

Carnet de bord

SAE 21 – BERRA PAUL

- Introduction :

Dans le cadre de cette SAE, nous devons mettre en place le réseau informatique d'une petite entreprise multi-sites. L'objectif est que nous répondions aux besoins de commutation, routage, service réseaux de base et minimums de sécurités formulés par la structure.

- Spécificités :

En raison d'un budget alloué de 0 euros, le réseau sera mis en place en deux parties : une première virtuelle (émulée sur GNS3) correspondant au LAN de l'entreprise, qui contiendras le serveur web interne ainsi que les postes des employés répartis sur plusieurs VLAN en fonction du service. La deuxième partie, sera quand a elle physique, elle assurera l'interconnexion avec internet et la DMZ, elle comprendra le serveur web de l'extranet, le DNS et le routeur firewall.

Journal de bord :

Jeudi 24/03/2022 :

Cours d'introduction à la SAE 21, lors de ce cours on nous a expliquer les différentes attentes et spécificités liés a cette saé. On nous à aussi expliquer les méthodes d'évaluation de cette SAE.

Vendredi 25/05/2022 & lundi 28/02/2022 :

Cours lors desquels on a réfléchi les méthodes que nous allons mettre en place pour la construction du réseau : choix de gns3 et pas packet-tracer, utilisation de apache2, bind9, et openssh.

Mardi 29/02/2022 & Lundi 04/04/2022 :

Cours lors desquels j'ai réalisé un plan plus complet du réseau sur Draw.io afin d'avoir une base de travail saine pour toute l'équipe : on est d'accord sur le plan d'adressage, quelle marque de routeur à quel endroit et répartition des vlan. Nous avons revu plusieurs fois l'adressage pour éviter des problèmes futurs, ce qui a pris du temps.

Vendredi 08/04/2022

Lors de ce cours je me suis renseigné sur openssh. Je me suis penché sur les différentes possibilités que ce protocole offre, comment on le configure et quelle sont les bonnes pratiques à avoir.

J'ai fait plusieurs tests et configuration , j'ai rencontré de nombreux problèmes que j'ai du régler les uns après les autres :

Comment installer openssh sans être en réseau ?

- Il faut se connecter directement au cloud

Pourquoi le paquet ssh était « intéléchargeable » ?

- Faire un apt-update avant d'essayer de le télécharger

Erreur de « Cypher » :

- Décommenter la ligne Ciphers et remplacer la chaîne de caractère par aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc.

Aucunes commandes en particulier n'a était taper, je les listerai toutes dans l'ordre et dans la partie « configuration du ssh »

Vendredi 15/04/2022 :

Lors de ce TP de 2H45 et du TD de 1h15, je me suis occupé de la réalisation d'un script en Bash permettant d'automatiser la configuration et le déploiement des serveurs DNS et WEB.

Pour cela j'ai d'abord créer les fichiers de configuration que je vais utiliser :

Pour le DNS

Fichier 1 : Le resolv.conf

la commande en tant que tel est

```
sudo nano resolv.conf
```

On y met ensuite le contenu suivant :

```
search ansinelliberrandeyeco
nameserver 123.123.14.53
```

Cela va permettre d'indiquer le serveur DNS a utiliser par défaut.

Fichier 2 : Le named.conf.options

Faire une manipulation similaire avec "named.conf.options"

```
sudo nano named.conf.options
```

Le contenu du fichier doit être le suivant :

```
options {
    directory "/var/cache/bind";
    forwarders {
        8.8.8.8;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    listen-on-v6 { ::1; };
};
```

Le décommentage de la partie forwarder permet de rediriger vers un autre DNS les requêtes que nous ne pourrions pas résoudre

Nous indiquons aussi au DNS d'écouter les requêtes IPV6 en provenance de sa loopback.

Fichier 3 : Le named.conf.local

Ensuite on continue avec le fichier d'enregistrement de zone :

```
sudo nano named.conf.local
```

On y met le contenu suivant :

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

Cela permet de lui indiquer que les données liées à la zone "ansinelliberrandeyeco" se situent dans "/etc/bind/db.ansinelliberrandeyeco". Cela permet aussi d'indiquer que le DNS est "maître" dans cette zone.

Enfin, le dernier fichier est le fichier de zone de notre enregistrement :

Fichier 4 : Le db.ansinelliberrandeyeco

faire :

```
sudo nano db.ansinelliberrandeyeco
```

Il faut ensuite y mettre le contenu suivant :

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@ IN SOA ns.ansinelliberrandeyeco. root.ansinelliberrandeyeco. (
                        3      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@ IN NS  ns.ansinelliberrandeyeco.
@ IN A   123.123.14.53
ns IN A   123.123.14.53
www IN CNAME ns
```

Voila, tous les fichier utiles a notre DNS sont maintenant créés et configurer il suffit maintenant de faire :

```
sudo apt-get --purge remove bind9 && sudo apt-get install bind9
```

Ensuite,

```
rm /etc/bind/named.conf.local | rm /etc/bind/named.conf.options | rm /etc/hosts
```

Puis :

```
cp named.conf.local rm /etc/bind/ | cp named.conf.options /etc/bind/ | cp hosts
/etc/ | cp db.ansinelliberrandeyeco /etc/bind/
```

Et enfin :

```
sudo systemctl restart bind9
```

Pour le serveur WEB

D'abord il faut nettoyer et installer apache2.

```
sudo apt-get --purge remove apache2 -y && sudo apt-get install apache2 -y && sudo  
systemctl enable apache2
```

Créer ensuite un fichier index.html comme suit :

```
nano index.html
```

Il faut y mettre le contenu suivant :

```
<HTML>  
  <head>  
    <!-- En-tête de la page -->  
    <meta charset="utf-8" />  
    <title> YONDBE21&CO </title>  
  </head>  
  <body>  
    <center>  
      <h1> ANSINELLI&BERRA&NDEYE&CO </h1>  
    </center>  
  </body>  
</HTML>
```

Faire ensuite :

```
sudo cp index.html /var/www/html/
```

On désactive ensuite le site par défaut :

```
sudo a2dissite 000-default.conf
```

Ensuite copier et renommer ce site par défaut

```
mv /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-  
available/ansinelliberrandeyeco.conf
```

Supprimer le fichier par défaut :

```
sudo rm /etc/apache2/sites-available/000-default.conf
```

Editer ensuite le fichier hosts avec la commande suivante :

```
sudo nano /etc/hosts
```

Y mettre ce contenu :

```
127.0.0.1          localhost
10.213.11.1        213-11
127.0.0.1          ANSINELLIBERRANDEYECO
# The following lines are desirable for IPv6 capable hosts
::1               localhost ip6-localhost ip6-loopback
ff02::1           ip6-allnodes
ff02::2           ip6-allrouters
```

Plus que quelques commandes :

```
Sudo a2ensite "ansinelliberrandeyeco.conf"
```

Cela va activer notre site

Enfin :

```
sudo systemctl reload apache2
```

Pour relancer apache2

Concrètement le script que j'ai réalisé automatise ces actions, de plus cela est bien pratique car les configurations DNS sont fournies par le DHCP et sont donc remis à jour plutôt régulièrement, cela évite aussi d'être parasité par des fichiers hosts et des sites configurés par d'autres personnes sur la machine.

Le script s'appelle « `apache2conf.sh` » sur le github.

Configuration du service SSH

Pour chaque machines :

POUR CHAQUE MACHINES :

1. Rajouter un DNS dans le fichier `/etc/resolv.conf`
2. Faire un apt update

3. Installer le packet openssh server :

```
apt install openssh-server
```

4. Démarrer les serveurs sur chaque machine avec la commande :

```
/etc/init.d/ssh start
```

5. Ne pas oublier de créer un utilisateur : adduser test et en passwd : test, le reste on ne mettra rien

6. Se rendre dans le fichier /etc/ssh/ssh_config avec nano ou vim :

- Ajouter la ligne : KexAlgorithms diffie-hellman-group1-sha1,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1
- Décommenter la ligne Ciphers et remplacer la chaîne de caractère par : aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc

Ces deux lignes vont vous permettre de pouvoir ssh le routeur.

7. Vous pouvez désormais ssh les machines que vous souhaitez avec la commande : ssh test@IP

ATTENTION !

Il se peut que vous ne puissiez toujours pas ssh la machine et que ça vous demande d'ajouter une chaîne de caractère en plus pour Ciphers dans le fichier ssh_config, ajouter celle qui est écrite et vous pourrez ensuite ssh.