Bind 9 DNS

Durée	2 périodes
Format	Individuel
Matériel	PC individuel

Contexte :
Le **DNS (Domain Name System)** est un service essentiel du réseau qui permet de traduire les noms de domaine (comme *www.example.com*) en adresses IP compréhensibles par les machines. Sans lui, les utilisateurs devraient mémoriser et saisir des adresses IP numériques pour accéder aux services en ligne. Le DNS joue donc un rôle d'« annuaire d'Internet », facilitant la navigation et la communication entre machines. Pour mettre en place ce service sur un réseau, on utilise fréquemment **BIND 9 (Berkeley Internet Name Domain)**, l'un des serveurs DNS les plus répandus et puissants dans le monde. BIND 9, disponible sur la plupart des systèmes Linux, permet de gérer différentes zones DNS, de configurer des serveurs faisant autorité, des serveurs récursifs ou encore des serveurs cache. Grâce à sa flexibilité et à sa robustesse, il est utilisé aussi bien dans de petites infrastructures que dans de grands environnements d'entreprise ou d'hébergement.

Pré-requis
- VM Ubuntu Server et Desktop 24.04
- Accès administrateur (sudo).
- Connexion réseau fonctionnelle.
- Connaissances de base en administration Linux et réseau.

Exercice 1 – Installation

Avant toute chose, faite un Snapshot appelé DHCPOK de votre VM server, afin de retomber dans un état fonctionnel en cas de problème avec Bind.

Sur la VM srv-keabind-01, où vous avez installé Kea, installez maintenant le serveur DNS Bind9 :

bind9
bind9-utils
bind9-doc

Exercice 2 – Configuration de base

Configurez le service Bind9 pour travailler uniquement en IPv4.

Editez le fichier **/etc/default/named** de cette façon :

```
OPTIONS="-u bind -4"
```

La configuration de Bind9 se fait via des fichiers de configuration, commencez par le fichier principal **/etc/bind/named.conf.local**.

Ajoutez ces zones à la fin du fichier :

```
zone "emf300.local" {
    type primary;
    file "/etc/bind/db.emf300.local";
};
zone "10.10.10.in-addr.arpa" {
    type primary;
    file "/etc/bind/db.10.10.10";
};
```

A quoi correspondent ces deux zones ?

Configurez ensuite les options dans **/etc/bind/named.conf.options** :

```
acl "trusted" {
        10.10.10.0/24;
        127.0.0.1;
};
options {
        directory "/var/cache/bind";
        recursion no;
        allow-recursion { trusted; };
        listen-on { 10.10.10.5; 127.0.0.1; };
        allow-transfer { none; };
        dnssec-validation auto;
        listen-on-v6 { none; };
};
```

Créez ensuite le fichier **/etc/bind/db.emf300.local** et ajoutez cette configuration :

```
$TTL    1h
@       IN      SOA     srv-keabind-01.emf300.local. admin.emf300.local. (
                        2025090101  ; Serial -> Incrémenter à chaque modif
                        1h          ; Refresh
                        15m         ; Retry
                        1w          ; Expire
                        1h )        ; Negative Cache TTL
;
; name servers - NS records
@    IN      NS      srv-keabind-01.emf300.local.
@    IN      A       10.10.10.5
srv-keabind-01.emf300.local.        IN      A      10.10.10.5
dhcp     IN      CNAME   srv-keabind-01.emf300.local.
```

Créez ensuite le fichier **/etc/bind/db.10.10.10** et ajoutez cette configuration :

```
$TTL 1h
@   IN SOA  srv-keabind-01.emf300.local. admin.emf300.local. (
        2025090101  ; Serial
        1h          ; Refresh
        15m         ; Retry
        1w          ; Expire
        1h )        ; Negative Cache TTL

@   IN NS   srv-keabind-01.emf300.local.

5   IN PTR  srv-keabind-01.emf300.local.
```

Dans le netplan du server :

Définissez 127.0.0.1 comme DNS

Définissez emf300.local comme domaine (search)

Appliquer le netplan.

Redémarrez-le service bind9 et contrôlez le status du service.

Exercice 3 – Test sur le client

Modifiez/ajoutez la configuration nécessaire dans le serveur **DHCP**, notamment le serveur DNS et le domain-name dans les option-data, pour que le client utilise les bonnes informations.

Redémarrer le service DHCP.

Faites un ping sur **srv-keabind-01.emf300.local**. Cela fonctionne-t 'il ?
Pourquoi ? Devez-vous faire une action sur le client ?
Si oui, effectuez cette action pour que la résolution DNS puisse se faire.

Grace à la commande dig, interrogez le serveur DNS pour savoir quelle IP à srv-keabind-01.emf300.local

> Tips :
> dig [@serveur] nom [type]
> - @serveur → optionnel, le serveur DNS à interroger (ex. @8.8.8.8)
> - nom → le nom de domaine à résoudre (ex. example.com)
> - type → le type d'enregistrement DNS (ex. A, AAAA, MX, NS, TXT, etc.)

Quelle est la différence entre l'enregistrement **srv-keabind-01.emf300.local** et **dhcp.emf300.local** ?

Faites un ping sur « **DHCP** », comment est-ce possible que ça fonctionne ?

Exercice 4 – Ajout d'un enregistrement

Modifiez la configuration du serveur DNS pour ajouter un enregistrement afin que l'entrée **dns.emf300.local** pointe sur **srv-keabind-01.emf300.local**
Testez sur le client avec un dig sur dns.emf300.local.

Exercice 5 – Résolveur récursif

Sur le client:
Effectuez un dig www.cff.ch, obtenez-vous une réponse ? Pourquoi ?
Effectuez un dig @8.8.8.8 www.cff.ch, obtenez-vous une réponse ? Pourquoi ?

Votre serveur DNS est actuellement configuré pour résoudre les requêtes du domaine emf300.local, mais il n'est pas configuré pour résoudre des noms de domaines sur Internet.

Un serveur DNS peut avoir deux rôles principaux :

Serveur **faisant autorité (authoritative server)** :

C'est le serveur DNS responsable d'une zone donnée (par exemple emf300.local), il héberge et fournit les enregistrements officiels de cette zone ;

Résolveur :

Il s'occupe de trouver les réponses pour les clients lorsqu'il ne connaît pas la réponse localement (www.cff.ch par exemple) Dans ce second cas, il peut être configuré de deux manières :

En mode récursif, où il interroge directement les serveurs de la hiérarchie DNS (racine, TLD, serveurs autoritaires)
En mode forwarder, où il délègue les requêtes à un autre serveur DNS (par exemple celui du FAI ou de Google).

Un serveur DNS comme **Bind9** peut assurer **les deux rôles en parallèle** :

- **Autoritaire** sur certaines zones internes (emf300.local)
- **Résolveur** pour toutes les autres demandes (sites Internet).

Activez la fonction résolveur récursif sur le serveur :
Dans **/etc/bind/named.conf.options**, passez la valeur recursion à yes

Redémarrez le service bind9.

Sur le client, effectuez un dig www.cff.ch. La réponse arrive-t-elle maintenant ?

Exercice 6 – Résolveur forwarder

Dans la pratique (école, entreprise, petits réseau) pour des raisons de performance et de simplicité, on utilise presque toujours un forwarder.
La récursion directe est généralement activée uniquement par les DNS exploités par les fournisseurs d'accès à Internet, les datacenters ou les infrastructures critiques, afin de garantir indépendance et fiabilité.

Dans le fichier **named.conf.options**, trouvez le moyen de définir un fowarder.
Configurez 8.8.8.8 comme forwarder.
Redémarrez le service bind9.