Serveur DNS/DHCP de secours BIND9 + ISC-DHCP

Période : 11/2025 – 01/2026	**Entreprise :** SNCF — DSI	**Candidat :** Soul Florian

Objectif de la mission

Déployer un serveur DNS secondaire BIND9 et un DHCP failover ISC-DHCP sous Debian 12 pour assurer la continuité de service réseau en cas de panne du contrôleur de domaine primaire.

Compétences BTS SIO mobilisées

Gérer le patrimoine informatique	Répondre aux incidents et demandes
Travailler en mode projet	Vérifier la continuité d'un service informatique

1. Présentation de la mission

Déploiement d'un serveur DNS secondaire BIND9 et d'un service DHCP de failover ISC-DHCP sous Linux Debian 12 pour assurer la continuité de service en cas de panne du contrôleur de domaine primaire Windows Server. La supervision des services est assurée par des scripts cron.

2. Architecture de redondance

Service	Serveur primaire	Serveur secondaire
DNS	SRV-AD-01 (192.168.10.1) — Windows DNS	SRV-DNS-SEC (192.168.10.2) — BIND9 Debian
DHCP	SRV-AD-01 (192.168.10.1) — DHCP Windows	SRV-DHCP-SEC (192.168.10.2) — ISC-DHCP
Active Directory	SRV-AD-01 — DC primaire	SRV-AD-02 (optionnel) — DC secondaire

3. Configuration DNS secondaire BIND9

3.1 — Installation

```
apt install -y bind9 bind9-utils bind9-doc systemctl enable bind9
```

3.2 — Configuration /etc/bind/named.conf.local

```
// Zone secondaire pour sncf-dsi.local zone "sncf-dsi.local" { type slave; masters {
192.168.10.1; }; // IP du DC Windows (DNS primaire) file
"/var/cache/bind/sncf-dsi.local.db"; notify no; }; // Zone inverse secondaire zone
```

```
"10.168.192.in-addr.arpa" { type slave; masters { 192.168.10.1; }; file
"/var/cache/bind/rev.10.168.192.db"; };
```

3.3 — Autoriser les transferts de zone depuis Windows DNS

- Sur Windows Server (DNS Manager) : clic droit sur la zone sncf-dsi.local > Propriétés > Transferts de zone
- Cocher « Autoriser les transferts de zone »
- Sélectionner « Uniquement aux serveurs listés » : 192.168.10.2
- Vérifier le transfert : named-checkconf && systemctl restart bind9
- Tester : dig @192.168.10.2 sncf-dsi.local SOA

4. Configuration DHCP de failover ISC-DHCP

```
# /etc/dhcp/dhcpd.conf (serveur secondaire) failover peer "dhcp-failover" { secondary;
address 192.168.10.2; port 647; peer address 192.168.10.1; peer port 647;
max-response-delay 30; max-unacked-updates 10; load balance max seconds 3; } subnet
192.168.20.0 netmask 255.255.255.0 { option routers 192.168.20.1; option
domain-name-servers 192.168.10.1, 192.168.10.2; option domain-name "sncf-dsi.local";
pool { failover peer "dhcp-failover"; range 192.168.20.50 192.168.20.200; } }
```

5. Supervision par cron

```
# Script /usr/local/bin/check_dns_dhcp.sh #!/bin/bash # Compare les numéros de série SOA
primaire / secondaire PRI_SOA=$(dig @192.168.10.1 sncf-dsi.local SOA +short | awk
'{print $3}') SEC_SOA=$(dig @192.168.10.2 sncf-dsi.local SOA +short | awk '{print $3}')
if [ "$PRI_SOA" != "$SEC_SOA" ]; then echo "ALERTE : SOA desynchronise!
Primaire=$PRI_SOA Secondaire=$SEC_SOA" | \ mail -s '[ALERTE] DNS Secondaire desync'
admin@sncf-dsi.local fi # Ajouter dans crontab */30 * * * *
/usr/local/bin/check_dns_dhcp.sh
```

6. Test de bascule

- Arrêter le service DNS sur SRV-AD-01 : net stop 'DNS Server'
- Configurer un poste test avec DNS secondaire uniquement (192.168.10.2)
- Tester la résolution : nslookup srv-ad-01.sncf-dsi.local 192.168.10.2
- Tester l'obtention d'une adresse DHCP depuis le serveur secondaire
- Redémarrer le DNS primaire et vérifier la resynchronisation

7. Livrables attendus

- Capture de dig @192.168.10.2 sncf-dsi.local SOA confirmant le transfert de zone
- Capture du test de résolution DNS depuis un poste en situation de bascule
- Capture du statut DHCP failover (dhcpd.leases avec mention failover)
- Log de supervision cron avec comparaison SOA