

PROJET NAVAJO

Documentation de mise en place

Services DHCP & DNS

Serveur	REZOLAB (Debian 12)
Réseau	Srv – 172.16.0.0/17
Domaine local	galaxy-swiss8.lan
DHCP pour	Réseau Dev – 192.168.150+8.0/24
Projet	AP3.1 – BTS SIO SISR

1. Présentation de l'infrastructure

Dans le cadre du projet Navajo (AP3.1), le serveur REZOLAB héberge deux services réseau fondamentaux pour l'intranet du laboratoire GSB :

- Le service DHCP (Dynamic Host Configuration Protocol), déporté, chargé d'attribuer dynamiquement les configurations IP aux postes du réseau Dev.
- Le service DNS (Domain Name System), pour la résolution de noms du domaine local galaxy-swiss8.lan, avec relais vers le DNS du FAI pour les zones externes.

Contexte réseau

REZOLAB : Debian 12 – Réseau Srv (172.16.0.0/17)

MUTLAB : Commutateur L3 HP 2615 – routage inter-VLAN

Dev8 : VLAN 158 – 192.168.158.0/24

FAI/DNS : 192.168.51.254 (réseau SIO émulé)

2. Prérequis et installation

2.1 Mise à jour du système

Avant toute installation, mettre à jour les paquets de la machine REZOLAB :

```
apt update && apt upgrade -y
```

2.2 Installation des paquets

Installer les services DHCP et DNS sur REZOLAB :

```
# Service DHCP
apt install isc-dhcp-server -y

# Service DNS
apt install bind9 bind9utils bind9-doc -y
```

2.3 Vérification des interfaces réseau

Identifier l'interface réseau connectée au réseau Srv (exemple : ens18) :

```
ip a
# Repérer l'interface avec l'adresse dans 172.16.0.0/17
```

3. Configuration du service DHCP

3.1 Principe de fonctionnement

Le DHCP est déporté : REZOLAB est serveur DHCP pour le réseau Dev (192.168.158.0/24), mais ces réseaux sont dans un VLAN différent. MUTLAB joue le rôle de relais DHCP (ip helper-address) pour acheminer les requêtes broadcast DHCP vers REZOLAB.

3.2 Configuration de l'interface d'écoute

Indiquer à isc-dhcp-server l'interface sur laquelle écouter (modifier selon votre interface) :

```
# Fichier : /etc/default/isc-dhcp-server
INTERFACESv4="ens18"
INTERFACESv6=""
```

3.3 Fichier de configuration principal (dhcpd.conf)

Éditer le fichier /etc/dhcp/dhcpd.conf avec la configuration suivante :

```
# /etc/dhcp/dhcpd.conf

# Paramètres globaux
default-lease-time 600;
max-lease-time 7200;
authoritative;
```

```
# Options globales
option domain-name "galaxy-swiss8.lan";
option domain-name-servers 172.16.8.1;    # IP de REZOLAB (DNS)

# Étendue pour le réseau Dev8
subnet 192.168.158.0 netmask 255.255.255.0 {
    range 192.168.158.10 192.168.158.200;
    option routers 192.168.158.254;        # Passerelle (MUTLAB)
    option domain-name "galaxy-swiss8.lan";
    option domain-name-servers 172.16.8.1; # REZOLAB DNS
    option ntp-servers 192.168.51.254;     # NTP via PROXYLAB
}

# Réserve IP fixe : imprimante HP LaserJet (.2)
host imprimante-hp {
    hardware ethernet AA:BB:CC:DD:EE:FF;  # MAC de l'imprimante
    fixed-address 192.168.158.2;
}
```

Points importants DHCP

- L'option 'option routers' pointe vers l'interface VLAN Dev de MUTLAB.
- L'option 'domain-name-servers' pointe vers REZOLAB (adresse réseau Srv).
- L'imprimante HP LaserJet reçoit toujours la même IP grâce à la réservation MAC.
- La plage dynamique commence en .10 pour réserver les 10 premières adresses.

3.4 Configuration du relais DHCP sur MUTLAB

Sur le commutateur de niveau 3 MUTLAB (HP 2615), configurer le relais DHCP pour le VLAN Dev :

```
# Sur MUTLAB (HP 2615) - interface VLAN Dev
vlan 158
    ip helper-address 172.16.8.1    # IP REZOLAB dans réseau Srv
exit
```

3.5 Démarrage et activation du service

```
systemctl enable isc-dhcp-server
systemctl start isc-dhcp-server
systemctl status isc-dhcp-server
```

3.6 Vérification et journaux DHCP

Pour vérifier les baux accordés et consulter les journaux :

```
# Voir les baux actifs
cat /var/lib/dhcp/dhcpd.leases
```

```
# Journaux temps réel
journalctl -u isc-dhcp-server -f

# Ou via syslog
tail -f /var/log/syslog | grep dhcpd
```

4. Configuration du service DNS (BIND9)

4.1 Architecture DNS

Le serveur BIND9 sur REZOLAB assure les rôles suivants :

- Serveur Maître (Primary) pour la zone directe : galaxy-swiss8.lan
- Serveur Maître pour la zone inversée du réseau Srv (172.16.0.0/17)
- DNS dynamique (dyndns) pour les STA du réseau Dev
- Relais DNS (Forwarder) vers le DNS du FAI (192.168.51.254) pour les zones externes

4.2 Configuration de named.conf.options

Ce fichier définit les options globales de BIND9, notamment les forwarders vers le DNS du FAI :

```
# /etc/bind/named.conf.options

options {
    directory "/var/cache/bind";

    // Forwarder vers le DNS du FAI
    forwarders {
        192.168.51.254;
    };
    forward only;

    // Écoute sur toutes les interfaces
    listen-on { any; };
    listen-on-v6 { none; };

    // Autoriser les requêtes du réseau local
    allow-query {
        localhost;
        172.16.0.0/17;      // Réseau Srv
        192.168.158.0/24;  // Réseau Dev
        172.18.8.0/27;     // Réseau DMZ
    };

    // DNSSEC
    dnssec-validation auto;
};
```

4.3 Configuration de named.conf.local

Ce fichier déclare les zones locales gérées par BIND9 en tant que serveur maître :

```
# /etc/bind/named.conf.local

// Zone directe - domaine galaxy-swiss8.lan
zone "galaxy-swiss8.lan" {
    type master;
    file "/etc/bind/db.galaxy-swiss8.lan";
    allow-update { key rndc-key; }; // pour dyndns
};

// Zone inversée - réseau Srv 172.16.0.0/17
// (sous-réseau .0.0/17 = 172.16.0-127.x)
zone "16.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.16.in-addr.arpa";
};
```

4.4 Fichier de zone directe (db.galaxy-swiss8.lan)

Ce fichier contient les enregistrements DNS pour le domaine local :

```
# /etc/bind/db.galaxy-swiss8.lan

$TTL      604800
@ IN SOA rezolab.galaxy-swiss8.lan. admin.galaxy-swiss8.lan. (
    2024010101 ; Serial (AAAAMMJJXX)
    604800     ; Refresh
    86400      ; Retry
    2419200    ; Expire
    604800 )   ; Negative Cache TTL

; Serveurs de noms
@ IN NS rezolab.galaxy-swiss8.lan.

; Enregistrements A - hôtes du réseau Srv
mutlab IN A 172.16.8.254 ; Commutateur L3
rezolab IN A 172.16.8.1 ; Serveur REZOLAB
extralab IN A 172.18.8.2 ; Serveur EXTRALAB (DMZ)
certilab IN A 172.16.8.40 ; Serveur PKI
proxylab IN A 172.16.8.30 ; Passerelle pfSense

; Alias CNAME
www IN CNAME extralab ; Alias web pour EXTRALAB
```

4.5 Fichier de zone inversée (db.172.16.in-addr.arpa)

Ce fichier permet la résolution inverse (IP vers nom) pour le réseau Srv :

```
# /etc/bind/db.172.16.in-addr.arpa
```

```
$TTL      604800
@ IN SOA rezolab.galaxy-swiss8.lan. admin.galaxy-swiss8.lan. (
                        2024010101 ; Serial
                        604800      ; Refresh
                        86400        ; Retry
                        2419200      ; Expire
                        604800 )     ; Negative Cache TTL

; Serveur de noms
@ IN NS  rezolab.galaxy-swiss8.lan.

; Enregistrements PTR (résolution inverse - réseau Srv)
; Format : dernier(s) octet(s) de l'IP PTR nom-complet.
8.1  IN  PTR  rezolab.galaxy-swiss8.lan.
8.2  IN  PTR  extralab.galaxy-swiss8.lan.
8.30 IN  PTR  proxylab.galaxy-swiss8.lan.
8.40 IN  PTR  certilab.galaxy-swiss8.lan.
8.254 IN PTR  mutlab.galaxy-swiss8.lan.
```

4.6 DNS dynamique (DynDNS) pour le réseau Dev

Les stations du réseau Dev doivent pouvoir être jointes par leur nom. Pour cela, le DHCP met à jour automatiquement le DNS. Configurer BIND9 et isc-dhcp-server pour fonctionner ensemble :

```
# Générer une clé TSIG pour la mise à jour sécurisée
tsig-keygen -a hmac-sha256 rndc-key > /etc/bind/rndc.key
chown bind:bind /etc/bind/rndc.key
chmod 640 /etc/bind/rndc.key
```

Ajouter dans dhcpd.conf la configuration DynDNS :

```
# Ajout dans /etc/dhcp/dhcpd.conf

ddns-update-style standard;
ddns-domainname "galaxy-swiss8.lan.";
ddns-rev-domainname "in-addr.arpa.";
update-static-leases on;

key "rndc-key" {
    algorithm hmac-sha256;
    secret "VOTRE_SECRET_ICI"; // contenu de /etc/bind/rndc.key
};

zone galaxy-swiss8.lan. {
    primary 127.0.0.1;
    key "rndc-key";
};
```

4.7 Démarrage et activation du service DNS

```
# Vérifier la syntaxe des fichiers de configuration
named-checkconf
named-checkzone galaxy-swiss8.lan /etc/bind/db.galaxy-swiss8.lan
named-checkzone 16.172.in-addr.arpa /etc/bind/db.172.16.in-addr.arpa

# Activer et démarrer BIND9
systemctl enable bind9
systemctl start bind9
systemctl status bind9
```

5. Tests de validation

5.1 Tests du service DHCP

Test	Commande / Action	Résultat attendu
Attribution IP dynamique	Connecter une STA Dev et vérifier sa config IP	IP dans 192.168.158.10–200, GW .254, DNS REZOLAB
Options DHCP	ipconfig /all (W10) ou ip a + cat /etc/resolv.conf (Kali)	Domaine, DNS et passerelle corrects
Réservation imprimante	Vérifier l'IP de l'imprimante HP LaserJet	Toujours 192.168.158.2
Journaux baux	cat /var/lib/dhcp/dhcpd.leases	Liste des baux actifs visible
Relais DHCP MUTLAB	Requête depuis VLAN Dev vers REZOLAB	IP attribuée depuis REZOLAB via relais

5.2 Tests du service DNS

Test	Commande	Résultat attendu
Résolution directe REZOLAB	nslookup rezolab.galaxy-swiss8.lan	172.16.8.1
Résolution directe EXTRALAB	nslookup extralab.galaxy-swiss8.lan	172.18.8.2
Alias www	nslookup www.galaxy-swiss8.lan	CNAME → extralab → 172.18.8.2
Résolution inversée	nslookup 172.16.8.1	rezolab.galaxy-swiss8.lan
Forwarder (DNS externe)	nslookup google.com	Résolu via 192.168.51.254

Test	Commande	Résultat attendu
DynDNS STA Dev	nslookup devsta01.galaxy-swiss8.lan	IP attribuée dynamiquement

5.3 Commandes de diagnostic utiles

```
# Tester la résolution DNS depuis une STA
nslookup extralab.galaxy-swiss8.lan 172.16.8.1
dig @172.16.8.1 www.galaxy-swiss8.lan

# Vérifier les journaux DNS
journalctl -u bind9 -f
tail -f /var/log/named/bind9.log

# Recharger la config BIND9 sans redémarrage
rndc reload
rndc status
```