# Application WebDNS
# Installation et configuration

**Pierre David, Jean Benoit**

Version 1.3 – 13 avril 2005

La composition de ce document a été effectuée par un ordinateur avec le système d'exploitation Unix (plus spécifiquement FreeBSD, une version libre), en utilisant le logiciel de composition TEX (logiciel libre). Les figures ont été dessinées sous X-Window (logiciel libre) avec le logiciel `xfig` (logiciel libre) et intégrées directement dans le document final.

La dernière version de ce document est accessible à l'adresse :

ftp://ftp.u-strasbg.fr/pub/crc/webdns/

Version 1.3, Avril 2005

# Table des matières

# Chapitre 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.

Par la suite, de nouvelles fonctionnalités sont apparues : gestion des rôles de messagerie, permettant une gestion fine et décentralisée du routage de messagerie sur un campus, et plus récemment intégration des informations liées au protocole DHCP.

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 ouverte 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.

La liste de diffusion `webdns@u-strasbg.fr` est ouverte à tous les utilisateurs de l'application WebDNS. Pour s'y abonner, il suffit d'envoyer un message à `sympa@u-strasbg.fr` avec « `SUBSCRIBE webdns` » dans le corps du message. Les archives sont consultables sur http://listes.u-strasbg.fr/.

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

# Chapitre 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.

Plus précisément, l'application WebDNS permet de gérer des informations associées à un parc de machines, comme le nom, l'adresse IP, l'adresse MAC (ou adresse Ethernet), mais également le type de système d'exploitation, la personne responsable ou un commentaire à usage général.

Le système de droits fins permet de déléguer l'administration d'un sous-réseau (ou une partie de sous-réseau, à l'adresse IP près si l'administrateur le souhaite) et d'un domaine à une ou plusieurs personnes, réunies dans un ou plusieurs groupes.

Certaines des informations sont rendues publiques via le DNS, comme l'association entre un nom et une adresse IP, mais également les adresses DNS reconnues comme des adresses de messagerie valides.

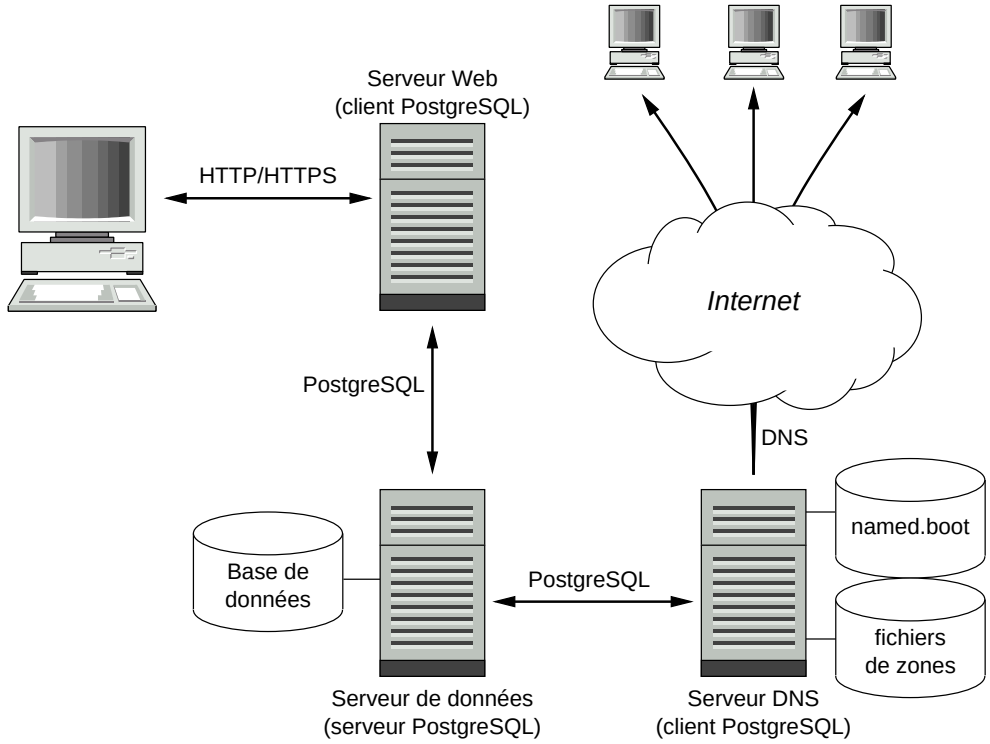
D'autres informations, comme l'association entre adresses MAC et adresses IP peuvent être utilisées par un serveur DHCP, pour réaliser une l'allocation statique. Des mécanismes permettent également d'associer des profils particuliers (comme les options nécessaires au *boot* d'une station sans disque ou d'un terminal X par exemple) à des machines, voire d'allouer des intervalles d'allocation dynamiques pour accueillir des portables.

D'autres informations, enfin, sont destinées à un usage interne, comme par exemple le nom et l'adresse électronique de la personne responsable de la machine.

Au delà de ces applications particulières, 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

L'application WebDNS est une application multitiers. Son principe de fonctionnement est résumé sur la figure ci-après, qui illustre plus particulièrement l'aspect de la génération de zones DNS :




Dans cette figure, l'utilisateur accède à ses données par l'intermédiaire de son navigateur Web, via le protocole 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.

Le même schéma s'applique également pour la génération de la configuration DHCP sur un serveur central (où le serveur DHCP, typiquement le serveur d'ISC, est client PostgreSQL du serveur de données), ou pour la génération de la table de routage de messagerie (où le serveur de messagerie est également client PostgreSQL du serveur de données).

## 2.3 Fonctionnalités

### 2.3.1 Génération de zones DNS

L'intérêt premier de l'application WebDNS est de faciliter la génération de zones DNS, toujours cohérentes (plus d'incompatibilités entre zone normale et zone inverse, numéro de SOA toujours à jour, etc.).

Le passage par une application Web, avec les mécanismes de verrouillage associés à un moteur de bases de données relationnel sérieux, permet à plusieurs personnes d'éditer la configuration simultanément.

L'application permet d'associer des informations complémentaires (nom et adresse électronique du responsable de la machine, commentaire) pour faciliter la gestion du parc.

### 2.3.2 Routage de messagerie

La configuration de l'application permet également de gérer les aspects liés au routage de la messagerie :

- soit en affectant, pour une zone donnée, des champs DNS (resource records) supplémentaires indiquant les MX associés à chaque machine ;
- soit en laissant aux correspondants réseaux, pour une zone donnée, la possibilité de spécifier les machines aptes à recevoir du courrier ; ceci suppose la configuration des relais de messagerie (MX) pour une zonne donnée ;

### 2.3.3 Utilisation de DHCP

Les fonctionnalités offertes par WebDNS en matière de gestion DHCP sont :

- l'association statique d'une adresse MAC à un nom (et une adresse IP) ; cette association peut être complétée par un « profil DHCP », c'est à dire un ensemble d'options de configuration du serveur DHCP communes à plusieurs machines (comme par exemple l'adresse du serveur de *boot* d'un PC sans disque) ;
- la déclaration d'intervalles d'adresses IP réservés pour l'allocation dynamique ; il est possible de déclarer des noms pour les adresses IP de l'intervalle (ex: `dhcp01`, `dhcp02`, etc.), mais pas d'adresse MAC : l'allocation dynamique est en effet incompatible avec l'allocation statique.

Ces fonctionnalités sont offertes réseau par réseau (dans l'application, mais également sur les routeurs concernés) et groupe de correspondant par groupe de correspondant.

## 2.4 Authentification

L'authentification des utilisateurs est réalisée par le serveur Web. La base des utilisateurs, externe à l'application WebDNS, repose sur le logiciel WebAuth (voir 4.1.1, page 13).

# Chapitre 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 |
| `upgrade/` | scripts de migration de la base... |
| `upgrade/12-13/` | ... de la version 1.2 vers la version 1.3 |
| `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 |
| `www/lib/util/` | utilitaires non liés au Web, mais placés ici pour profiter du Makefile |

# Chapitre 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[1] « 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.

### 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.

[1] Également développée par les mêmes auteurs.

### 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 43)
– le serveur DHCP.

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.

# Chapitre 5

# Personnalisation des pages HTML et LaTeX

Voir WebAuth.

# Chapitre 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 37) ainsi que l'annexe B (voir page 39) 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[1].

## 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[2] 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` ».

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

Le groupe choisi devra être spécifié dans la configuration Apache d'accès à l'application (voir 7.2, page 26), ainsi que dans l'application elle-même (voir plus bas, 6.4.2, page 20) 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 :

- 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 | dhcp          | table | pda
 public | dhcpprofil    | table | pda
 public | dhcprange     | table | pda
 public | domaine       | table | pda
 public | dr_dhcpprofil | table | pda
 public | dr_dom        | table | pda
 public | dr_ip         | table | pda
 public | dr_mbox       | table | pda
 public | dr_reseau     | table | pda
 public | etablissement | table | pda
 public | groupe        | table | pda
 public | hinfo         | 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
(27 rows)
```

```
dns=# \q
```

## 6.4 Chargement initial des données

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

Les fichiers de configuration fournis en exemple décrivent un réseau fictif. Le premier objectif est de fournir un exemple complet et représentatif. Le deuxième objectif est de vous permettre de tester rapidement l'application WebDNS sur des données imaginaires, avant de procéder au chargement de vos données.

### 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`, `dr_reseau`, `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 ne sont pas indispensables pour la reprise d'un existant, et n'ont donc pas été

intégrées dans les scripts de chargement initial.

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 `group.txt`, 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
  lma    marcel
  ```

  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 `subnet.txt` contenant des entrées de la forme :

  ```
  nom=LMA
  subnet=172.16.11.0
  netmask=255.255.255.0
  gateway=172.16.11.254
  communaute=Recherche
  etablissement=UM
  localisation=Campus 1 - Batiment bidule
  groupes=lma
  ```

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[3]. Si vous devez introduire un réseau IPv6 existant, faites-le après le chargement initial, avec l'interface Web.

– les droits sur les plages d'adresses IP. Pour tout réseau défini dans le fichier `subnet.txt`, l'accès est donné aux membres du groupe à l'ensemble des adresses du réseau, en retirant les droits sur l'adresse de *broadcast* et sur l'adresse du routeur par défaut si elle est indiquée.
  Certains groupes doivent avoir accès à tous les réseaux, comme par exemple les membres d'un service gérant l'ensemble du réseau. Il n'est pas conseillé d'indiquer ces groupes dans tous les réseaux listés dans `subnet.txt`, car sinon les droits seraient retirés sur les adresses particulières (*broadcast* et routeur par défaut) ; il vaut mieux introduire, après le chargement initial, des droits d'accès agrégés pour l'ensemble des réseaux gérés. Par exemple, le réseau « Osiris » étant constitué d'une classe B, le groupe des administrateurs n'est pas listé dans les réseaux individuellement décrits dans `subnet.txt`, mais le droit « allow 130.79/16 » a été ajouté a posteriori grâce au menu de *modification des caractéristiques d'un groupe*.

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.

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

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

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 43).

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 41). 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 | UM
       2 | ESIATF
       3 | INCONNU
(4 rows)

dns=# SELECT COUNT(*) FROM rr ;        -- compter le nombre de noms enregistrés
 count
-------
    36
(1 row)

dns=# SELECT COUNT(*) FROM rr_ip ;     -- compter le nombre d'adresses IP
 count
-------
    39
(1 row)

dns=# \q
```

Essayez quelques-unes des tables de l'application (voir annexe A, page 37). Si les valeurs sont correctes, vous avez terminé la phase délicate de l'installation, vous pouvez maintenant passer à la suite.

# Chapitre 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 E, page 51). 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 » |
| `DEFUSER` | utilisateur par défaut dans les scripts auxiliaires de modification de la base (ajout d'adresse IP, d'adresse MAC, etc.) |
| `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. |
| `VERSION` | Numéro de version de l'application. Normalement pas à modifier. |

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"

#
# Pour effectuer en une seule opération
# - l'accès via l'url /applis/dns, qui redirige en réalité vers un script
# - les redirections vers HTTPS
#
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
```

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 ;

## 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.

En particulier, pensez à vérifier et modifier les droits de votre groupe, pour avoir accès à tous les réseaux que vous êtes susceptible de gérer, par l'intermédiaire du menu de *modification des caractéristiques d'un groupe*.

## 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 14) ;
- 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[1] modifications par jour), avec une entrée de la forme :

```
#
# 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 43), 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*]

[1] 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.

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[2].

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 14) ;
– le mot de passe d'accès à la base.

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

### 7.5.2 Script `mkroutages`

Le script `mkroutages` est conçu pour être lancé par `cron`, par exemple toutes les 5 minutes 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 Génération de la configuration DHCP

L'application WebDNS gère les associations entre adresses IP et adresses MAC, ainsi que les plages d'adresses réservées pour l'allocation dynamique. Vous pouvez donc facilement générer la configuration d'un serveur DHCP.

De plus, grâce au mécanisme standard du « relayage DHCP » sur les routeurs, vous pouvez offrir un service DHCP centralisé sur un campus.

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

### 7.6.1 Configuration du serveur DHCP

L'exemple de configuration ci-dessous repose sur l'utilisation du serveur DHCP de l'ISC[3].

```
log-facility local2 ;    # logs distincts des autres démons
authoritative ;
ddns-update-style none ;

lease-file-name "/local/dhcpd/db/leases" ;

option domain-name-servers ns1.u-strasbg.fr;
option ntp-servers ntp.u-strasbg.fr ;
option nntp-server news.u-strasbg.fr ;

allow duplicates ;       # double boot: même mac, mais pas même client id
deny declines ;          # ignorer les refus des clients

ping-check false ;       # ne pas essayer de vérifier les adr dynamiques

max-lease-time 7200 ;    # 2 heures
default-lease-time 600 ; # 10 minutes

include "/local/dhcpd/gen.conf" ;    # tout ce qui est généré est là-dedans
```

Comme on peut le voir, toute la partie dynamique de la configuration est concentrée dans le fichier `gen.conf` inclus à la dernière ligne. Ce mécanisme d'inclusion permet de simplifier la génération.

### 7.6.2 Activation du relayage DHCP

Si vous souhaitez offrir le service DHCP à des sous-réseaux, vous devez activer le relayage DHCP sur vos routeurs. La suite vous donne quelques éléments pour

#### Activation du relayage DHCP sur Juniper

Pour activer le relayage sur un routeur Juniper (avec JunOS 6.4), vous devez saisir les lignes suivantes dans la configuration :

```
forwarding-options {
  helpers {
    bootp {
      description "Service DHCP pour les sous-reseaux d'Osiris" ;
      server 130.79.200.2 ;     /* adresse du serveur DHCP */
      interface {
        all {
          no-listen ;           /* par défaut, pas de DHCP sur les interfaces */
        }
        ge-1/2/0.5 ;            /* mais activé sur le Vlan 5 de l'interface */
        ge-2/1/2.546 ;          /* et sur le vlan 546 */
        ...
      }
    }
```

[3] http://www.isc.org/

```
    }
}
```

Bien entendu, vous devez vérifier également que les ports 67 et 68 ne sont pas filtrés.

#### Activation du relayage DHCP sur Cisco

Partie à rédiger.

#### Activation du relayage DHCP sur des PC

Si vous utilisez des PC en guise de routeur (cas d'un garde-barrière routé par exemple), vous pouvez utiliser le logiciel de relayage fourni avec le serveur DHCP de l'ISC.

### 7.6.3 Script `generer-dhcp`

Le script `generer-dhcp` a deux comportements différents suivant l'argument fourni :

- avec l'argument `test`, il teste si la configuration DHCP doit être regénérée, grâce à la table `dhcp` de la base DNS (qui contient une seule colonne et une seule ligne, valant soit 0 soit 1) ;
- avec l'argument `gen`, il génère la configuration DHCP (sans tester la table `dhcp`), puis remet cette table `dhcp` à 0.

Le fichier généré sur la sortie standard est prêt pour être utilisé comme partie de `dhcpd.conf` (fichier `gen.conf`, voir 7.6.1, page 30). Il contient en particulier :

- les déclarations des réseaux configurés pour DHCP, avec les paramètres associés (masque et routeur), et les intervalles dynamiques éventuellement déclarés ;
- les déclarations des machines individuelles ;
- de plus, si des profils DHCP sont définis dans la base, ceux-ci sont restitués dans un bloc « *group* » avec le texte défini pour ce profil. Les déclarations des machines individuelles avec ce profil sont ensuite listées dans ce bloc.

Le 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 14) ;
- le mot de passe d'accès à la base.

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

### 7.6.4 Script `mkdhcp`

Le script `mkdhcp` 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/mkdhcp
```

Le principe de fonctionnement du script est de générer un fichier `gen.conf` (voir section précédente), puis en testant la syntaxe du nouveau fichier de configuration. S'il n'y a aucun problème, le démon `dhcpd` est redémarré.

Pour être installé :

- vous devez avoir au préalable modifié et installé le script `generer-dhcp` ;
- vous devez adapter `mkdhcp` pour votre usage local ;
- vous devez copier `mkroutages` vers votre serveur DHCP ;
- et vous devez enfin activer la crontab ci-dessus sur votre serveur DHCP.

## 7.7 Utilitaires complémentaires

L'application WebDNS contient également quelques programmes conçus pour être utilisés hors contexte Web, ce qui permet d'automatiser certaines tâches, comme l'ajout de machine, d'adresse IP, d'adresse MAC, etc.

### 7.7.1 Localisation des utilitaires

Les programmes sont localisés dans le répertoire `./www/lib/util/`. Comme le reste de l'application, ils contiennent des paramètres qu'il serait fastidieux de changer fichier par fichier. Ils sont donc modifiés et installés, comme les autres scripts CGI ou les pages HTML à trous, vers l'arboresnce Web par `make` (voir 7.1, page 25).

Une fois localisés dans l'arborescence Web, ils peuvent être utilisés comme n'importe quel programme. Par exemple :

```
/local/services/www/applis/dns/lib/util/dnsaddhost toto.machin.fr 192.168.1.2
```

Vous pourrez avantageusement ajouter ce répertoire dans votre `PATH`, ou alors réaliser des liens symboliques, comme :

```
cd /local/sbin ; ln -s /local/services/www/applis/dns/lib/util/* .
```

### 7.7.2 Description des utilitaires

Les programmes sont les suivants :

- `dnsaddhost` *`fqdn ip`*
  Ajoute une machine avec l'adresse IP donnée, ou ajoute une adresse IP supplémentaire à une machine déjà existante.
  Exemple : `dnsaddhost toto.machin.fr 192.168.1.2`
- `dnsdelhost` *`fqdn`*
  Supprime la machine indiquée.
  Exemple : `dnsdelhost toto.machin.fr`
- `dnsaddalias` *`alias fqdn`*
  Ajoute un alias à une machine existante.
  Exemple : `dnsaddhost alias.machin.fr toto.machin.fr`
- `dnsdelip` *`ip`*
  Supprime l'adresse IP, et éventuellement la machine si elle n'a que cette adresse IP.
  Exemple : `dnsdelip 192.168.1.2`
- `dnsmodattr` *`fqdn clef val`* [ *`clef val`* ...]
  Modifie les attributs d'une machine. Les attributs (clefs) peuvent être :

  - `mac` : une adresse MAC
  - `dhcpprofil` : un nom de profil DHCP existant
  - `hinfo` : un nom de type de machine
  - `respnom` : le nom du responsable
  - `respmel` : l'adresse électronique du responsable
  - `commentaire` : le commentaire associé à la machine

  Chaque attribut peut être cité au plus une fois. Plusieurs attributs peuvent être modifiés au cours de la même opération.
  Exemple : `dnsdelip toto.machin.fr mac 01:02:03:04:05:06 dhcpprofil un-profil`
- `dnsreadprol` *`zone`*
  Lit le prologue associé à la zone et l'affiche sur la sortie standard.
  Exemple : `dnsreadprol machin.fr > $HOME/prologue`
- `dnswriteprol` *`zone fichier`*
  Écrit le prologue associé à la zone, à partir du fichier, dans la base.
  Exemple : `dnswriteprol machin.fr $HOME/prologue`

## 7.8 Scripts auxiliaires de maintenance de la base

L'application WebDNS est complétée par des scripts auxiliaires, lancés par `cron` sur le serveur de données, pour réaliser les opérations de maintenance et de sauvegarde de la base PostgreSQL

### 7.8.1 Script `quotidien`

Le premier 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
```

### 7.8.2 Script `sauvegarde`

À l'usage, il appert que les données contenues dans la base DNS revêtent un caractère très sensible et leur perte peut s'avérer catastrophique. Si vous êtes conscient de cet enjeu, vous trouverez dans le script `./expl/sauvegarde` le moyen d'effectuer une sauvegarde toutes les heures ; celle-ci peut par exemple être lancée par `cron` :

```
#
# Sauvegarde toutes les heures ouvrées du lundi au vendredi
# Sauvegarde une fois par jour le samedi et le dimanche
#
0 8-18 * * Mon-Fri $HOME/expl/sauvegarde
0 12   * * Sat,Sun $HOME/expl/sauvegarde
```

Il est vivement conseillé d'appliquer cette politique de sauvegarde...

# Chapitre 8

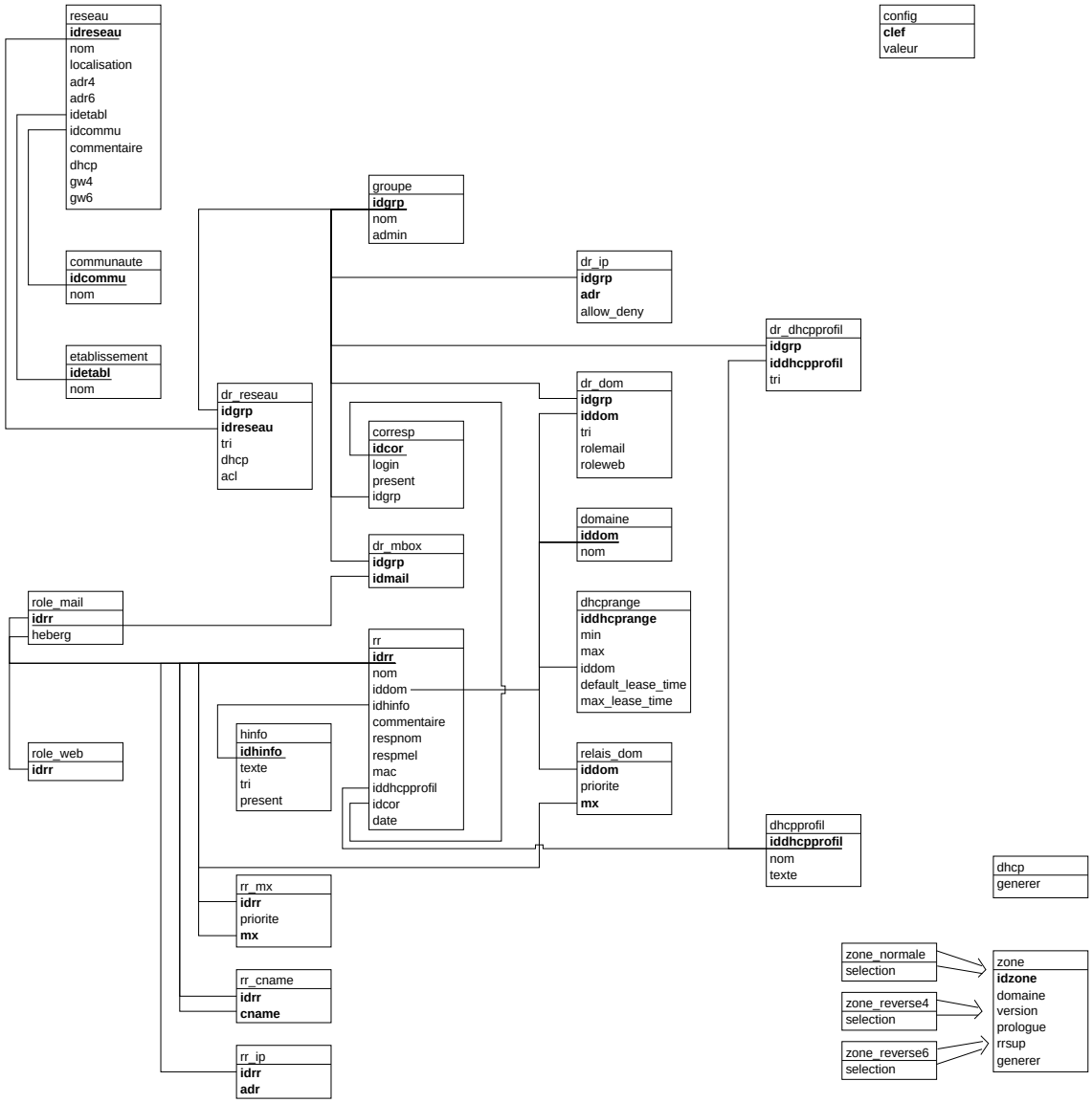
# Conclusion

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

# Annexe A

# Modèle des données

***Base DNS − Modèle logique des données au 31/03/2005***



# Annexe 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 37).

## B.1 Les réseaux

Un réseau doit être compris comme un « domaine de broadcast »[1], 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.
- une **passerelle IPv4** et une **passerelle IPv6**. Seule la passerelle IPv4 est utilisée pour le moment, en cas d'activation du service DHCP.
- un indicateur d'**activation DHCP**, qui permet de signaler que les adresses MAC de ce réseau doivent être prises en compte lors de la génération du fichier `dhcpd.conf` (voir 7.6.1, page 30).

La notion de réseau est utilisée, à l'heure actuelle, principalement 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[2].

[1] Évitez d'identifier votre classe B comme un seul réseau...

[2] Et c'est l'occasion de documenter vos réseaux, non ? ;-)

## 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 :

- 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 des intervalles d'allocation DHCP dynamique et d'utiliser des profils DHCP
- 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. ;
- est associé éventuellement à une **adresse MAC** et à un **profil DHCP**. Ces informations permettent de générer des allocations statiques avec DHCP.
- 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**.

Il faut noter que l'adresse MAC est associée à un nom, et non à une adresse IP. Ce choix a été dicté par la simplicité d'implémentation et par l'ergonomie générale de WebDNS. Le cas de machines ayant plusieurs adresses IP et utilisant cependant DHCP a paru suffisamment rare pour relever de cas particulier et ne pas être pris en compte par cette interface.

## 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 42) ;
– 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 27) 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[3] 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.

### 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 27) 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.

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

### 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 27) 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 28), vous pouvez créer dynamiquement une table de routage pour `sendmail` telle que l'attend le kit Jussieu par exemple.

## B.7 Gestion DHCP

La gestion DHCP est intimement liée au DNS. Elle ne concerne que les adresses IPv4 pour le moment.

### B.7.1 Configuration d'un réseau

Pour que la génération d'associations DHCP puisse se faire, il faut qu'un réseau donné ait l'attribut **dhcp** associé à 1, ainsi que l'**adresse IPv4** du routeur par défaut.

### B.7.2 Association statique

La génération d'allocations statiques (adresse IP, adresse MAC) repose sur l'attribut **dhcp** du réseau, mais également sur la présence d'une adresse MAC.

Si un profil DHCP est défini pour le RR considéré, l'association statique est placée dans un « *groupe* » (au sens du serveur ISC).

### B.7.3 Profils DHCP

L'application laisse à l'administrateur la possibilité de définir des profils DHCP, constitués d'un **nom** (unique) et d'un **texte**, consituté d'options du serveur DHCP.

Ces profils doivent ensuite être associés à un groupe de correspondants pour pouvoir être rendus *visibles*, par l'intermédiaire de la table `dr_dhcpprofil`. Cette visibilité n'est cependant pas exclusive : l'attribut ne sert qu'à restreindre l'apparition des profils dans les menus (avec un critère de **tri**), mais n'empêche

nullement un correspondant de falsifier un champ de formulaire pour insérer un autre profil ; les profils ne sont en effet pas considérés comme une ressource confidentielle et critique.

### B.7.4 Intervalles dynamiques

Les droits associés à un groupe (en plus de la visibilité de profils DHCP comme vu dans la section précédente) sont la possibilité de configurer des intervalles DHCP dynamiques, via le champ **dhcp** de la table `dr_reseau`.

Pour pouvoir configurer un intervalle dynamique, un correspondant réseau doit avoir l'accessibilité sur *toutes* les adresses entre l'adresse **min** et l'adresse **max**. L'intervalle est associé à un **domaine** par défaut, ainsi que des paramètres spécifiques (**default_lease_time** et **max_lease_time**) qui sont transmis au serveur DHCP et ne peuvent être hors de l'intervalle défini par les paramètres de configuration globaux (**min_lease_time** et **max_lease_time**, accessible via l'interface d'*administration des paramètres de configuration*).

### B.7.5 Indicateur de génération

La table `dhcp` ne contient qu'une seule valeur (une seule colonne et une seule ligne), qui vaut soit 0 soit 1. Un *trigger* permet de passer cette valeur à 1 lorsqu'une adresse MAC est modifiée et que la configuration DHCP doit être regénérée.

L'utilitaire de génération remet la valeur à 0 en fin d'exécution.

## B.8 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.9 Procédures

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

### B.9.1 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.9.2 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.9.3 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 caractéristiques 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.

### B.9.4 Configurer un terminal X par DHCP

Cette procédure est complexe, car elle met en œuvre beaucoup de mécanismes. On suppose que vous voulez permettre à un correspondant réseau de saisir une association pour un terminal X avec des options DHCP particulières (pour le serveur de boot, par exemple)..

Il faut donc :

- vérifier que le réseau a bien la capacité d'utiliser DHCP, en se rendant dans le menu de *modification des réseaux* (regarder en particulier les colonnes « Passerelle IPv4 » et « DHCP activé ») ;
- vérifier sur le routeur concerné que le relayage DHCP est activé ;
- définir le nouveau profil DHCP. Pour cela, se rendre dans le menu de *modification des profils DHCP* dans la page d'administration, et saisir le nom du profil, et les options DHCP que vous souhaitez ;
- par l'intermédiaire du menu de *modification des caractéristiques des groupes*, vérifier d'une part que le groupe du correspondant réseau a accès à la gestion DHCP (case « Accès à la gestion DHCP » dans la partie « Réseaux autorisés »), et lui associer d'autre part le profil DHCP (partie « Profils DHCP visibles »).

Une fois ces modifications effectuées, le correspondant réseau peut saisir l'adresse MAC et le profil que vous aurez défini. Il verra également le texte du profil DHCP s'il consulte ses droits.

# Annexe C

# Version 1.3

La version 1.3 de l'application représente un pas supplémentaire vers l'utilisation de la base DNS pour d'autres applications que la simple gestion du DNS. Le support de DHCP, très demandé par les utilisateurs, est la principale innovation de cette version.

## C.1 Changements apparus dans la version 1.3

Les changements de la version 1.3 par rapport à la version précédente sont :

- correction d'un bug affectant la génération des zones lorsqu'une adresse IPv6 était mal saisie (avec un « /64 » à la fin par exemple). Ce type d'adresse est maintenant interdit à la saisie. Patch diffusé dans la liste webdns le 28 octobre 2004.
- correction d'un bug affectant la recherche d'un correspondant à partir d'un nom qui n'est qu'un rôle de messagerie. Patch diffusé dans la liste webdns le 24 février 2005.
- correction d'un bug dans le package `webapp.tcl` de génération HTML.
- correction de méthodes de formulaires HTML qui étaient en méthode GET au lieu d'être en POST.
- changement du format interne des dates de dernière modification associées à chaque RR. C'était auparavant un nombre de secondes (format `time_t` d'Unix). C'est maintenant une date au format SQL, plus facile à manipuler.
- affichage du numéro de version de WebDNS dans le bandeau de chaque page.
- création d'un script de sauvegarde horaire, compte-tenu de la sensibilité des données hébergées par WebDNS.
- création d'utilitaires auxiliaires pour réaliser des opérations sans passer par l'interface Web :
  - ajouter une machine (nom + adresse IP) ;
  - ajouter un alias ;
  - supprimer une machine ou un alias ;
  - supprimer une adresse IP ;
  - modifier les autres attributs (adresse MAC, profil DHCP, commentaire, etc.) d'un RR ;
  - lire le prologue d'une zone et l'afficher sur la sortie standard ;
  - modifier le prologue d'une zone à partir d'un fichier ;

  Les deux derniers utilitaires ont été envoyés, dans une version « shell » sur la liste WebDNS le 25 mai 2004. Ils ont été réécrits en Tcl pour bénéficier de la substitution automatique des variables opérée par le `Makefile` de l'application Web.
- ajout de la fonctionnalité DHCP :
  - activation DHCP réseau par réseau ;
  - gestion et délégation des allocations statiques (adresse MAC / nom) ;
  - accès aux profils DHCP et à la gestion des intervalles d'allocation dynamique, groupe de correspondants par groupe de correspondants.

– ajout du droit ACL : ce droit est réservé à une utilisation future.

## C.2 Migration de la version 1.2 vers la version 1.3

La migration de la version 1.2 vers la version 1.3 nécessite une modification en profondeur de la base. Pour cela, suivez les étapes ci-après :

1. **Arrêt de l'application**
   Commencez par interdire aux utilisateur l'accès à l'application en mettant en message dans le fichier défini par la variable `NOLOGIN` (voir 7.1, page 25) sur le serveur Web. À ce stade, seuls les utilisateurs définis par la variabble `ROOT` sont habilités à utiliser l'application.
2. **Sauvegarde**
   Sauvegardez la base :

   ```
   pg_dump dns > /tmp/dns.dump
   ```

3. **Installation du langage pltcl**
   Le langage Pl/Tcl doit être installé dans le moteur PostgreSQL. Sur le serveur de données, faites :

   ```
   createlang pltcl dns
   ```

4. **Migration de la base**
   Rendez-vous dans le répertoire de migration `./upgrade/12-13/` sur le serveur de données. Éditez le fichier `upgrade.sql` et modifiez y les directives `GRANT` pour les adapter aux utilisateurs actifs (les utilisateurs de PostgreSQL, pas les utilisateurs de l'application). Lorsque vous avez fini, vous pouvez exécuter la commande :

   ```
   psql -f upgrade.sql dns
   ```

5. **Installation de la nouvelle application**
   Installez les fichiers de l'application Web, tels que définis en 7.1 (page 25), en prenant soin d'adapter les pages à trous si vous en éprouvez le besoin.
   Attention : le package `./pkgtcl/webapp.tcl` a été changé.
6. **Installation des autres fichiers**
   Reprenez les scripts de génération des zones, des routages de messagerie.
   Installez également, si vous le souhaitez, les scripts de génération DHCP.
7. **Redémarrage**
   Supprimez le fichier défini par la variable `NOLOGIN` pour autoriser les utilisateurs à accéder de nouveau à l'application.

# Annexe D

# Contributions

L'application WebDNS suscite des contributions qui peuvent intéresser la communauté des utilisateurs, via la liste `webdns@u-strasbg.fr`

Ces contributions sont décrites dans cette documentation pour faciliter votre information. Elles n'engagement pas les auteurs de WebDNS, qui n'assurent en outre bien évidemment pas leur support.

## D.1 Canal pour Esup-Portail

Cette contribution provient de Philippe Martin (`philippe.martin at univ-pau.fr`) du CRI de l'Université de Pau et des Pays de l'Adour.

L'université ayant mis en place le portail Esup[1], le CRI a développé un canal pour ce portail. Il permet aux correspondants d'effectuer, pour les plages qui les concernent, les opérations d'ajout et modification d'adresse.

Les fonctionnalités accessibles par ce canal concernent uniquement les correspondants :

- consultation de la liste des réseaux autorisés ;
- consultation de la liste des machines dans un des réseaux autorisés ;
- ajout d'une machine (nom et adresse IPv4) ;
- ajout d'une liste de machines (noms et adresses IPv4) ;
- pour une machine autorisée, les possibilités offertes sont :
  - supprimer la machine,
  - modifier les informations (système, commentaire, responsable, email),
  - modifier l'adresse IPv4,
  - ajouter une adresse IPv6,
  - modifier l'adresse IPv6,
  - supprimer l'adresse IPv6,
  - ajouter un alias,
  - supprimer un alias.

L'administration de l'application continue à se faire par l'application WebDNS elle-même.

Le canal est téléchargeable sur : ftp://ftp.univ-pau.fr/pub/ACO/canaux/ (disponible pour la version 1.2 de WebDNS à l'heure de mise sous presse).

[1] http://www.esup-portail.org

# Annexe E

# Pages à trous

| Fichier | Trou | Signification |
|---|---|---|
| (tous) | %HOMEURL% | adresse relative de la page d'accueil par rapport à la racine du serveur Web |
| | %VERSION% | numéro de version de l'application WebDNS |
| 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 |
| | %LISTEDHCPPROFILS% | liste des profils DHCP visibles |
| | %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 |

| Fichier | Trou | Signification |
|---|---|---|
| | %TABCIDRHORSRESEAU% | liste des plages hors des réseaux sélectionnés |
| | %TABDHCPPROFILS% | liste des profils DHCP visibles |
| 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 |
| | %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 |
| | %DHCPPROFIL% | menu de sélection de profil DHCP (ou champ caché) |
| consulter.html | %CORRESP% | tableau contenant l'identité du correspondant |
| | %PLAGES% | liste sélectionnable des réseaux autorisés |
| consultmx.html | %LISTEDOMAINES% | liste sélectionnable des domaines |

| Fichier | Trou | Signification |
|---|---|---|
| consultnet.html | %LISTECOMMU% | liste sélectionnable des communautés |
| | %LISTEETABL% | liste sélectionnable des établissements |
| | %MENUTRI1% | menu de sélection du critère de tri primaire |
| | %MENUTRI2% | menu de sélection du critère de tri secondaire |
| corresp.html | %CRITERE% | précédent critère de recherche de machine |
| | %RESULTAT% | résultat d'une précédente recherche d'une machine |
| dhcpedit.html | %RESEAU% | réseau pour lequel les intervalles DHCP dynamiques sont en cours d'édition |
| | %IDRESEAU% | champ caché contenant l'identificateur du réseau en cours d'édition |
| | %TABLEAU% | tableau d'édition des intervalles |
| dhcpmodif.html | %RESEAU% | réseau pour lequel les intervalles DHCP dynamques ont été modifiés |
| dhcpsel.html | %MENURESEAU% | menu de sélection du réseau |
| 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 |
| | %TABDHCPPROFIL% | le cas échéant, récapitulatif des profils DHCP visibles |
| editmodif-infos.html | %NOM% | nom du RR en cours de modification |
| | %DOMAINE% | domaine du RR en cours de modification |
| | %MAC% | champ de saisie de l'adresse MAC |
| | %DHCPPROFIL% | menu de saisie du profil DHCP ou champ caché |
| | %MENUHINFO% | menu des types de machines |
| | %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 | %ORIENTATION% | `portrait` ou `landscape` (pour liste.tex uniquement) |
| et | %NBMACHINES% | nombre de machines trouvées |
| liste.tex | %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 |

| Fichier | Trou | Signification |
|---|---|---|
| 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 |
| | %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 |
| | %MAC% | adresse MAC |
| | %DHCPPROFIL% | profil DHCP |
| | %IDDHCPPROFIL% | identificateur du profil DHCP |
| | %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 |

| Fichier | Trou | Signification |
|---|---|---|
| | %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 IP de la machine ajoutée |
| | %MAC% | adresse MAC de la machine ajoutée |
| | %DHCPPROFIL% | profil DHCP 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 |
| | %MAC% | adresse MAC de la machine modifiée |
| | %DHCPPROFIL% | profil DHCP 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 |
| | %LISTEADR% | adresses trouvées pour cette machine |
| | %MAC% | adresse MAC de la machine |
| | %DHCPPROFIL% | profil DHCP |
| | %HINFO% | type de la machine |

| Fichier | Trou | Signification |
|---|---|---|
| | %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 |
| | %MAC% | adresse MAC de la machine |
| | %DHCPPROFIL% | profil DHCP |
| | %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 |
| | %MAC% | adresse MAC de la machine |
| | %DHCPPROFIL% | profil DHCP |
| | %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 |