PROCEDURE DE DEPLOIEMENT RSYNC

Index

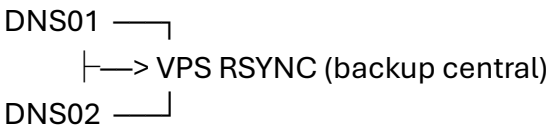
Environnement :

- Srv-btsdns01 → 51.255.202.249
- Srv-btsdns02 → 51.255.196.208
- Srv-btsrsync → 51.255.200.17

Objectif :

- Sauvegarde automatique Unbound depuis DNS01/DNS02 vers VPS RSYNC
- Restauration contrôlée depuis VPS RSYNC vers DNS01/DNS02
- SSH sans mot de passe (clé dédiée)
- Compatibilité UFW + fail2ban

ARCHITECTURE LOGIQUE



VPS RSYNC ——> DNS01 / DNS02 (restore)

PRÉREQUIS COMMUNS (TOUS VPS)

Installer rsync + ssh

Sur les 3 serveurs :

```
sudo apt update
sudo apt install -y rsync openssh-client openssh-server
```

Vérifier SSH actif

```
sudo systemctl status ssh
```

UFW (minimum recommandé)

DNS01 / DNS02

sudo ufw allow 22/tcp
sudo ufw enable

VPS RSYNC

sudo ufw allow 22/tcp
sudo ufw allow from 51.255.202.249 to any port 22
sudo ufw allow from 51.255.196.208 to any port 22
sudo ufw enable

CLÉS SSH (SANS MOT DE PASSE)

Principe

- clé backup : DNS → RSYNC
- clé restore : RSYNC → DNS

CLÉ BACKUP (DNS → RSYNC)

Sur DNS01

ssh-keygen -t ed25519 -f ~/.ssh/dns01-backup

ssh-copy-id -i ~/.ssh/dns01-backup.pub backup@51.255.200.17

Sur DNS02

ssh-keygen -t ed25519 -f ~/.ssh/dns02-backup

ssh-copy-id -i ~/.ssh/dns02-backup.pub backup@51.255.200.17

Sur VPS RSYNC

Créer user backup :

sudo adduser backup

CLÉ RESTORE (RSYNC → DNS)

Sur VPS RSYNC

sudo ssh-keygen -t ed25519 -f /root/.ssh/restore-dns

Déployer vers DNS01

sudo ssh-copy-id -i /root/.ssh/restore-dns.pub secadmin@51.255.202.249

Déployer vers DNS02

sudo ssh-copy-id -i /root/.ssh/restore-dns.pub secadmin@51.255.196.208

Test

sudo ssh -i /root/.ssh/restore-dns secadmin@51.255.202.249

VPS RSYNC – STRUCTURE BACKUP

Créer arborescence :

sudo mkdir -p /backup/dns01/current
sudo mkdir -p /backup/dns02/current
sudo chown -R backup:backup /backup

SCRIPTS BACKUP (DNS01 / DNS02)

DNS01 – backup

sudo nano /root/backup_unbound.sh

Script :

#!/bin/bash

BACKUP_DATE=$(date +%F)

rsync -az --delete \

-e "ssh -i /home/secadmin/.ssh/dns01-backup" \
/etc/unbound/unbound.conf.d/ \
backup@51.255.200.17:/backup/dns01/current/

Explication

- BACKUP_DATE : date (option future extension)
- rsync : synchronisation
- -a : conserve permissions
- -z : compression
- --delete : miroir exact
- ssh -i : clé SSH dédiée DNS01
- source : config Unbound
- destination : VPS central

rendre exécutable

sudo chmod +x /root/backup_unbound.sh

test

sudo /root/backup_unbound.sh

DNS02 – backup

#!/bin/bash

rsync -az --delete \
-e "ssh -i /home/secadmin/.ssh/dns02-backup" \
/etc/unbound/unbound.conf.d/ \
backup@51.255.200.17:/backup/dns02/current/

AUTOMATISATION (CRON)

Sur DNS01 et DNS02 :

sudo crontab -e

Ajout :

0 21 * * * /root/backup_unbound.sh

backup automatique à 21h

VPS RSYNC – SCRIPTS RESTAURATION

RESTORE DNS01

sudo nano /backup/restore_dns01.sh

#!/bin/bash

rsync -rvz --delete \
--exclude="*.bak" \
-e "ssh -i /root/.ssh/restore-dns" \
/backup/dns01/current/ \
secadmin@51.255.202.249:/etc/unbound/unbound.conf.d/

RESTORE DNS02

#!/bin/bash

rsync -rvz --delete \
--exclude="*.bak" \
-e "ssh -i /root/.ssh/restore-dns" \
/backup/dns02/current/ \
secadmin@51.255.196.208:/etc/unbound/unbound.conf.d/

rendre exécutables

sudo chmod +x /backup/restore_dns01.sh
sudo chmod +x /backup/restore_dns02.sh

EXPLICATION RESTORE

- --delete → miroir exact
- --exclude *.bak → ignore fichiers de backup locaux
- ssh -i restore-dns → clé sans mot de passe
- destination → dossier Unbound actif

MÉTHODOLOGIE DE TEST (IMPORTANT AUDIT)

TEST 1 – SSH sans mot de passe

sudo ssh -i /root/.ssh/restore-dns secadmin@51.255.202.249

Doit se connecter directement.

TEST 2 – backup manuel

Sur DNS01 :

sudo /root/backup_unbound.sh

Vérifier sur RSYNC :

ls -l /backup/dns01/current/

TEST 3 – restore manuel

Sur RSYNC :

sudo /backup/restore_dns01.sh

TEST 4 – vérification DNS01

ls -l /etc/unbound/unbound.conf.d/

TEST 5 – cron

sudo grep CRON /var/log/syslog

Résumé logique

- Séparation backup / restore
- Clé SSH dédiée par flux
- Pas de root SSH distant
- Cron côté source uniquement
- Rsync centralisé
- Exclusion .bak
- Logs possibles extension