-machine-id-setup
```

3.3 Changement d'adresse IP (VM clone — BACKUP)

L'interface réseau est configurée via /etc/network/interfaces.

Modifier la configuration réseau

```
sudo nano /etc/network/interfaces
```

Contenu à appliquer sur la VM BACKUP (clone) :

```
auto eth0
iface eth0 inet static
    address 10.51.10.12
    netmask 255.255.0.0
    gateway 10.51.10.254
    dns-nameservers 8.8.8.8 8.8.4.4
```

Appliquer et vérifier

```
sudo systemctl restart networking
```

```
ping 10.51.10.11    # vérifier la connectivité avec le MASTER
```

4. CONFIGURATION KEEPALIVED

4.1 Installation

À exécuter sur les deux VMs :

```
sudo apt update && sudo apt install keepalived -y
```

4.2 Configuration VM MASTER (10.51.10.11)

Fichier : /etc/keepalived/keepalived.conf

```
vrrp_script chk_nginx {
    script "pidof nginx"
    interval 2
    weight 11
}

vrrp_script chk_vsftpd {
    script "pidof vsftpd"
    interval 2
    weight 11
}

vrrp_script chk_bind {
    script "pidof named"
    interval 2
    weight 11
}

vrrp_instance VI_1 {
    state MASTER
    interface eth0
    virtual_router_id 51
    priority 100
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1234
    }
    virtual_ipaddress {
        10.51.10.67
    }
    track_script {
        chk_nginx
        chk_vsftpd
        chk_bind
    }
}
```

> 💡 Les vrrp_script surveillent nginx, vsftpd et named via pidof. Si un service meurt, la priorité baisse de weight=2. Le failover se déclenche si la priorité tombe sous celle du BACKUP (90).

4.3 Configuration VM BACKUP (10.51.10.12)

Seuls state et priority changent. Les track_scripts sont volontairement vides sur le BACKUP.

```
vrrp_instance VI_1 {
    state BACKUP
    interface eth0
    virtual_router_id 51
    priority 90
    advert_int 1
    authentication {
        auth_type PASS
        auth_pass 1234
    }
    virtual_ipaddress {
        10.51.10.67
    }
    track_script {
    }
}
```

4.4 Démarrage et activation

Sur les deux VMs :

```
sudo systemctl enable keepalived
sudo systemctl start keepalived
sudo systemctl status keepalived
```

5. RECONFIGURATION NAT APRÈS MIGRATION VIP

Suite à la mise en place de la VIP 10.51.10.67, les règles NAT statiques des routeurs Rnet1 et Rnet92i ont été mises à jour pour pointer vers la VIP plutôt que vers l'IP fixe de la VM originale (10.51.10.11).

5.1 Rnet92i — Suppression des anciennes règles

Suppression des règles NAT pointant vers 10.51.10.11 :

```
Rnet92i#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Rnet92i(config)#no ip nat inside source static tcp 10.51.10.11 80 172.18.55.51 51 extendable
Rnet92i(config)#no ip nat inside source static tcp 10.51.10.11 80 172.18.55.51 80 extendable
Rnet92i(config)#no ip nat inside source static tcp 10.51.10.11 21 172.18.55.51 21 extendable
Rnet92i(config)#no ip nat inside source static tcp 10.51.10.11 443 172.18.55.51 443 extendable
Rnet92i(config)#no ip nat inside source static 10.51.10.11 172.18.55.51
Rnet92i(config)#
```

Rnet92i — Suppression des règles NAT statiques vers 10.51.10.11 (ports 80, 443, 21, 51)

5.2 Rnet1 — Mise à jour vers la VIP

Suppression des anciennes règles et création des nouvelles vers 10.51.10.67 :

```
Rnet1(config)#no ip nat inside source static tcp 10.51.10.11 80 192.168.4.51 80 extendable
Rnet1(config)# no ip nat inside source static tcp 10.51.10.11 443 192.168.4.51 443 extendable
Rnet1(config)#ip nat inside source static tcp 10.51.10.67 443 192.168.4.51 443 extendable
Rnet1(config)#ip nat inside source static tcp 10.51.10.67 80 192.168.4.51 80 extendable
Rnet1(config)#
```

Rnet1 — Nouvelles règles NAT statiques vers la VIP 10.51.10.67 (ports 80 et 443)

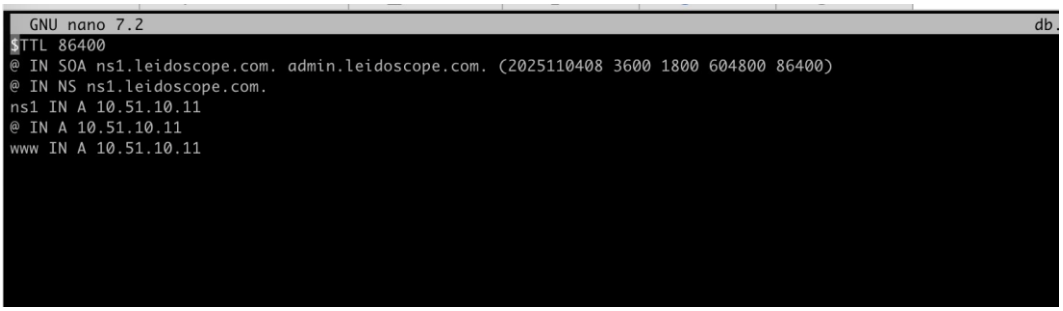
> ⚠ Toutes les règles NAT doivent pointer vers la VIP 10.51.10.67 et non vers l'IP statique d'un nœud. Ainsi, le NAT reste fonctionnel quel que soit le nœud actif.

6. MISE À JOUR DE LA ZONE DNS BIND

Le serveur BIND (named) est déployé sur la VM MASTER et supervisé par Keepalived. La zone leidoscope.com doit pointer vers la VIP 10.51.10.67 pour garantir la résolution DNS même lors d'un basculement.

6.1 Ancienne configuration (avant HA)

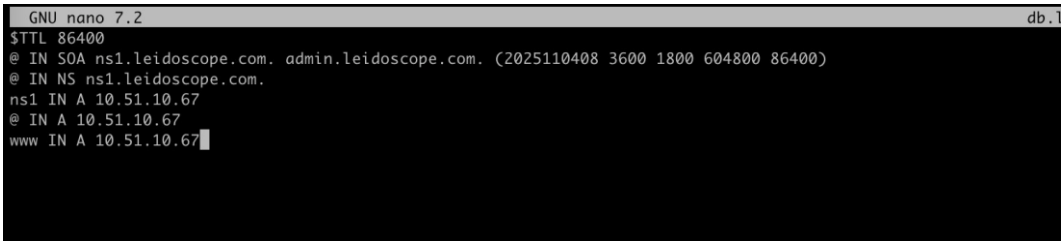
Tous les enregistrements A pointaient vers 10.51.10.11 (IP fixe VM1) :



Ancienne zone DNS — enregistrements A sur 10.51.10.11 (avant VIP)

6.2 Nouvelle configuration (après HA)

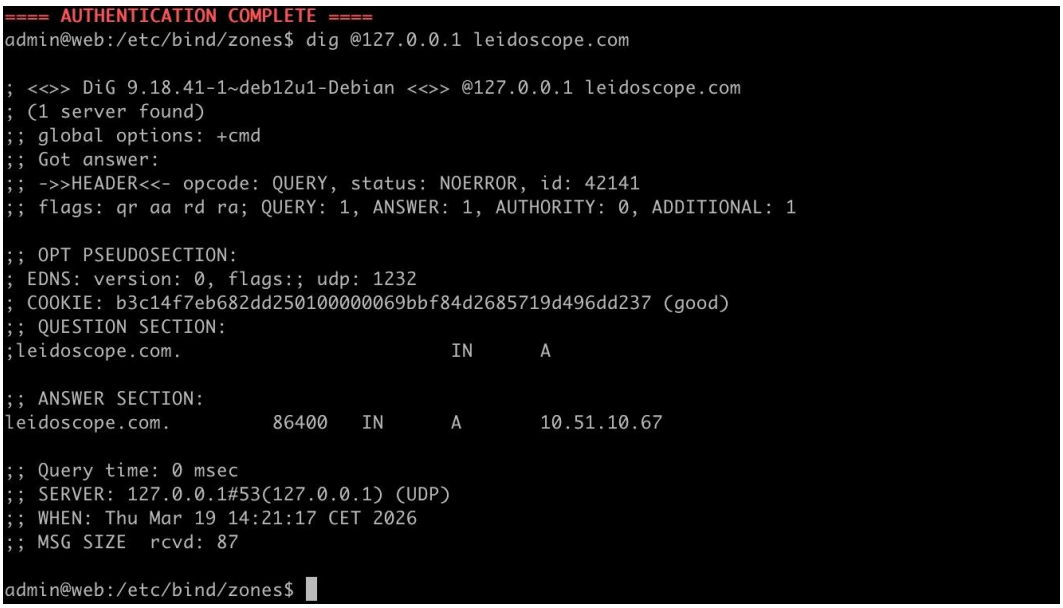
Les enregistrements ns1, @, www pointent désormais tous vers la VIP 10.51.10.67 :



Nouvelle zone DNS — enregistrements A mis à jour vers la VIP 10.51.10.67

6.3 Vérification de la résolution

Test de la résolution DNS depuis le serveur web :



dig @127.0.0.1 leidoscope.com — Résolution correcte vers 10.51.10.67 (NOERROR)

> ☑ La commande dig confirme que leidoscope.com résout bien vers 10.51.10.67 (enregistrement A, TTL 86400, status NOERROR). Le DNS suit désormais la VIP et reste cohérent lors d'un failover.

```
nano /etc/bind/zones/db.leidoscope.com    # éditer la zone
named-checkzone leidoscope.com /etc/bind/zones/db.leidoscope.com
sudo systemctl reload named               # recharger sans coupure
dig @127.0.0.1 leidoscope.com             # vérification locale
```

7. PROBLÈMES FRÉQUENTS ET SOLUTIONS

Problème	Cause probable	Solution
Conflit IP après clonage	IP identique entre VM source et clone	Modifier /etc/network/interfaces avec une IP unique sur le clone
machine-id dupliqué	Clone hérite du machine-id source	sudo rm /etc/machine-id && sudo systemd-machine-id-setup
VIP n'apparaît pas	Keepalived non démarré ou erreur de config	Vérifier systemctl status keepalived et journalctl -u keepalived
Pas de failover automatique	virtual_router_id ou auth_pass différents entre MASTER/BACKUP	Synchroniser les deux keepalived.conf (même virtual_router_id et auth_pass)
VIP sur les deux VMs (split-brain)	Firewall bloquant les paquets VRRP multicast	Autoriser le protocole VRRP (multicast 224.0.0.18) sur le réseau
DNS non résolu après changement VIP	Zone BIND encore sur l'ancienne IP	Mettre à jour tous les enregistrements A vers 10.51.10.67 et recharger named
NAT ne redirige plus après failover	Règles NAT pointent vers IP fixe et non VIP	Reconfigurer les règles NAT statiques pour pointer vers 10.51.10.67

8. COMMANDES DE RÉFÉRENCE

Réseau

```
ip a                                    # Toutes les IPs et interfaces
ip a show eth0                          # Interface eth0 uniquement
sudo ifdown eth0 && sudo ifup eth0      # Redémarrer l'interface
sudo systemctl restart networking       # Alternative réseau
```

Keepalived

```
sudo systemctl start keepalived         # Démarrer
sudo systemctl stop keepalived          # Arrêter (déclenche failover)
sudo systemctl restart keepalived       # Redémarrer
sudo systemctl enable keepalived        # Activer au démarrage
sudo systemctl status keepalived        # État
sudo journalctl -u keepalived -f        # Logs en temps réel
```

Services supervisés

```
sudo systemctl status nginx             # État Nginx
sudo systemctl status vsftpd            # État vsftpd
sudo systemctl status named             # État BIND
pidof nginx                             # Vérification track_script
```

DNS BIND

```
named-checkconf                         # Vérifier la config BIND
named-checkzone leidoscope.com /etc/bind/zones/db.leidoscope.com
sudo systemctl reload named             # Recharger la zone sans coupure
dig @127.0.0.1 leidoscope.com           # Test résolution locale
```

Diagnostic

```
ip route show                           # Table de routage
cat /etc/network/interfaces             # Config réseau
cat /etc/keepalived/keepalived.conf     # Config Keepalived
```

ANNEXE — RÉCAPITULATIF DES FICHIERS MODIFIÉS

Fichier	VM(s)	Modification
/etc/network/interfaces	BACKUP	Nouvelle IP statique 10.51.10.12
/etc/machine-id	BACKUP	Régénéré après clonage
/etc/keepalived/keepalived.conf	MASTER	state MASTER, priority 100, track_scripts nginx/vsftpd/bind
/etc/keepalived/keepalived.conf	BACKUP	state BACKUP, priority 90, track_scripts vides
/etc/bind/zones/db.leidoscope.com	MASTER	Enregistrements A mis à jour → VIP 10.51.10.67
NAT Rnet1	Routeur	Règles NAT ports 80/443 → 10.51.10.67
NAT Rnet92i	Routeur	Suppression règles NAT vers 10.51.10.11