Configurer le service DNS pour les ordinateurs du réseau utilisateurs

Présentation

Pour chaque agence, il est nécessaire d'installer et configurer :

- le serveur DNS ayant autorité sur le domaine <agence>.cub.fr (non récursif) dans un conteneur Debian appelé ns0 situé dans la DMZ:
- le serveur DNS ayant autorité sur la zone lan.<agence>.cub.fr (non récursif) dans un conteneur Debian appelé ns0 situé dans la DMZ:
- le résolveur récursif dans un conteneur Debian appelé dns0 situé dans le VLAN Utilisateur.

Vous devez:

- Mettre en place les serveurs DNS de votre agence:
 - o serveur DNS ns0.<agence>.cub.fr dans la DMZ avec l'adresse IP 172.16.x.10
 - o serveur DNS ns0.lan.<agence>.cub.fr dans la DMZ avec l'adresse IP 172.16.x.20
 - o résolveur DNS dns0 dans le réseau Utilisateur (LAN) avec l'adresse IP 192.168.x.10
 - 1. Procéder aux ajouts nécessaires sur le pare-feu pour le cas particulier du réseau Wan-CUB pour permettre notamment l'accessibilité des serveurs DNS et Web.
 - 2. Vérifier le fonctionnement des services DNS et Web.

Liste des tâches que vous devez effectuer

Tâche à faire sur le serveur DNS ns0

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

- Installer puis configurer le service DNS (Bind9) dans un conteneur nommé ns0 ;
- 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 utilisateurs.gsb.fr (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.

Tâche à faire sur les postes client

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 <agence>.cub.fr;
- Tester (bien sûr).

Vérification de l'ordre des méthodes de résolution sur les postes clients

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@equipexdns:~# 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 expression, 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@equipexdns:~# cat /etc/hosts
127.0.0.1 localhost localdomain
adresseip equipexdns
...
```

Indiquer l'IP du serveur de noms

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

Vous devez renseigner ce fichier pour tous les ordinateurs du réseau, PC et serveurs et même votre serveur DNS ns0 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 de l'agence dans lequel vous êtes situés (domain) et comment compléter un nom DNS si on n'indique pas le domaine (search). Indiquez également l'adresse IP de votre résolveur DNS (192.168.x.10) :

```
root@ns0:~# nano /etc/resolv.conf
domain agence.cub.fr
search agence.cub.fr
nameserver 192.168.x.10
```

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

```
root@ns0:~# host ns0
Host ns0 not found: 5(REFUSED)
```

Installer le service DNS (Bind)

```
root@ns0:~# apt update && apt upgrade
root@ns0:~# apt -y install bind9 dnsutils
```

Configurer le service DNS (Bind)

Modification du fichier /etc/bind/named.conf.options

Editez le fichier /etc/bind/named.conf.options pour :

- désactiver la récursivité,
- indiquer l'interface d'écoute du serveur (127.0.0.1 et 172.16.x.10) :

/ Printed on 2025/11/06 18:06

```
version none;
};
```

Modifiez le fichier de configuration /etc/bind/named.conf.local

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 "agence.cub.fr" {
   type master;
   file "/etc/bind/db.agence.cub.fr";
};
```

Voyons la signification de chaque champ :

Option	Commentaires		
zone "agence.cub.fr" {	Le nom de la zone entre guillemets et suivi d'une accolade.		
	Master indique que vous avez l'autorité sur la zone. D'autres serveurs (esclaves) pourront se synchroniser avec votre serveur.		
file "/etc/bind/db.agence.cub.fr";	Emplacement et nom du fichier de zone. Il sera placé dans /etc/bind/ et s'appellera db.agence.cub.fr		
};	L'accolade ferme la définition de la zone.		

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. Choisissez de créer des enregistrements pour vos serveurs DHCP et DNS.

Voici un contenu minimaliste pour ce fichier /etc/bind/db.agence.cub.fr que vous devez créer :

```
$TTL 1D
agence.cub.fr.
                      IN
                              SOA
                                       ns0.agence.cub.fr. root.agence.cub.fr. (
        2006031201
                         ; serial
                         ; refresh
        1D
        1H
                         ; retry
        1W
                         ; expire
        3H)
                         ; Negative Cache TTL
agence.cub.fr. IN
                        NS
                                 ns0.agence.cub.fr.
ns0
                IN
                        Α
                                 172.162.x.10
                IN
                        Α
                                 172.162.x.11
WWW
dhcp
                ΙN
                        Α
                                 172.168.x.y
```

Chaque ligne (qui ne commence pas par un \$) s'appelle un enregistrement DNS.

La première ligne (\$TTL 1D) indique la durée de vie des informations transmises par votre serveur 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 demandes. 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 deuxième ligne définit le nom du domaine (Notez bien le point à la fin du nom de domaine) et est 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 agence.cub.fr.

Voici sa structure :

agence.cub.fr. IN SOA	ns0.agence.cub.fr.	root.agence.cub.fr.	(2006031201; serial\\1D; refresh\\1H; retry\\1W; expire\\3H); Negative Cache TTL
Enregistrement DNS de type Internet (IN) déclarant notre autorité (SOA).			

From:

/ - Les cours du BTS SIO

Permanent link: /doku.php/reseau/dns/dnslan?rev=1700216536

Last update: 2023/11/17 11:22

