Activité : Configurer le service DNS(contexte GSB)

Présentation

Les tâches d'administration sur le serveur qui héberge le service DNS vont être les suivantes :

- **Installer** puis **configurer** le service DNS (Bind9) ;
- Vérifier **l'ordre** des méthodes de résolution dans le fichier **/etc/nsswitch.conf** ;
- Vérifier le fichier de **résolution** locale **/etc/hosts** ;
- Indiquer l'IP de votre serveur de noms dans **/etc/resolv.conf**, lorsque vous êtes client DNS ;
- Modifier le fichier de **configuration générale** du serveur DNS **/etc/named.conf.local** ;
- Créer le fichier de **zone maître gsb.local** (l'annuaire contenant les IP et les noms) ;
- Créer le fichier de **zone inverse** (un fichier qui permet de donner le nom à partir d'une IP. On appelle cela la résolution inverse) ;
- Tester.

> Dans le réseau de GSB c'est **REZOLAB** qui a le rôle de serveur DNS. Dans cet atelier ce rôle sera configuré sur l'un de vos serveurs qui héberge le service **DHCP**. Pour cela :
>
> - renommez-le **REZOLABXX**, XX étant le numéro de votre VLAN,
> - **déplacez-le** dans le **VLAN Serveur** et **modifiez** son adresse IP en conséquence (réseau 172.17.0.0/17).

Sur les postes clients, les tâches d'administration sont beaucoup plus simples. Il faut :

- Renseigner l'**adresse IP du serveur DNS** ;
- Renseigner le nom du domaine gsb.local ;
- Tester (bien sûr).

Vérification de l'ordre des méthodes de résolution

Avant que n'existent les serveurs DNS, la résolution de noms était locale à chaque machine. Le fichier **/etc/hosts** sous Linux contenait tous les noms DNS et toutes les adresses IP auxquelles on souhaitait accéder. La méthode du fichier local et celle du serveur DNS peuvent cohabiter notamment pour des raisons d'optimisation car il est plus rapide de regarder dans un fichier local que de contacter un serveur).

Historiquement, le fichier **/etc/host.conf** était utilisé par les outils de résolution de nom pour connaître l'ordre dans le choix de la méthode de résolution. Ce fichier est toujours présent pour des raisons de compatibilité ascendante, mais maintenant, c'est le fichier **/etc/nsswitch.conf**, plus complet, qui est utilisé.

Entre d'autres lignes, vous devriez voir dans ce fichier /etc/nsswitch.conf :

```
root@REZALABXX:~# cat /etc/nsswitch.conf
hosts: files … dns …
```

La résolution la résolution locale (fichier **/etc/hosts**) est favorisée sur la résolution avec DNS comme vous pouvez le voir dans l'ordre indiqué : **files** puis ensuite **dns**. Mais vous allez changer cela dans la suite de l'atelier.

Vérifier le fichier de résolution locale

Dans un réseau avec serveur DNS, le fichier **/etc/hosts** devrait être réduit à sa plus simple ex-pression, puisque c'est votre serveur qui servira à la résolution de noms.

Votre fichier /etc/hosts devrait avoir un contenu similaire à ce qui suit :

```
root@REZOLABXX:~# cat /etc/hosts
127.0.0.1 REZOLAB
127.0.0.1 localhost localhost.localdomain
…
```

Indiquer l'IP du serveur de noms

Le fichier **/etc/resolv.conf** doit contenir l'adresse IP du serveur DNS. Ce fichier est vide par défaut.

Vous devez renseigner ce fichier pour tous les ordinateurs du réseau, STA et serveurs et même le serveur DNS REZOLAB qui est aussi une

machine cliente de son propre service DNS. Cette VM peut avoir besoin de trouver une IP à partir d'un nom.

Vous allez indiquer également le domaine dans lequel vous êtes situés (domain) et comment compléter un nom DNS si on n'indique pas le domaine (search) :

```
root@REZOLABXX:~# nano /etc/resolv.conf
domain gsb.local
search gsb.local
nameserver 172.17.xxx.xxx
```

Vérifiez que la résolution de noms ne fonctionne pas pour l'instant :

```
root@REZOLABXX:~# host rezolab
Host rezolabxx not found: 5(REFUSED)
```

Installer le service DNS (Bind)

```
root@REZOLABXX:~# apt-get install bind9
```

Configurer le service DNS (Bind)

Modifiez le fichier de configuration locale du serveur DNS REZOLAB.

> Attention : Respectez rigoureusement la syntaxe. Bind est très sensible à la moindre erreur !!! Le fichier de configuration de Bind contient de très nombreuses options de configuration qui ne seront pas toutes abordées. Vous allez vous contenter d'un fichier minimaliste

Editez le fichier **/etc/bind/named.conf.local** et ajoutez les informations de zones suivantes :

```
zone "gsb.local" {
    type master;
    file "/etc/bind/db.gsb.local";
};

zone "0.17.172.in-addr.arpa" {
    type master;
    file "/etc/bind/db.172.17.0";
};
```

Voyons la signification de chaque champ :

Option	Commentaires
zone “gsb.local” {	Le nom de la zone entre guillemets et suivi d'une accolade.
type master;	**Master** indique que vous avez l'autorité sur la zone. D'autres ser-veurs (esclaves) pourront se synchroniser avec votre serveur.
file “/etc/bind/db.gsb.local”;	Emplacement et nom du fichier de zone. Il sera placé dans /etc/bind/ et s'appellera db.gsb.local
};	L'accolade ferme la définition de la zone.

La zone suivante porte la mention « **in-addr.arpa** » qui indique la zone inverse. Cette zone in-verse permet au serveur de fournir un nom d'hôte à partir d'une adresse IP.

Cette fonctionnalité est rendue nécessaire par certains services réseau. Le nom de la zone ré-pond à une structure très précise. Le début du nom de la zone est constitué par le préfixe ré-seau de l'adresse IP. Les conventions sont les suivantes : Les tâches d'administration sur le serveur vont être les suivantes :

- Pour les réseaux IP de classe A (a.0.0.0), il faut un fichier de zone inverse a.in-addr.arpa;
- Pour les réseaux IP de classe B (a.b.0.0), il faut un fichier de zone inverse b.a.in-addr.arpa;
- Pour les réseaux IP de classe C (a.b.c.0), il faut un fichier de zone inverse c.b.a.in-addr.arpa

Notez bien au passage l'inversion des octets !

Création du fichier de zone maître

Vous devez maintenant créer les deux fichiers indiqués pour nos zones dans **/etc/bind/named.conf.local**.

Dans votre zone, vous avez plusieurs serveurs avec des adresses IP précises. Par exemple REZOLABXX (172.17.0.xxx), INTRALAB (172.17.0.100) et LABANNU (172.17.0.30).

Voici un contenu minimaliste pour ce fichier /etc/bind/db.gsb.local que vous devez créer :

```
$ORIGIN gsb.local.
$TTL 1D
@       IN      SOA     labannu.gsb.local. root.gsb.Local. (
        2006031201      ; serial
        28800           ; refresh
        14400           ; retry
        3600000         ; expire
        86400 )         ; minimum

       NS      labannu.gsb.local.

rezolabxx     A       172.17.0.xxx
intralab      A       172.17.0.100
labannu       A       172.17.0.30
```

Chaque ligne (qui ne commence pas par un $) s'appelle un enregistrement DNS. La première ligne ($ORIGIN) définit le nom du domaine. Notez bien le point à la fin du nom de domaine.

La deuxième ligne ($TTL 1D) indique la durée de vie des informations transmises par votre ser-veur DNS. En effet, les machines qui feront appel à votre serveur vont conserver dans un cache les informations découvertes afin de ne pas refaire en permanence les mêmes de-mandes. Ici, au bout de trois jours (1D = 1 day), les informations doivent être retirées du cache. Comment déterminer ce TTL ? Cela dépend de votre zone. Si elle change souvent, il faut un TTL court.

La troisième ligne est la plus importante. C'est un enregistrement SOA (Start Of Authority) qui indique que les informations en-dessous sont de votre responsabilité. En effet, vous êtes le serveur maître de la zone gsb.local. Voici sa structure :

@ IN SOA	labannu.gsb.local.	root.gsb.Local.	(2006031201; serial\\28800; refresh\\14400; retry\\3600000; expire\\86400); minimum
Enregistrement DNS de type Internet (IN) déclarant notre autorité (SOA). Le @ fait référence à $ORIGIN.			