# Installation de l'application WebDNS

Version 1.2 – 12 avril 2004
Pierre David, Jean Benoit

## Table des matières

# 1 Introduction

L'application WebDNS a été présentée[1] pour la première fois aux Jres 2003 à Lille. Depuis, elle a suscité un intérêt qui a motivé les auteurs à rentrer dans une logique de diffusion pour la communauté.

L'objectif principal de WebDNS est de déléguer la gestion du DNS à un public de « correspondants réseau » sur un réseau, qu'il soit de laboratoire, de campus, métropolitain, etc.

Jusqu'en 2002, le réseau métropolitain strasbourgeois Osiris[2] fonctionnait sans délégation : pour toute modification, les correspondants faisaient appel au service réseau qui saisissait manuellement les informations. Parmi les caractéristiques du réseau Osiris, on trouve une cinquantaine de zones, dont une (`u-strasbg.fr`) regroupe à l'heure actuelle plus de 20 000 noms, ainsi qu'une population d'environ une centaine de correspondants réseau appartenant à une quinzaine d'établissements différents. Souhaitant offrir à ces correspondants davantage d'indépendance tout en leur apportant un meilleur service, les auteurs se sont donc attelés à la rédaction de WebDNS et l'application a été rendue accessible aux correspondants réseau en juin 2002.

Ce document décrit en détail l'installation de l'application, ainsi que certains éléments du paramétrage. Une bonne connaissance du DNS, du système Unix, et de la configuration d'un serveur Web sont requises.

[1] http://2003.jres.org/actes/paper.144.pdf
[2] http://www-crc.u-strasbg.fr/osiris

# 2 Principes

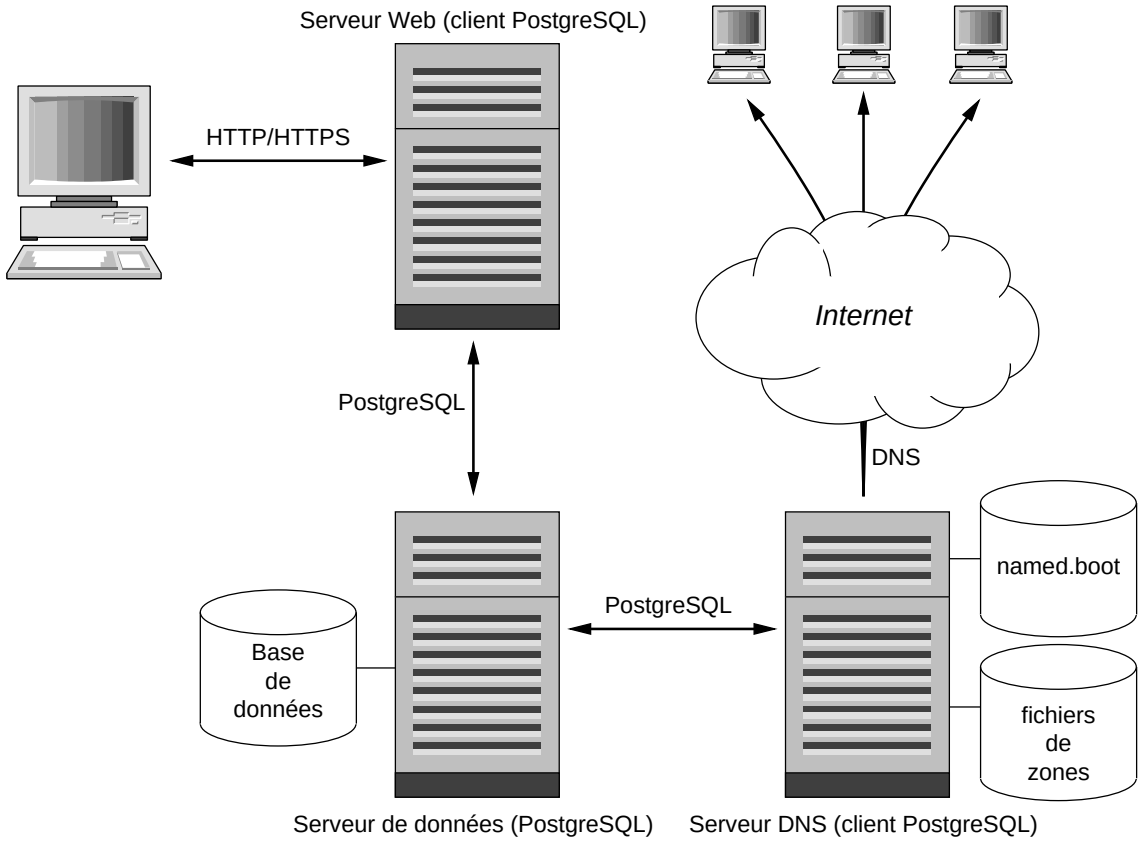
## 2.1 Objectifs

L'application WebDNS est une application permettant de gérer une ou plusieurs zones DNS, et d'en déléguer tout ou partie à une population d'utilisateurs (les correspondants réseaux) par un mécanisme de droits assez fin.

De plus, l'application WebDNS constitue le cœur d'un système complet de gestion d'un réseau universitaire (qu'il soit de laboratoire, de campus, métropolitain ou régional).

## 2.2 Les constituants de l'application WebDNS

Le principe général de fonctionnement de l'application est résumé sur la figure ci-dessous :




Dans cette figure, l'utilisateur accède à ses données par l'intermédiaire de son navigateur Web, via les protocoles HTTP/HTTPS. Le **serveur Web** (typiquement Apache) ne fait que mettre en forme des données, qui elles-mêmes stockées sur le **serveur de données**. Le serveur de données abrite la base de données PostgreSQL, et le serveur Web communique avec le serveur de données par l'intermédiaire du protocole PostgreSQL.

Le serveur DNS (typiquement Bind) récupère périodiquement (via `cron`) les informations qui ont changé dans la base de données, via là encore le protocole PostgreSQL, et les stocke dans les fichiers de zone classiques. Le fichier `named.conf` de Bind, quant à lui, est constitué par l'administrateur du système et n'est pas généré par l'application.

### 2.3 Authentification

L'authentification des utilisateurs est réalisée par le serveur Web. La base des utilisateurs, qui est externe à l'application WebDNS, repose sur le logiciel WebAuth (voir 4.1.1, page 4).

## 3 Structure de la distribution

La distribution de l'application WebDNS est organisée comme suit :

| | |
|---|---|
| `doc/` | documentation |
| `dump/` | répertoire de sauvegarde quotidienne de la base |
| `expl/` | scripts de maintenance et d'exploitation de la base |
| `htg/` | générateur de pages Web |
| `inst/` | scripts d'installation et de chargement initial de la base |
| `pkgtcl/` | paquetages Tcl utilisés par les divers scripts |
| `www/` | arborescence visible par le serveur Web, fichiers HTML |
| `www/bin` | l'application Web elle-même : les scripts CGI |
| `www/lib` | fichiers utilisés par les scripts, y compris les pages HTML à trous |

## 4 Pré-requis

Cette section décrit les pré-requis avant d'entamer l'installation.

### 4.1 Composants nécessaires

Les composants logiciels nécessaires pour l'application WebDNS sont décrits ci-après.

#### 4.1.1 WebAuth

L'authentification des utilisateurs repose sur une base externe à l'application, gérée par l'application[3] « WebAuth ».

L'installation de WebAuth est un prérequis indispensable pour l'installation de WebDNS. Le lecteur attentif pourra noter que beaucoup d'éléments (comme notamment ces prérequis et leur installation) sont communs entre les deux applications. Par conséquent, beaucoup d'éléments de cette documentation font référence directement à la documentation de WebAuth.

Disponibilité : http://www-crc.u-strasbg.fr/webdns/

#### 4.1.2 Apache

Voir WebAuth.

[3] Également développée par les mêmes auteurs.

#### 4.1.3 Tcl

Voir WebAuth.

#### 4.1.4 PostgreSQL

Voir WebAuth.

Note : la gestion des adresses IPv6 dans WebDNS repose sur le type de données « INET » de PostgreSQL, et plus spécifiquement sur son extension aux adresses IPv6 à partir de PostgreSQL version 7.4.

#### 4.1.5 mod_auth_pgsql

Voir WebAuth.

#### 4.1.6 LaTeX

Voir WebAuth.

### 4.2 Contexte système

#### 4.2.1 Activer les mots de passe PostgreSQL

Voir WebAuth.

#### 4.2.2 Utilisateur PostgreSQL

Voir WebAuth.

L'application WebDNS utilise l'utilisateur PostgreSQL nommé « `dns` ». Comme dans WebAuth, il n'y a pas besoin de créer un compte Unix pour cet utilisateur.

#### 4.2.3 Accès à PostgreSQL depuis les autres serveurs

La plupart du temps, vous séparerez diverses fonctions sur des serveurs physiquement différents :

– le serveur Web ;
– le serveur DNS ;
– le relais de messagerie, si vous utilisez les « rôles de messagerie » (voir B.6.2, page 22).

Il faut donc configurer le serveur PostgreSQL pour autoriser l'accès depuis ces différents serveurs. Pour cela, modifiez le fichier `~pgsql/data/pg_hba.conf` pour y insérer des lignes de la forme :

```
host dns dns 192.168.1.2 255.255.255.255 password
```

Cette ligne autorise l'accès à la base `dns` par l'utilisateur `dns` depuis la machine d'adresse IPv4 192.168.1.2. Bien sûr, si l'accès se fait par IPv6, vous remplacerez l'adresse et le masque par les valeurs appropriées.

# 5 Personnalisation des pages HTML et LaTeX

Voir WebAuth.

# 6 Installation et chargement de la base PostgreSQL

Ce chapitre décrit la mise en place de la base de données.

Il est vraisemblable que vous ne faites pas une installation ex-nihilo de l'application WebDNS, mais que vous cherchez à intégrer un existant, sous forme de zones DNS, de listes de réseaux et de correspondants. Cette section est donc consacrée au chargement initial de la base en reprenant votre existant.

Il est très conseillé de lire attentivement le modèle des données (voir annexe A, page 18) ainsi que l'annexe B (voir page 19) sur le paramétrage de l'application WebDNS. Ces deux annexes décrivent en détail les principaux concepts utilisés dans la suite.

La reprise d'un existant, parfois chargé d'histoire, représente un défi majeur. L'insertion des données dans une base, avec les contraintes que cela représente, nécessite un effort important de rationalisation dont vous n'avez pas forcément conscience à ce stade. C'est pour cela que les opérations de reprise de l'existant sont effectuées par des scripts que vous pouvez « rejouer » autant de fois que vous le souhaitez. En tout état de cause, ne vous découragez pas : le résultat en vaut la peine[4].

## 6.1 Vérification de vos zones

L'étape indispensable, avant d'aller plus loin, consiste à vous assurer que vos zones sont correctes. Deux outils sont essentiels pour cela :

– les fichiers de journalisation de votre serveur DNS ;
– l'utilitaire ZoneCheck[5] de l'AFNIC.

Si, si, regardez encore. Vraiment. C'est indispensable.

## 6.2 Création d'un groupe dans la base d'authentification

Il faut maintenant créer un groupe dans la base d'authentification pour les utilisateurs de l'application WebDNS. Ceci est réalisé au moyen de l'application WebAuth (menu « Groupes/Ajouter »).

Par exemple, les correspondants du réseau métropolitain strasbourgeois « Osiris » sont regroupés dans le groupe « `osiris` ».

Le groupe choisi devra être spécifié dans la configuration Apache d'accès à l'application (voir 7.2, page 14), ainsi que dans l'application elle-même (voir plus bas, 6.4.2, page 9) pour la création de nouveaux correspondants.

Une fois le groupe créé avec WebAuth, n'oubliez pas de vous y ajouter (par l'intermédiaire du menu « Groupes/Modifier » par exemple).

## 6.3 Création de la base

Examinez le script `./inst/creer-base`. Dans ce script :

[4] Sinon, vous ne liriez pas cette documentation, n'est-ce pas ?
[5] http://www.afnic.fr/outils/zonecheck

– modifiez votre mot de passe PostgreSQL ;
– mettez en commentaire la ligne « `exit 0` » située vers le début du fichier. Lorsque vous aurez exécuté le script, remettez le # qui vous protégera ainsi d'une maladresse si vite arrivée !
– modifiez les logins des utilisateurs privilégiés. Ces utilisateurs (PostgreSQL) doivent pouvoir réaliser toutes les opérations dans la base. Pour cela, tous les droits sont donnés aux tables de l'application.

Après avoir changé votre répertoire courant pour `./inst`, vous pouvez à présent exécuter le script.

Pour vérifier si tout s'est bien passé, vous pouvez utiliser « `psql` » pour passer les deux commandes `\dt` (afficher les tables) et `\q` (sortir) :

```
$ psql dns dns
dns=# \dt
           List of relations
 Schema |     Name      | Type  | Owner
--------+---------------+-------+-------
 public | communaute    | table | pda
 public | config        | table | pda
 public | corresp       | table | pda
 public | domaine       | table | pda
 public | dr_dom        | table | pda
 public | dr_ip         | table | pda
 public | dr_mbox       | table | pda
 public | etablissement | table | pda
 public | groupe        | table | pda
 public | hinfo         | table | pda
 public | plage         | table | pda
 public | relais_dom    | table | pda
 public | reseau        | table | pda
 public | role_mail     | table | pda
 public | role_web      | table | pda
 public | rr            | table | pda
 public | rr_cname      | table | pda
 public | rr_ip         | table | pda
 public | rr_mx         | table | pda
 public | zone          | table | pda
 public | zone_normale  | table | pda
 public | zone_reverse4 | table | pda
 public | zone_reverse6 | table | pda
(23 rows)

dns=# \q
```

## 6.4 Chargement initial des données

Tous les scripts d'initialisation et de chargement sont situés dans le sous-répertoire `./inst`.

### 6.4.1 Script `init-base`

Le script `init-base` est normalement le seul que vous lancerez directement. Il enchaîne toutes les actions individuelles, qui sont schématisées dans le tableau ci-après :

| Script | Action | Tables concernées | Fichiers en entrée |
|---|---|---|---|
| `remplir-config` | Initialise les tables de configuration du référentiel | `config`, `hinfo` | (aucun) |
| `remplir-grpnet` | Charge les réseaux, crée les correspondants (qui sont censés pré-exister dans WebAuth), crée les groupes et leur affecte les réseaux et les adresses IP autorisées. | `communaute`, `corresp`, `dr_ip`, `etablissement`, `groupe`, `plage`, `reseau` | `subnet.txt` `group.txt` |
| `charger-domaines` | Enchaîne les appels au script `remplir-domaine` pour chacun des domaines gérés, dans le bon ordre. | cf ci-dessous | (aucun) |
| `remplir-domaine` | Explore un fichier de zone pour remplir la base avec tous les RR de type A, AAAA ou CNAME trouvés après le prologue. | `domaine`, `rr`, `rr_cname`, `rr_ip` | fichier de zone |
| `remplir-grpdom` | Initialise les domaines accessibles par chaque correspondant | `domaine`, `dr_dom` | `grpdom.txt` |
| `remplir-rolemail` | Associe un hébergeur à toutes les adresses de messagerie déclarées, initialise les relais associés aux domaines et ajoute les droits correspondants aux groupes. | `dr_dom`, `role_mail`, `rr` | `rolemail.txt`, `relaisdom.txt` |
| `charger-zones` | Enchaîne les appels au script `remplir-zone` pour chacune des zones DNS. | cf ci-dessous | (aucun) |
| `remplir-zone` | Remplit les paramètres de génération d'une zone, dont le prologue, extrait du fichier de zone. | `zone_normale`, `zone_reverse4`, `zone_reverse6` | fichier de zone, `rrsup.txt` |
| `remplir-triggers` | Crée les *triggers* et les fonctions PL/SQL qui seront appelés pour marquer une zone comme étant « à générer » lorsqu'un nom ou une adresse IP est modifiée. | (aucune) | (aucun) |

Le lecteur attentif constatera que toutes les tables de la base ne sont pas modifiées par ces scripts. En effet, les tables non citées sont apparues après la rédaction des scripts, qui n'ont pas été modifiés depuis.

Normalement, le script n'est censé être appelé qu'une seule fois, au chargement initial. Cependant, il est très vraisemblable que vos données devront être modifiées à la lumière des premières incohérences détectées par les scripts, ou lors des tests de l'application. Vous pouvez bien sûr recréer la base (script `creer-base`) et refaire le chargement (script `init-base`) autant de fois que vous le désirez.

Les scripts `remplir-domaine` et `remplir-zone` utilisent tous deux vos fichiers de zones existants, tels qu'ils sont utilisés par votre serveur DNS. Vous allez devoir séparer deux parties dans chaque fichier : le prologue, et la liste des RR. Pour cela, il vous suffit d'insérer un commentaire (voir la description des scripts) à l'endroit de la coupure. Ainsi, les fichiers consultés pour le chargement peuvent directement être les fichiers que vous exploitez sur le serveur DNS. Ceci peut s'avérer intéressant si le chargement initial prend plus de temps que prévu et si vous voulez continuer à ajouter ou supprimer des machines sur le serveur DNS pendant toute la durée de l'opération.

Enfin, tous les scripts (de la forme `remplir-*`) doivent être modifiés pour référencer l'interprète Tcl et fournir le mot de passe que vous aurez choisi pour accéder à la base. Le script `substituer` pourrait bien vous être d'un grand secours pour automatiser ces modifications.

### 6.4.2 Script `remplir-config`

Ce script est le plus simple de tous. Il remplit les deux tables `config` (paramètres de l'application) et `hinfo` (types de machines reconnues).

Hormis le mot de passe (variable `PGPASSWORD`), il faut modifier la liste des groupes WebAuth qui peuvent accéder à l'application. Cette dernière information n'est utilisée que lorsque vous procéderez à la création d'un compte pour un correspondant.

### 6.4.3 Script `remplir-grpnet`

Ce script est sans doute un des plus complexes. Il crée :

- les établissements et les communautés, à partir de valeurs dans le script lui-même ;
- les groupes et les correspondants, à partir d'un fichier contenant, sur chaque ligne, le nom d'un groupe suivi par le ou les logins des correspondants rattachés à ce groupe.
  Par exemple :

  ```
  sysadm pda jean
  laboX toto
  ```

  Dans cet exemple, le groupe WebDNS `sysadm` est créé, rassemblant les correspondants de logins `pda` et `jean`. Les correspondants sont supposés avoir déjà été créés dans la base WebAuth.
  Attention : la notion de groupe WebDNS (autorisation de modification d'un domaine et d'une plage d'adresses IP) ne doit pas être confondue avec la notion de groupe WebAuth (autorisation d'accès à une portion de l'arborescence Web).
- les réseaux à partir d'un fichier contenant des entrées de la forme :

  ```
  nom=Serveurs
  subnet=192.168.1.0
  netmask=255.255.255.0
  gateway=192.168.1.254
  commentaire=Réseau des serveurs
  etablissement=ULP
  communaute=Recherche
  localisation=Batiment principal
  groupes=sysadm
  ```

  Note : ce script ne gère pour le moment que des adresses IPv4. Le portage pour charger un réseau IPv6 existant n'est pas encore effectué[6].

Le script `remplir-grpnet` doit être modifié pour :

- le chemin de l'interprète Tcl ;
- le mot de passe d'accès à la base DNS ;
- la liste des établissements (en laissant la chaîne « `INCONNU` » en fin de liste) ;
- la liste des communautés (en laissant la chaîne « `INCONNUE` » en fin de liste) ;
- la liste des groupes ayant l'autorisation de paramétrer l'application (il n'y aura vraisemblablement qu'un seul groupe, le vôtre);

### 6.4.4 Scripts `charger-domaines` et `remplir-domaine`

Le script `remplir-domaine` analyse un fichier de zone et charge dans la base les RR de type A, AAAA ou CNAME qui se trouvent après le prologue. Les RR de type MX sont ignorés. Les autres types de RR sont également ignorés, mais ils sont signalés par un message.

[6] Rassurez-vous, le script de chargement des machines, `remplir-domaine`, sait traiter les RR de type AAAA contenant des adresses IPv6.

Tous les RR créés le sont avec un nom de login de correspondant. Sur Osiris, nous avons chargé tous les RR avec un login d'un correspondant fictif. Ceci nous permet de déterminer facilement les RR issus du chargement initial, par opposition aux RR ajoutés depuis.

La fin du prologue est déterminée par la recherche d'une expression régulière dans le fichier de zone. Cette expression est, par défaut :

```
^; COUPER ICI
```

En insérant cette ligne (qui est un commentaire, le `^` désigne le début de la ligne) dans vos fichiers de zone, vous pouvez aisément délimiter la fin du prologue sans perturber l'exploitation du serveur DNS pendant que vous mettez au point le chargement de la base.

Attention : les RR doivent avoir une syntaxe valide pour le nom en partie gauche. En particulier, le nom ne doit comporter aucun point. Un problème souvent rencontré est la tentative de chargement d'un RR de type « `www.truc IN CNAME www.univ-machin.fr` » : la partie gauche n'est pas valide puisque `www.truc` n'est pas un nom valide. Si vous rencontrez ce cas, vous avez deux solutions : soit créer une nouvelle zone pour `truc.univ-machin.fr`, soit déplacer le RR fautif dans le prologue, auquel cas il devient une exception gérée manuellement avec tous les risques d'incohérence ultérieure que cela comporte.

Les RR de type CNAME sont ajoutés dans la base à la fin de la lecture du fichier de zone. Cela signifie qu'on peut très bien écrire le CNAME d'abord, puis écrire le A ou le AAAA correspondant après. Lorsqu'un CNAME pointe sur un nom inexistant, l'information est signalée. Si vous avez deux fichiers de zones (f1 et f2 par exemple) avec un CNAME dans f1 qui pointe sur un A dans f2, cela signifie qu'il faut charger d'abord f2, puis ensuite f1. Dans le cas d'une référence croisée (un CNAME dans f2 qui pointe en plus sur un A dans f1), cela signifie qu'il faudra charger deux fois le même fichier (f1 ou f2) pour résoudre la référence : il faudra donc par exemple charger f1, puis f2, puis f1 à nouveau. Lors du rechargement d'une zone, les RR déjà introduits sont ignorés.

Le script `remplir-domaine` doit être modifié pour :

- le chemin de l'interprète Tcl ;
- le mot de passe d'accès à la base DNS ;
- le motif de détection de fin du prologue, si vous décidez d'en choisir un autre.

Le script `charger-domaines` enchaîne les appels individuels à `remplir-domaine`. Vous devez modifier ce script pour paramétrer le remplissage des domaines, dans le bon ordre, avec éventuellement le rechargement de fichiers déjà introduits si vous avez des références croisées.

### 6.4.5 Script `remplir-grpdom`

Le script `remplir-grpdom` associe une liste de domaines à chaque groupe. De plus, cette liste de domaines est ordonnée selon une classe de tri (les valeurs les plus proches de 0 sont les plus prioritaires), de façon que chaque membre d'un groupe puisse voir en premier les domaines qui le concernent.

Ce script est dirigé par un fichier `grpdom.txt` contenant des lignes de la forme :

*domaine* `ALLBUT`|`SET` *tri groupe ... groupe*

- les lignes de type `SET` associent le domaine aux groupes désignés, avec la classe de tri spécifiée ;
- les lignes de type `ALLBUT` associent le domaine à tous les groupes (avec la classe de tri spécifiée), sauf ceux désignés explicitement.

Le script suppose que tous les groupes et les domaines cités dans ce fichier existent dans la base. Les premiers ont été chargés par le script `remplir-grpnet` et les seconds ont été chargés par le script `remplir-domaine`.

Le script `remplir-grpdom` doit être modifié pour :

– le chemin de l'interprète Tcl ;
– le mot de passe d'accès à la base DNS.

### 6.4.6 Script `remplir-rolemail`

Le script `remplir-rolemail` initialise la liste des adresses de messagerie, et leur associe un hébergeur. Pour plus d'information sur la gestion des rôles de messagerie, voir l'annexe B.6.2 (page 22).

Ce script est dirigé par deux fichiers. Le premier est `rolemail.txt` contenant des lignes de la forme :

*adresse* [ *nom-de-l'hébergeur* ]

L'« *adresse* » est l'adresse de messagerie pour laquelle un MX doit être publié, et le « *nom-de-l'hébergeur* » est le nom de la machine hébergeant les boîtes aux lettres. Si ce dernier n'est pas fourni, il correspondant par défaut à l'adresse de messagerie.

Le deuxième fichier, `relaisdom.txt`, précise les relais de messagerie associés à chaque domaine, qui seront publiés dans les MX des adresses de messagerie spécifiées dans le précédent fichier. Le fichier contient des lignes de la forme :

*domaine priorité machine ... priorité machine*

Le script suppose que tous les domaines et tous les relais existent dans la base : ils doivent avoir été chargés par les scripts `remplir-domaine` et `remplir-grpdom`.

Si vous choisissez de ne pas utiliser les rôles de messagerie, videz les deux fichiers. Vous pourrez toujours utiliser ultérieurement ce script sur la base de production.

Le script `remplir-rolemail` doit être modifié pour :

– le chemin de l'interprète Tcl ;
– le mot de passe d'accès à la base DNS.

### 6.4.7 Scripts `charger-zones` et `remplir-zone`

Le script `remplir-zone` analyse un fichier de zone et charge dans la base les informations de génération de zone : le nom et le type (normale, reverse IPv4 ou reverse IPv6) de la zone, le critère de sélection des RR devant figurer dans la zone, le numéro de version initial, le fichier de zone contenant le prologue, les RR supplémentaires éventuels ainsi que la valeur initiale du flag « générer ».

Comme dans le script `remplir-domaine`, la fin du prologue est déterminée par recherche d'une expression régulière dans le fichier de zone. Là encore, cette expression est, par défaut :

```
^; COUPER ICI
```

Le numéro de version fourni en paramètre est le numéro initial devant être inscrit dans la base. Il doit être de la forme AAAAJJMMnn (voir annexe B.5, page 21). La valeur du numéro de version que vous fournissez au script n'a pas grande importance, à partir du moment où elle est antérieure à la date courante, si vous mettez le flag de génération à 1 : la première génération provoquera une actualisation automatique du numéro de version.

Le prologue contient le RR de type SOA de la zone. Ce SOA contient en particulier le numéro de version. Lors de la génération des zones, la chaîne « `%VERSION%` » sera substituée par le numéro de version courant dans la base (en l'actualisant bien sûr). Pour cette raison, le script `remplir-zone` recherche dans le SOA le numéro de version courant et le substitue par la chaîne « `%VERSION%` » lors du remplissage du prologue dans la base. Ceci est réalisé grâce à une expression régulière, qui vaut par défaut :

```
^([ \t]+)([0-9]+)([ \t]+;[ \t]*Version.*)
```

Cette expression recherche une ligne décomposée en trois parties par les parenthèses : la première est située avant le numéro de version, la deuxième est le numéro de version lui-même et la troisième est ce qui suit (soit le commentaire « ; `Version` » ici). Grâce à cette expression régulière, la cohérence du numéro de version actuel est vérifiée, puis il est remplacé par la fameuse chaîne « `%VERSION%` ».

Le script `remplir-domaine` doit être modifié pour :

– le chemin de l'interprète Tcl ;
– le mot de passe d'accès à la base DNS ;
– le motif de détection de fin du prologue, si vous décidez d'en choisir un autre ;
– le motif de détection du numéro de version dans le SOA, si vous décidez d'en choisir un autre ;

Le script `charger-zones` enchaîne les appels individuels à `remplir-zone` avec les bons paramètres. Vous devez modifier ce script pour paramétrer le remplissage des zones.

#### 6.4.8 Script `remplir-triggers`

Le script `remplir-triggers` est indépendant des données du chargement initial de la base. Il implémente les *triggers* associés à certaines tables, qui permettent en particulier de mettre le flag de génération d'une ou plusieurs zones à 1 lorsqu'un RR est modifié. Il implémente également les fonctions appelées lors de l'exécution de ces *triggers*.

Étant donné que les *triggers* pénalisent les performances, ils ne sont activés qu'à la fin du chargement initial. Rassurez-vous, en temps normal, avec des modifications unitaires, l'impact sur les performances est absolument négligeable.

Le script `remplir-triggers` doit être modifié pour :

– le mot de passe d'accès à la base DNS.

#### 6.4.9 Exécution !

Une fois tous les scripts modifiés selon vos souhaits, lancez le script `./inst/init-base`. Lorsque vous n'aurez plus d'erreurs et que vous saurez expliquer tous les messages d'avertissement, vous pourrez vérifier si l'installation s'est bien passée. Par exemple, vous pouvez utiliser « `psql` » pour vérifier quelques tables :

```
$ psql dns dns
dns=# \encoding latin9
dns=# SELECT * FROM etablissement ;    -- lister les établissements
 idetabl |   nom
---------+---------
       1 | ULP
       2 | UMB
       3 | URS
       4 | INCONNU
(4 rows)

dns=# SELECT COUNT(*) FROM rr ;        -- compter le nombre de noms enregistrés
 count
-------
 19223
(1 row)
```

```
dns=# SELECT COUNT(*) FROM rr_ip ;     -- compter le nombre d'adresses IP
 count
-------
 18936
(1 row)

dns=# \q
```

Essayez quelques-unes des tables de l'application (voir annexe A, page 18). Si les valeurs sont correctes, vous avez terminé la phase délicate de l'installation, vous pouvez maintenant passer à la suite.

# 7 Installation de l'application

## 7.1 Installation des fichiers de l'application

Choisissez un répertoire pour placer les pages Web et les scripts CGI de l'application, qui ne doit pas être le répertoire dans lequel vous avez détarré l'application. Dans l'installation par défaut, ce répertoire est nommé `/local/services/www/applis/dns/`.

- si vous souhaitez utiliser HTG, recopiez les fichiers du répertoire `./www/lib/` en modifiant éventuellement les parties « bannière », « titrepage » et « bandeau » ;
- si vous souhaitez concevoir des nouvelles pages à trous, installez-les dans le répertoire `./www/lib/`. Vous devrez supprimer chaque fichier « .htgt » et le remplacer par un fichier « .html » équivalent, en respectant le nom des trous que les scripts CGI s'attendent à trouver (voir annexe C, page 24). Vous prendrez soin également à adapter les fichiers LaTeX `liste.tex` et `listedes.tex`.

Rendez-vous ensuite dans le répertoire `./www` et éditez le fichier `Makefile`. Modifiez les variables :

| Variable | Signification |
|---|---|
| `TCLSH` | localisation de l'exécutable `tclsh` |
| `BASE` | nom de la base de données et paramètres d'ouverture |
| `AUTH` | méthode d'authentification et paramètres |
| `HOMEURL` | chemin relatif à la racine de l'arborescence Web |
| `NOLOGIN` | nom du fichier à créer pour rentrer en mode « maintenance » |
| `DESTDIR` | localisation de l'application dans l'arborescence Web |
| `PKGTCL` | localisation des packages Tcl inclus avec l'application |
| `HTG` | localisation de l'exécutable `htg` |
| `ROOT` | utilisateurs (Apache) habilités à intervenir en mode « maintenance » |
| `INTERVALLE` | intervalle entre deux générations de zones (doit correspondre à la valeur spécifiée avec `cron`) afin d'informer les utilisateurs |
| `DOCDNS` | URL d'une page présentant votre architecture DNS, pointée par diverses pages de l'application. |

Puis, lancez `make` (dans le répertoire `./www`) pour installer tous les fichiers de l'application dans l'arborescence Web.

## 7.2 Configuration du serveur Apache

Le serveur Apache doit être configuré pour :

– autoriser l'accès en consultation à `/local/services/www/applis/dns/`
– autoriser l'accès en exécution CGI à `/local/services/www/applis/dns/bin`
– interdire tout accès à `/local/services/www/applis/dns/lib`

Ceci peut être réalisé grâce aux quelques lignes suivantes (voir `./inst/httpd.conf`) dans le fichier `httpd.conf` de configuration d'Apache, que vous prendrez soin d'adapter :

```
ScriptAlias "/applis/dns/bin/" "/local/services/www/applis/dns/bin/"

<Directory /local/services/www/applis/dns>
    #
    # Ces lignes peuvent astucieusement être mises en commun
    # en les déclarant dans le répertoire racine de votre
    # serveur Web.
    #
    AuthName "Intranet CRC"
    Auth_PG_host             localhost
    Auth_PG_port             5432
    Auth_PG_database         auth
    Auth_PG_user             auth
    Auth_PG_pwd              mot-de-passe-en-clair-de-auth
    Auth_PG_pwd_table        utilisateurs
    Auth_PG_uid_field        login
    Auth_PG_pwd_field        password
    Auth_PG_grp_table        membres

    # Attention : version avec mod_auth_pgsql
    #Auth_PG_gid_field       groupe
    # Attention : version avec mod_auth_pgsql2
    Auth_PG_grp_group_field  password
    Auth_PG_grp_user_field   membres

    #
    # Fin des lignes pouvant être mises en commun dans le
    # répertoire racine de votre serveur Web.
    #

    AuthType            Basic

    # Attention : adaptez les groupes ci-dessous en conséquence
    # Ici : sont autorisés les groupes "osiris" (correspondants réseau
    #    Osiris) et "crc" (personnels du CRC)
    require             group osiris crc

    # si vous avez une page prévue pour signaler les erreurs, mettez-la ici
    ErrorDocument       401 /errauth/cor.html
</Directory>

<Directory /local/services/www/applis/dns/lib>
    order deny,allow
    deny from all
```

```
</Directory>

Alias "/applis/dns" "/local/services/www/applis/dns"

RedirectMatch permanent ^/applis/dns/$ \
                https://www-crc.u-strasbg.fr/applis/dns/bin/accueil
RedirectMatch permanent ^/applis/dns/index.html$ \
                https://www-crc.u-strasbg.fr/applis/dns/bin/accueil
```

Quelques notes cependant :

- ces lignes font également référence à la directive `ErrorDocument` pour renvoyer une page d'erreur appropriée en cas d'échec d'authentification ; si vous n'avez pas une telle page, qui doit forcément être externe à l'application, supprimez la ligne ;
- enfin, l'utilisation du moteur de réécriture (directives `Rewrite...`) est nécessaire pour aiguiller les utilisateurs qui auraient spécifié `http` au lieu de `https`. Si vous ne disposez pas de l'extension SSL, vous pouvez supprimer ces lignes

## 7.3 Paramétrage de l'application

Une fois les étapes précédentes effectuées, vous devriez être en mesure d'accéder à l'URL de votre application. Vous pouvez alors rentrer dans le module « administration » pour finaliser les paramétrages.

## 7.4 Génération des zones

Les scripts `mkzones` et `generer-zone` doivent tous deux être copiés du répertoire `./expl/` vers le serveur DNS. Pour des raisons de sécurité, le mot de passe d'accès à la base figurant dans le script `generer-zone`, vous aurez intérêt à installer ces scripts sous le compte de votre utilisateur `bind` ou équivalent, si vous en avez un, et illisibles par tout autre utilisateur que le propriétaire.

### 7.4.1 Script `generer-zone`

Le script `generer-zone` a deux comportements différents :

- sans argument, il affiche sur la sortie standard la liste des zones qui ont été modifiées depuis la dernière génération (c'est-à-dire la liste des zones pour lesquelles l'attribut « generer » vaut 1) ;
- avec un argument (un nom de zone), il procède à la génération de la zone sur la sortie standard, et remet l'attribut « generer » à 0).

Ce script doit être modifié pour indiquer :

- le chemin vers l'interprète Tcl ;
- le nom du serveur de données (sur lequel vous aurez pris soin d'autoriser l'accès, voir 4.2.3, page 5) ;
- le mot de passe d'accès à la base.

Une fois ce script modifié, vous pouvez l'installer dans le répertoire de votre choix.

### 7.4.2 Script `mkzones`

Le script `mkzones` est conçu pour être lancé par `cron`, par exemple toutes les 10 minutes (soit au maximum 144[7] modifications par jour), avec une entrée de la forme :

[7] Ceci est théoriquement supérieur à 99 modifications autorisées par le numéro de version, mais dans la pratique, cette limite n'a jamais été rencontrée. Si cela devait être le cas, la génération échouerait, jusqu'au lendemain.

```
#
# La crontab de l'utilisateur "bind"
#
# Historique
#   2002/05/02 : génération des zones DNS à partir de la base
#

SHELL = /bin/sh
MAILTO = hostmaster@u-strasbg.fr

*/10 * * * * /local/sbin/mkzones
```

Le corps du script est très simple : un premier appel à `generer-zone` permet de récupérer la liste des zones à générer. Cette liste est utilisée dans une boucle qui génère chaque zone dans le répertoire temporaire. Si au moins une zone a été générée avec succès, le fichier correspondant est déplacé vers le répertoire où le serveur DNS s'attend à trouver les zones, puis le serveur est stimulé pour relire les fichiers.

Pour être installé :

- vous devez avoir au préalable modifié et installé le script `generer-zone` ;
- vous devez adapter `mkzones` pour votre usage local ;
- vous devez copier `mkzones` vers le serveur DNS ;
- et vous devez enfin activer la crontab ci-dessus.

## 7.5 Génération des routages de messagerie

Si vous utilisez les « rôles de messagerie » (voir B.6.2, page 22), vous souhaitez sans doute générer dynamiquement le fichier de routage de messagerie utilisé par `sendmail` ou équivalent.

Pour vous aider dans cette tâche, les scripts `mkroutages` et `generer-routages` doivent tous deux être copiés du répertoire `./expl/` vers les relais de messagerie. Pour des raisons de sécurité, le mot de passe d'accès à la base figurant dans le script `generer-routages`, vous aurez intérêt à installer ces scripts sous le compte d'un utilisateur spécifique et les rendre illisibles par tout autre utilisateur que le propriétaire.

### 7.5.1 Script `generer-routages`

Le script `generer-routages` génère sur la sortie standard un fichier prêt pour être utilisé comme table de routages avec le Kit Jussieu de configuration de `sendmail`, c'est-à-dire une liste de lignes de la forme :

*adresse* `smtp.`[*relais*]

où *adresse* est le nom du « rôle de messagerie », *relais* est l'adresse de l'hébergeur des boîtes aux lettres pour cette adresse de messagerie, telle que définie dans la base. Enfin, le mot-clef `smtp` indique que le *mailer* SMTP de `sendmail` doit être utilisé, et les crochets indiquent que l'envoi doit être effectué directement vers le relais, sans tenir compte des MX du DNS. Pour plus d'information, consulter la documentation du Kit Jussieu[8].

Ce script doit être modifié pour indiquer :

- le chemin vers l'interprète Tcl ;
- le nom du serveur de données (sur lequel vous aurez pris soin d'autoriser l'accès, voir 4.2.3, page 5) ;
- le mot de passe d'accès à la base.

Une fois ce script modifié, vous pouvez l'installer dans le répertoire de votre choix.

[8] http://www.kit-jussieu.org

### 7.5.2 Script `mkroutages`

Le script `mkroutages` est conçu pour être lancé par `cron`, par exemple toutes les 5 minutes, par exemple avec une entrée de la forme :

```
#
# La crontab de "root"
#

SHELL = /bin/sh
MAILTO = hostmaster@u-strasbg.fr

*/5 * * * * /local/sbin/mkroutages
```

Le script fonctionne en concaténant deux parties :

- la première est issue d'un fichier `routages.prologue`, contenant tous les cas particuliers, repris sans modification d'aucune sorte ;
- la deuxième est la sortie du script `generer-routages`.

Le script `mkroutages` concatène ces deux parties, compare le résultat à l'existant, et installe la nouvelle version si elle diffère. L'ancienne version est conservée avec le suffixe `.old`. L'utilitaire `makemap` est alors appelé pour reconstruire le fichier `.db` correspondant et rendre les données accessibles à `sendmail`.

Pour être installé :

- vous devez avoir au préalable modifié et installé le script `generer-routages` ;
- vous devez adapter `mkroutages` pour votre usage local ;
- vous devez copier `mkroutages` vers vos relais de messagerie ;
- et vous devez enfin activer la crontab ci-dessus sur chacun des relais de messagerie..

## 7.6 Script auxiliaire de maintenance de la base

L'application WebDNS est complétée par un script auxiliaire, lancé par `cron` sur le serveur de données, pour réaliser les opérations de maintenance et de sauvegarde de la base PostgreSQL. Ce script, `./expl/quotidien`, effectue une sauvegarde dans le répertoire `./dump`, ainsi qu'un « `VACUUM` » (spécifique PostgreSQL) sur la base.

De plus, il permet également de créer une copie de la base d'exploitation dans une base de développement, mais ceci n'est pas activé par défaut.

Après l'avoir modifié selon vos besoins, vous pouvez le lancer toutes les nuits par `cron`, de préférence avant minuit pour avoir des noms de fichiers de sauvegarde représentatifs du jour sauvegardé. Par exemple, voici un exemple de `crontab` utilisé (voir fichier `./expl/crontab.dns`) :

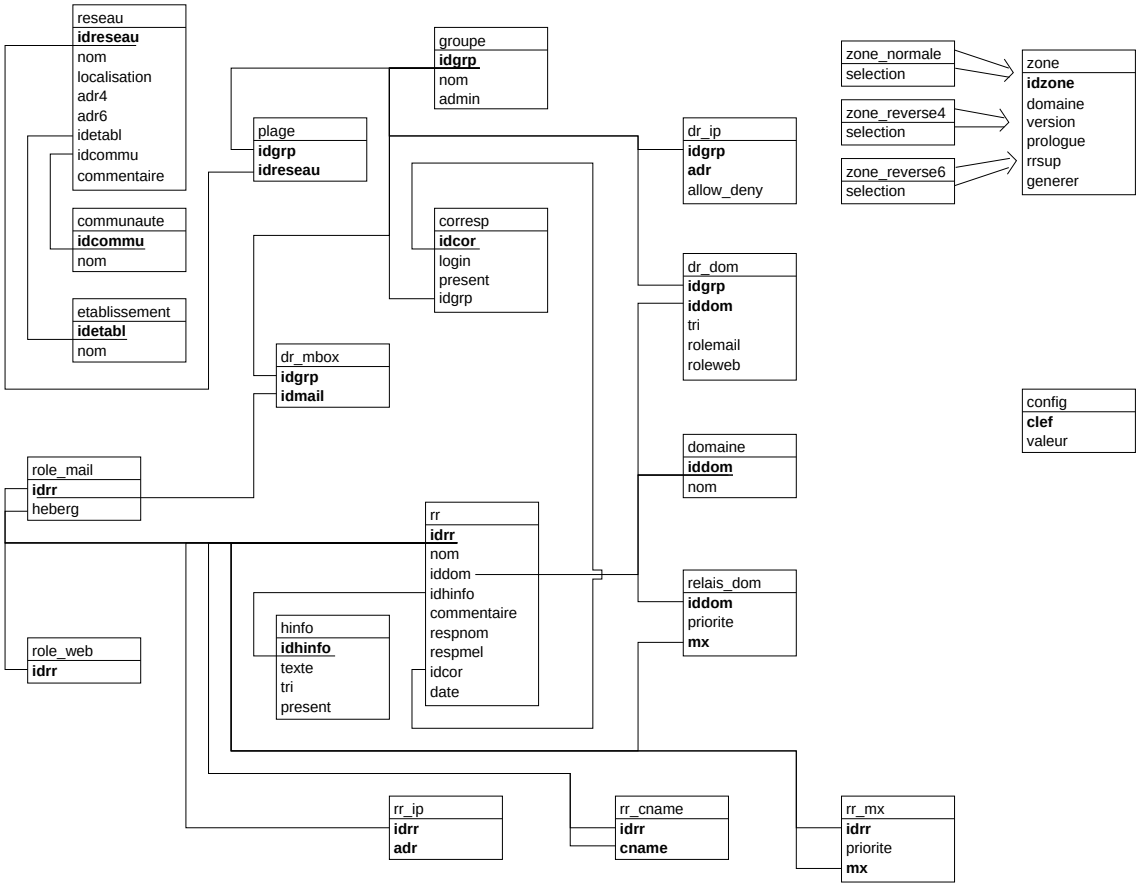
```
40 22 * * * $HOME/expl/quotidien
```

# 8 Conclusion

Si ça marche, n'oubliez pas d'envoyer une bouteille de champagne aux auteurs...

# A Modèle des données

***Base DNS – Modèle logique des données au 12/02/2004***



# B Paramétrage de WebDNS

L'application WebDNS permet de gérer et déléguer finement des droits à des correspondants réseau. Il importe donc de bien comprendre les enjeux du paramétrage afin de réussir son implantation.

Le lecteur intéressé pourra se référer avantageusement au modèle des données, fourni en annexe A (page 18).

## B.1 Les réseaux

Un réseau doit être compris comme un « domaine de broadcast »[9], autrement dit un réseau relie un ensemble de machines qui peuvent communiquer entre elles sans utiliser de routeur intermédiaire.

À chaque réseau sont associées deux **adresses** : un CIDR **IPv4** (de la forme « 130.79.201.128/25 », par exemple) et l'équivalent **IPv6** (de la forme « 2001:660:2402:1::/64 » par exemple). L'une des deux adresses peut bien évidemment être vide.

Les autres attributs d'un réseau sont :

- son **nom** (chaîne alphanumérique sans restriction)
- son **établissement** : si vous n'avez qu'un seul établissement (réseau d'établissement et non réseau métropolitain ou régional), vous pourrez remplacer la notion d'établissement par la notion de service, de laboratoire, de client, etc.
- sa « **communauté** » : cette notion nous permet, sur Osiris, d'identifier les réseaux d'enseignement, de recherche, d'administration, de backbone, d'interconnexion, etc. Vous pouvez l'utiliser de cette manière, ou ne pas considérer ce champ. Cet attribut n'a pas d'autre utilité, pour l'instant, que la documentation des réseaux.
- sa **localisation** géographique : texte libre, par exemple une adresse, un bâtiment, un étage, etc.
- un **commentaire** : texte libre.

La notion de réseau est utilisée, à l'heure actuelle, uniquement pour des raisons cosmétiques, afin de permettre à un correspondant de choisir dans une liste le réseau qu'il souhaite consulter. Toutefois, cette notion est appelée à évoluer avec la mise en place de nouvelles fonctionnalités dans les versions ultérieures de WebDNS. C'est pourquoi nous vous recommandons de bien renseigner ces informations[10].

## B.2 Les correspondants et les groupes

L'application WebDNS est conçue pour déléger la gestion du DNS à un ensemble de **correspondants réseau**. Le correspondant est donc la personne physique qui va réaliser les opérations d'ajout, de modification et de suppression des informations dans la base.

Peu d'informations sont associées à un correspondant dans la base, car la plupart sont inscrites dans l'application WebAuth. Les informations spécifiques à WebDNS sont :

- le **login** du correspondant, faisant ainsi la jonction avec l'application WebAuth ;
- un indicateur servant à savoir si un correspondant est **présent** ou non. Cet indicateur autorise le correspondant à se connecter à l'application. On met cet indicateur à 0 lorsque le correspondant est parti (départ, mutation, etc.), afin de le laisser inactif dans la base : en effet, il peut y avoir des informations à son nom, qui deviendraient orphelines si le compte était simplement détruit. Si plus aucune information ne fait référence au correspondant, le compte peut bien sûr être directement détruit.
- le **groupe** auquel appartient le correspondant. Tout correspondant appartient à un (et un seul) groupe.

C'est par l'intermédiaire des **groupes** que les droits sont attribués aux correspondants. Ces droits peuvent être :

[9] Évitez d'identifier votre classe B comme un seul réseau...
[10] Et c'est l'occasion de documenter vos réseaux, non ? ;-)

– le droit de déclarer des noms dans un domaine
– le droit de déclarer des adresses IP dans un intervalle
– le droit de consulter des réseaux
– le droit de déclarer des rôles de messagerie pour un domaine
– le droit d'administrer la base

Deux groupes différents peuvent avoir des droits qui se chevauchent. Par exemple, on peut imaginer un droit sur un réseau pour les correspondants d'une composante ou d'un laboratoire (formant un groupe), et des droits sur ce même réseau pour les personnes du CRI d'établissement (formant un autre groupe).

Les groupes décrits ici (appelés groupes WebDNS) ne doivent pas être confondus avec les groupes de l'application WebAuth : les groupes WebDNS permettent d'attribuer des droits spécifiques à l'application WebDNS, alors que les groupes WebAuth permettent à un serveur tel que Apache à délimiter l'accès à des portions d'une arborescence Web.

## B.3 Les domaines et les *resource-records*

Un domaine est un ensemble de *resource-records* (encore appelés RR).

Chaque RR porte un **nom** (sans point à l'intérieur), conforme à la RFC 1035, et fait référence au **domaine**. De plus, un RR :

– porte un type (encore appelé **hinfo**) paramétrable par l'administrateur de la base ;
– est géré par un **responsable** (avec un nom et une adresse électronique), ce qui peut permettre à un correspondant réseau de retrouver l'utilisateur principal d'un PC s'il renseigne cette information ;
– contient un **commentaire**, qui peut typiquement être une référence à une prise, à un équipement, à un local, etc. ;
– contient la référence du **dernier correspondant** ayant modifié le RR, ainsi que la **date**.

Il faut insister sur le fait qu'un nom de RR ne comporte pas de point. Ainsi, vous ne pouvez pas ajouter « www.labo » dans le domaine « domaine.fr », par exemple. Pour cela, il faut créer le domaine « labo.domaine.fr » et y rentrer le RR de nom « www » (ou alors gérer ceci comme une exception à l'aide du *prologue* de la zone, comme décrit ci-après).

À un RR sont rattachées différentes informations : une ou plusieurs **adresses IP** (v4 aussi bien que v6), un ou plusieurs **aliases**, des **rôles de messagerie** ou des **MX**.

## B.4 Droits sur les adresses IP et les noms

En premier lieu, un groupe a accès à un ou plusieurs domaines (via la table `dr_dom`). À chaque domaine est associé une classe de tri, de façon que le groupe puisse voir en premier les domaines qui le concernent. Si un seul domaine est défini pour un groupe, ses membres ne verront qu'un champ fixe au lieu d'un menu déroulant.

En second lieu, un groupe a accès à des plages d'adresses IP (IPv4 ou IPv6, via la table `dr_ip`). Une plage d'adresses IP est définie comme une suite de droits de type « `allow` » ou « `deny` » sur des préfixes IP. Ainsi, pour permettre aux membres d'un groupe de déclarer des machines dans toute une plage d'adresses, sauf l'adresse de *broadcast* et l'adresse du routeur (définie par exemple comme la dernière adresse du réseau), on déclarera les deux plages :

– *allow* `192.168.1.0/24`
– *deny* `192.168.1.254/31`

Un correspondant peut donc déclarer des machines si les deux conditions sont réunies :

– l'adresse fait partie des plages autorisées
– le domaine fait partie des domaines autorisés

Dans le cas d'une machine déclarée avec plusieurs adresses (comme un routeur, par exemple), un correspondant peut y accéder (ajouter ou supprimer une adresse, modifier un attribut, ajouter un alias, etc.) si et seulement si toutes les adresses IP sont dans les plages du correspondant.

## B.5 Les zones

Les « zones » ne doivent pas être confondues avec les « domaines » : si les « domaines » regroupent des RR dans la base, les « zones » quant à elles contiennent les renseignements nécessaires pour générer les fichiers de zone sur votre serveur DNS.

Les zones comprennent entre autres :

- le **nom de la zone** (« `u-strasbg.fr` », ou « `79.130.in-addr.arpa` » par exemple) ;
- le **critère** servant, lors de la génération, à sélectionner les informations dans la base :
  - pour une zone « inverse » (dans `in-addr.arpa` ou `ip6.arpa`), il s'agit d'un préfixe de réseau (par exemple `130.79.201.128/25`) ;
  - pour une zone « normale », il s'agit du domaine associé à chaque nom (`u-strasbg.fr` pour sélectionner les RR devant figurer dans la zone `u-strasbg.fr`)
- le **numéro de version** qui devra être inséré dans le SOA. Ce numéro de version est toujours de la forme AAAAMMJJnn, où AAAA est l'année, MM le mois, JJ le jour et nn le numéro de modification dans la journée (limité à 99, donc) ;
- le **prologue**, ensemble de commentaires et de RR, qui figurera avant les RR générés dans la zone. En particulier, le prologue contient le RR de type SOA, ainsi que les RR de type NS ou MX associés au domaine lui-même ;
- des **RR supplémentaires** à insérer pour chaque RR de type A ou AAAA. Il s'agit d'une chaîne de caractères (sur plusieurs lignes éventuellement si vous avez plusieurs RR à ajouter) dans laquelle toutes les occurrences de la chaîne « `%NOM%` » sont substituées par le nom du RR de type A ou AAAA. Pour l'utilisation de ce champ, voir B.6.1 (page 22) ;
- et enfin, un **indicateur** servant à indiquer si la zone doit être regénérée sur le serveur DNS, c'est à dire si au moins un RR de la zone a été modifié.

Le script de génération de zone (`generer-zone`, voir 7.4, page 15) calcule un nouveau numéro de version à partir de celui qui figure dans la base, puis il extrait le prologue, y recherche la chaîne « `%VERSION%` » et la substitue par le nouveau numéro de version calculé précédemment, et enfin génère les RR associés à la zone en les sélectionnant à partir du critère, et en y ajoutant éventuellement les RR supplémentaires associés à la zone.

Le prologue ne contient habituellement que les informations liées à la zone elle-même, soit les RR de type SOA, NS et MX associés au domaine. Dans la pratique, le prologue peut également contenir tous les cas particuliers[11] qui ne peuvent être pris en compte dans le modèle.

## B.6 MX et rôles de messagerie

Le DNS est souvent utilisé pour implanter une politique de messagerie, par le biais des RR de type MX.

Alors que les autres parties du modèle sont assez génériques, la gestion des informations de politique de messagerie n'a pas fait l'objet d'une étude de généricité aussi poussée. L'expérience d'autres sites permettra sans doute d'adapter le modèle décrit ci-dessous.

Les auteurs ont conçu la gestion de la messagerie en supposant un routage centralisé par domaine (avec par exemple un filtrage sur le port SMTP en entrée de site), bien que cette restriction puisse souffrir des exceptions.

[11] Certains diront les « scories de l'histoire d'un site ».

### B.6.1 Utilisation des RR supplémentaires

Une première méthode de gestion des MX consiste à associer un ou plusieurs MX standards à toute adresse IP (v4 ou v6).

Cette méthode était utilisée jusqu'en avril 2004 sur Osiris. Elle a prouvé ses limites, notamment parce qu'elle publie toute adresse de machine comme adresse utilisable.

Néanmoins, si vous souhaitez l'utiliser, il suffit d'activer les RR supplémentaires pour la ou les zones correspondantes. Par exemple, sur Osiris, nous utilisions :

```
%NOM% IN MX 10 ns1.u-strasbg.fr.
%NOM% IN MX 10 ns2.u-strasbg.fr.
```

Ainsi, après tout RR de type A ou AAAA, le script de génération de zone (`generer-zone`, voir 7.4, page 15) ajoute le texte ci-dessus en remplaçant la chaîne « `%NOM%` par le nom du RR de type A ou AAAA.

Afin de permettre de créer des RR de type MX qui ne sont pas associés à des adresses IP (comme par exemple pour des adresses de messagerie virtuelles), l'application WebDNS permet de renseigner la table des MX. Celle-ci associe à un RR, c'est-à-dire à un nom :

– une **priorité** ;
– un **autre RR**, qui sera le RR pointé par le MX.

Il est bien sûr possible de déclarer plusieurs MX pour un nom donné.

Cette possibilité est restreinte aux administrateurs de l'application. Elle permet de gérer des cas particuliers à la règle « une adresse, un MX », comme notamment les adresses virtuelles de messagerie.

### B.6.2 Utilisation des rôles de messagerie

La deuxième méthode de gestion des MX s'appelle les « rôles de messagerie ». Elle est nettement plus souple, car elle permet aux correspondant autorisés de gérer eux-mêmes, de manière contrôlée, les adresses de messagerie.

L'utilisation des rôles de messagerie passe par :

– l'affectation du droit correspondant à la gestion des domaines de messagerie au groupe, pour chacun des domaines autorisés (menu de modification des caractéristiques d'un groupe dans l'application, table `dr_dom`) ;
– l'affectation d'un ou plusieurs relais pour le domaine (menu de modification des relais de messagerie dans l'applcation, table `relais_dom`) ;

Fonctionnellement, un correspondant dont le groupe a le droit de gérer les rôles de messagerie pour un domaine particulier peut associer à une **adresse de messagerie** (qui peut correspondre ou non à une adresse IP existante) une machine réalisant l'**hébergement** des boîtes aux lettres pour cette adresse.

Le script de génération de zone (`generer-zone`, voir 7.4, page 15) générera, pour chaque rôle de messagerie déclaré par un correspondant, un MX par relais enregistré pour le domaine. Ainsi, les correspondants autorisés peuvent définir eux-mêmes les adresses de messagerie qu'ils gèrent, tout en respectant le filtrage sur le port SMTP en entrée.

Bien sûr, pour que ceci soit pleinement opérationnel, il faut que le ou les relais de messagerie actualisent leur table de routage de messagerie. En utilisant le script `generer-routages` (voir 7.5, page 16), vous pouvez créer dynamiquement une table de routage pour `sendmail` telle que l'attend le kit Jussieu par exemple.

## B.7 Tables non utilisées

Quelques unes des tables existant dans la base sont prévues pour un usage futur :

- la table `role_web` ainsi que l'attribut **roleweb** de la table `dr_dom` sont prévus pour permettre aux correspondants de déclarer les serveurs Web autorisés dans leur domaine. Au delà de l'identification de la responsabilité éditoriale, ceci permettra dans le futur de générer des filtres sur les routeurs ;
- la table `dr_mbox` est prévue pour une gestion plus intégrée de l'hébergement de boîtes aux lettres sur un serveur de messagerie multi-domaines. L'idée est d'associer un groupe à une adresse de messagerie, afin de lui déléguer la gestion des boîtes aux lettres correspondantes.

## B.8 Procédures

Une bonne connaissance du modèle des données permet de déduire toutes les procédures.

### B.8.1 Ajouter ou supprimer un correspondant

Pour ajouter un correspondant, il faut au préalable que le groupe existe.

Si ce n'est pas le cas, il faut utiliser :

- d'abord le menu de *modification des groupes*, pour créer le groupe ;
- ensuite le menu de *modification des caractéristiques d'un groupe* pour lui affecter des droits sur les réseaux consultables, sur les domaines et les plages autorisés.

Il ne reste plus ensuite qu'à ajouter le correspondant au moyen du menu de *gestion des correspondants*. Ceci a pour effet d'ajouter le correspondant à la base d'authentification (WebAuth) pour l'accès au serveur Web, ainsi que dans la base WebDNS pour l'affectation à un groupe.

Pour supprimer un correspondant, il faut utiliser le menu de *gestion des correspondants*. La suppression échouera sur une contrainte d'intégrité de la base si le correspondant a modifié des RR. Dans ce cas, il ne faut pas supprimer le correspondant, mais le rendre « absent » (i.e. non présent) par le menu de *modification d'un correspondant*.

### B.8.2 Ajouter un réseau

Pour ajouter ou supprimer un réseau, il faut passer par le menu de *modification des réseaux*. Une fois le réseau créé, il faut le rendre accessible (en consultation et par les plages d'adresses) par tous les groupes concernés, par l'intermédiaire du menu de *modification des caractéristiques d'un groupe*.

Éventuellement, il faut créer une zone inverse pour le réseau sur le serveur DNS, et créer la zone avec le menu de *modification des zones reverse IPv4* (ou IPv6).

### B.8.3 Ajouter un domaine

L'ajout d'un domaine nécessite :

- d'ajouter le domaine par le menu de *modification des domaines* ;
- d'ajouter les droits sur le domaine à tous les groupes concernés, par l'intermédiaire du menu de *modification des caractéristique des groupes* ;
- d'ajouter la zone correspondante sur le serveur DNS ;
- d'ajouter la zone dans la base par le menu de *modification des zones*.

La suppression d'un domaine nécessite les opérations inverses. En cas de violation d'une contrainte d'intégrité, la modification correspondante sera annulée.

# C Pages à trous

| Fichier | Trou | Signification |
|---|---|---|
| (tous) | %HOMEURL% | adresse relative de la page d'accueil par rapport à la racine du serveur Web |
| accueil.html | %ADMIN% | lien permettant d'aller vers le menu d'administration. Seul et unique moyen de se rendre dans ce menu. |
| | %DOCDNS% | adresse d'une page publique (hors de l'application) décrivant la documentation de votre service DNS. |
| | %INTERVALLE% | intervalle entre deux générations de zones sur le serveur DNS. |
| admgenliste.html | %ZONES% | liste de zones permettant les sélections multiples |
| admgenset.html | %DOCDNS% | adresse d'une page publique (hors de l'application) décrivant la documentation de votre service DNS. |
| | %INTERVALLE% | intervalle entre deux générations de zones sur le serveur DNS. |
| admgrpconfirm.html | %GROUPE% | nom du groupe à modifier |
| | %HIDDEN% | liste de paramètres cachés pour propager les informations sélectionnées par l'utilisateur. |
| | %MESSAGE% | incohérences trouvées dans la demande de l'utilisateur |
| admgrpliste.html | %GROUPE% | nom du groupe en cours de modification |
| | %LISTECOR% | liste des correspondants inscrits dans le groupe |
| | %LISTEDOMAINES% | tableau de domaines modifiables |
| | %LISTEDROITS% | tableau de droits allow/deny modifiables |
| | %LISTERESEAUX% | tableau de réseaux sélectionnables |
| admgrpmodif.html | %GROUPE% | nom du groupe modifié |
| | %TABDOMAINES% | liste des domaines saisis |
| | %TABRESEAUX% | liste des réseaux sélectionnés |
| | %TITRECIDRHORSRESEAU% | titre inscrit s'il y a des plages hors des réseaux sélectionnés |
| | %TABCIDRHORSRESEAU% | liste des plages hors des réseaux sélectionnés |
| admgrpsel.html | %MENUGROUPE% | menu de sélection du groupe à modifier |
| admmxedit.html | %DOMAINE% | domaine sélectionné |
| | %NOM% | nom du MX sélectionné |
| | %TABLEAU% | tableau des MX trouvés, éditable |
| admmxmodif.html | %DOMAINE% | domaine sélectionné |
| | %NOM% | nom sélectionné |
| | %TABLEAU% | liste des MX modifiés |
| admmxsel.html | %DOMAINE% | menu des domaines autorisés |
| admparliste.html | %TAB% | tableau éditable des paramètres de l'application |
| admrefliste.html | %TABLEAU% | tableau des paramètres éditables |

| Fichier | Trou | Signification |
|---|---|---|
| | %TITREPAGE% | titre de la page contenant le type d'objet en cours de modification |
| | %TYPE% | type d'objet en cours de modification |
| admreledit.html | %DOMAINE% | domaine sélectionné |
| | %TABLEAU% | tableau éditable des relais de messagerie pour ce domaine |
| admrelmodif.html | %DOMAINE% | domaine sélectionné |
| | %TABLEAU% | relais de messagerie enregistrés pour ce domaine |
| admrelsel.html | %DOMAINE% | menu de sélection du domaine |
| admutiajoutinit.html | voir WebAuth | |
| admutichoix.html | voir WebAuth, page utichoix.html | |
| admutiliste.html | voir WebAuth, page utiliste.html | |
| admutimenu.html | %URL% | lien vers le script de gestion des utilisateurs |
| admutimodif.html | voir WebAuth, page utimodif.html | |
| admutiok.html | voir WebAuth, page actionok.html | |
| admutipasswd.html | voir WebAuth, page utipasswd.html | |
| admutisel.html | voir WebAuth, page utisel.html | |
| admutisuppr.html | voir WebAuth, page utisuppr.html | |
| admvalide.html | %TYPEENCLAIR% | type de l'objet modifié |
| | %URL% | lien vers le script de modification du type d'objet modifié |
| ajout.html | %DOMAINE% | menu de présentation des domaines |
| | %DOMAINEREF% | menu de présentation des domaines, pour l'ajout d'alias |
| | %MENUHINFO% | menu des types de machines |
| consulter.html | %CORRESP% | tableau contenant l'identité du correspondant |
| | %PLAGES% | liste sélectionnable des réseaux autorisés |
| consultmx.html | %LISTEDOMAINES% | liste sélectionnable des domaines |
| consultnet.html | %LISTECOMMU% | liste sélectionnable des communautés |
| | %LISTEETABL% | liste sélectionnable des établissements |
| corresp.html | %CRITERE% | précédent critère de recherche de machine |
| | %RESULTAT% | résultat d'une précédente recherche d'une machine |
| droits.html | %CORRESP% | tableau contenant l'identité du correspondant |
| | %TABRESEAUX% | liste des réseaux autorisés en consultation |
| | %TABDOMAINES% | liste des domaines autorisés |
| | %TITRECIDRHORSRESEAU% | le cas échéant, titre de la section des plages hors des réseaux enregistrés |
| | %TABCIDRHORSRESEAU% | le cas échéant, liste des plages hors des réseaux enregistrés |
| editmodif-infos.html | %NOM% | nom du RR en cours de modification |
| | %DOMAINE% | domaine du RR en cours de modification |
| | %MENUHINFO% | menu des types de machines |

| Fichier | Trou | Signification |
|---|---|---|
| | %COMMENTAIRE% | champ de saisie du commentaire |
| | %RESPNOM% | dchamp de saisie du nom du responsable de la machine |
| | %RESPMEL% | champ de saisie de l'adresse électronique du responsable de la machine |
| erreur.html | %MESSAGE% | message d'erreur |
| liste.html et liste.tex | %ORIENTATION% | `portrait` ou `landscape` (pour liste.tex uniquement) |
| | %NBMACHINES% | nombre de machines trouvées |
| | %S% | « s » si le nombre de machine est supérieur à 1 |
| | %DATE% | date de l'extraction |
| | %TABLEAU% | liste des machines trouvées |
| listecorresp.html | %TITREPAGE% | titre de la page |
| | %LISTECOR% | liste des correspondants trouvés |
| listedes.html et liste.tex | %ORIENTATION% | `portrait` ou `landscape` (pour liste.tex uniquement) |
| | %TITRE% | type d'objet dont on a la liste |
| | %DATE% | date de l'extraction |
| | %TXT% | texte d'explication sur les paramètres de l'extraction |
| | %TABLEAU% | liste extraite |
| mail.html | %DOMAINE% | menu de sélection d'un domaine |
| mailheberg-edit.html | %NOM% | nom de l'adresse de messagerie en cours d'édition |
| | %DOMAINE% | domaine de l'adresse de messagerie en cours d'édition |
| | %NOMH% | nom éditable de l'hébergeur trouvé |
| | %DOMAINEH% | menu pour modifier l'hébergeur trouvé |
| mailheberg-liste.html | %DOMAINE% | domaine dont on demande la liste des adresses de messagerie |
| | %TABLEAU% | liste des adresses de messagerie, avec les hébergeurs |
| mailmodif.html | %NOM% | nom (complet) de l'adresse de messagerie modifiée |
| | %ACTION% | type d'action (ajout, modification, suppression) effectuée |
| modif.html | %DOMAINE% | menu de sélection de domaine |
| statcor.html | %NBRRCOR% | tableau contenant le nombre de RR modifiés par correspondant |
| statetab.html | %NBMACHETABL% | nombre de machines et d'adresses par établissement |
| suppr.html | %DOMAINE% | menu de sélection de domaine |
| traiteajout-alias.html | %DOCDNS% | adresse d'une page publique (hors de l'application) décrivant la documentation de votre service DNS. |
| | %INTERVALLE% | intervalle entre deux générations de zones sur le serveur DNS. |
| | %NOM% | nom de l'alias |
| | %DOMAINE% | domaine de l'alias |
| | %NOMREF% | nom de la machine |

| Fichier | Trou | Signification |
|---|---|---|
| | %DOMAINEREF% | domaine de la machine |
| traiteajout-existe.html | %NOM% | nom de la machine existante |
| | %DOMAINE% | nom du domaine de la machine existante |
| | %LISTEADR% | liste des adresses déjà affectées à la machine |
| | %HINFO% | type de la machine existante |
| | %COMMENTAIRE% | commentaire sur la machine existante |
| | %RESPNOM% | nom du responsable de la machine existante |
| | %RESPMEL% | adresse électronique du responsable de la machine existante |
| | %ADR% | nouvelle adresse à ajouter |
| traiteajout-machine.html | %DOCDNS% | adresse d'une page publique (hors de l'application) décrivant la documentation de votre service DNS. |
| | %INTERVALLE% | intervalle entre deux générations de zones sur le serveur DNS. |
| | %NOM% | nom de la machine ajoutée |
| | %DOMAINE% | domaine de la machine ajoutée |
| | %ADR% | adresse de la machine ajoutée |
| | %HINFO% | type de la machine ajouée |
| | %COMMENTAIRE% | commentaire sur la machine ajoutée |
| | %RESPNOM% | nom du responsable de la machine ajoutée |
| | %RESPMEL% | adresse électronique du responsable de la machine ajoutée |
| traitemodif-infos.html | %DOCDNS% | adresse d'une page publique (hors de l'application) décrivant la documentation de votre service DNS. |
| | %INTERVALLE% | intervalle entre deux générations de zones sur le serveur DNS. |
| | %NOM% | nom de la machine modifiée |
| | %DOMAINE% | domaine de la machine modifiée |
| | %HINFO% | type de la machine modifiée |
| | %COMMENTAIRE% | commentaire sur la machine modifiée |
| | %RESPNOM% | nom du responsable de la machine modifiée |
| | %RESPMEL% | adresse électronique du responsable de la machine modifiée |
| traitesuppr-alias.html | %NOM% | nom de l'alias à supprimer |
| | %DOMAINE% | domaine de l'alias à supprimer |
| | %NOMREF% | nom de la machine |
| | %DOMAINEREF% | domaine de la machine |
| traitesuppr-ip-objet.html | %ADR% | adresse dont la suppression est demandée |
| | %NOM% | nom correspondant à l'adresse |
| | %DOMAINE% | domaine correspondant à l'adresse |

| Fichier | Trou | Signification |
|---|---|---|
| | %LISTEADR% | adresses trouvées pour cette machine |
| | %HINFO% | type de la machine |
| | %COMMENTAIRE% | commentaire sur la machine |
| | %RESPNOM% | nom du responsable |
| | %RESPMEL% | adresse électronique du responsable |
| | %ALIASES% | aliases éventuels sur la machine |
| traitesuppr-ip-uneip.html | %ADR% | adresse dont la suppression est demandée |
| | %NOM% | nom correspondant à l'adresse |
| | %DOMAINE% | domaine correspondant à l'adresse |
| | %LISTEADR% | adresses trouvées pour cette machine |
| | %HINFO% | type de la machine |
| | %COMMENTAIRE% | commentaire sur la machine |
| | %RESPNOM% | nom du responsable |
| | %RESPMEL% | adresse électronique du responsable |
| | %ALIASES% | aliases éventuels sur la machine |
| traitesuppr-nom.html | %NOM% | nom dont la suppression est demandée |
| | %DOMAINE% | domaine correspondant |
| | %LISTEADR% | adresses trouvées pour ce nom |
| | %HINFO% | type de la machine |
| | %COMMENTAIRE% | commentaire sur la machine |
| | %RESPNOM% | nom du responsable |
| | %RESPMEL% | adresse électronique du responsable |
| | %ALIASES% | aliases éventuels sur la machine |
| traitesuppr-ok.html | %DOCDNS% | adresse d'une page publique (hors de l'application) décrivant la documentation de votre service DNS. |
| | %INTERVALLE% | intervalle entre deux générations de zones sur le serveur DNS. |
| | %OBJET% | type d'objet (adresse IP, nom) supprimé |