Une application pour décentraliser la gestion du DNS

Pierre DAVID
Centre Réseau Communication - Université Louis Pasteur
Pierre.David@crc.u-strasbg.fr

Jean BENOIT
Centre Réseau Communication - Université Louis Pasteur
Jean.Benoit@crc.u-strasbg.fr

Résumé

Le CRC, opérateur du réseau Osiris, gère plusieurs domaines, pour un parc total d'environ 18 000 machines. Jusqu'en juin 2002, l'administration DNS était centralisée au CRC. Depuis cette époque, une application Web permet à la centaine de correspondants réseau dûment enregistrés de gérer leur propre portion de l'espace d'adressage, et de générer automatiquement les zones DNS correspondantes.
L'application présentée est réutilisable dans d'autres environnements, car elle ne contient aucun élément de politique locale. Elle peut être implantée dans un petit laboratoire comme sur un gros campus, et peut même servir d'application d'inventaire.

Mots clefs

DNS, Application Web, SGBD

1 Introduction

Qui n'a jamais rêvé d'en finir avec la syntaxe absconse des zones DNS ? Qui n'a jamais rêvé d'une zone DNS exempte d'erreur ? Qui n'a jamais oublié de mettre à jour le champ SOA, ou de maintenir en cohérence la zone « inverse » ? Quel CRI d'établissement n'a jamais rêvé de se débarrasser des demandes de modification de ses correspondants réseau de laboratoires ? Quel correspondant réseau de laboratoire n'a jamais rêvé de voir ses demandes de modification DNS effectuées rapidement par son CRI ?
Convaincus que le rôle d'un gestionnaire de réseau de campus n'est pas d'enregistrer des adresses dans le DNS pour le compte de ses correspondants réseau, avec toute la lourdeur et la latence que cela signifie, nous avons réalisé une application Web afin de déléguer la gestion de ces informations au plus près des utilisateurs.
Grâce à cette application, le CRC s'est débarrassé d'une charge de travail pénible et ingrate, et les correspondants réseau bénéficient d'un outil efficace pour réaliser leurs modifications en totale autonomie et voir leur effet rapidement.
Au delà d'une simple application Web pour déléguer la gestion d'une ou plusieurs zones DNS, l'outil proposé doit être vu comme le début d'un véritable système d'information pour la gestion d'un réseau IP.

2 Contexte

Le Centre Réseau Communication (CRC) de l'Université Louis Pasteur gère et exploite le réseau métropolitain Osiris pour le compte des établissements d'enseignement supérieur et de recherche strasbourgeois ; à ce titre, il gère également les serveurs DNS d'une grande partie des domaines.
La configuration DNS est caractérisée par la présence d'une zone « u-strasbg.fr » regroupant la quasi-totalité des adresses Osiris (plus de 18 000 à ce jour). Cette configuration est due à des raisons historiques qu'il ne convient pas de juger ici, mais dont il est aisé de voir qu'elle pose des problèmes de gestion : le CRC doit réaliser les modifications pour le compte de la centaine de correspondants réseau. Outre cette grande zone, une vingtaine d'autres est également gérée, dont certaines se résument parfois à une seule déclaration (www.n'importe-quoi).
Confrontés à une quinzaine d'établissements, une quantité et une diversité de sous-réseaux et de correspondants, nous avons dû concevoir un mécanisme très générique de délégation de droits sur les domaines et sur des plages d'adresses IP, facilement adaptable dans d'autres situations.

3 Fonctionnalités

Les **correspondants réseau** disposent d'une interface permettant :
– d'ajouter une machine, ou un alias sur une machine existante ; il est également possible, moyennant confirmation pour éviter les erreurs grossières, d'ajouter une adresse IP à un nom déjà existant ;
– de supprimer une machine, un alias, ou une adresse IP ;

– de modifier les informations associées à une machine : parmi ces informations figurent des commentaires optionnels (que certains utilisent sur Osiris pour mettre des informations supplémentaires, comme le numéro de prise ou le port du commutateur concerné), le nom du propriétaire de la machine ou encore le type de machine ;
– de consulter (en HTML ou en PDF pour impression) la liste des machines d'un réseau ou d'une portion de réseau ;
– de consulter ses droits d'accès (droits sur les sous-réseaux et les domaines) et de modifier son mot de passe.

Toute modification est prise en compte dans un intervalle relativement court : 10 minutes au CRC, ce qui semble suffisant pour la plupart des correspondants réseau.

Les **administrateurs de l'application** disposent d'une interface permettant :
– de définir des groupes, avec des droits associés. Ces droits se décomposent en réseaux (pour des raisons d'esthétique d'affichage), en plages CIDR pour définir des droits (*allow* ou *deny* sur chaque plage) et en domaines ;
– de définir des utilisateurs, et de les associer dans un (et un seul) groupe ;
– de définir des réseaux, des domaines, des établissements et des types de machines ;
– de définir des paramètres de zones, qui seront utilisées pour la génération automatique des zones DNS. Ces zones sont caractérisées par :
  – un prologue, à ajouter avant tous les *resource records* générés automatiquement, et qui permet de mettre les cas particuliers qu'on ne peut modéliser dans le schéma d'un SGBD ;
  – des *resource records* qui seront ajoutés systématiquement à chaque nom, ce qui permet par exemple de mettre un MX systématique à chaque machine ;
  – un critère de sélection des objets de la zone : domaine pour une zone normale, ou notation CIDR pour une zone « inverse ».
– de consulter (en HTML ou en PDF pour impression) la liste des réseaux suivant plusieurs critères (plage d'adresses, établissements, etc.) ;

4 Architecture

L'application est bâtie sur une architecture « multi-tiers ». Les différents composants sont :
– le serveur de données, supportant le moteur SGBD PostgreSQL choisi pour ses fonctionnalités avancées, comme par exemple les notions objets (héritage de tables), le type de données « adresse IP » (qui a allégé la programmation et accéléré les requêtes), les transactions et les « triggers » ;
– le serveur Web, avec l'application elle-même ;
– le serveur DNS, qui interroge le serveur de données à intervalle régulier (via `cron`). La génération des zones a été optimisée, de telle manière que moins de 5 secondes sont nécessaires pour générer la zone de 18 000 machines sur un PC (processeur à 1 GHz) sous FreeBSD, bien que le serveur de données ne soit pas sur la même machine.

5 Installation

L'application est en cours de mise en place dans d'autres environnements, très différents d'Osiris. Le retour d'expérience obtenu montre que pour des grands environnements, de taille comparable à Osiris, l'installation exige une grande rigueur dans la définition des zones DNS (élimination des cas particuliers et des erreurs), dans la définition des correspondants réseau (en particulier lorsqu'il y en a beaucoup) et de leurs plages d'adresses autorisées.

L'application est pour le moment disponible auprès des auteurs. Si les retours, lors de ces JRES, sont encourageants, un effort sera fait pour la rendre plus largement accessible (ftp anonyme).

6 Conclusion

L'application est installée en production sur Osiris depuis juin 2002. En l'espace d'un an, 3 000 adresses ont été ajoutées, montrant combien elle est utilisée, et un nombre croissant de correspondants réseau s'en servent comme outil d'inventaire de parc. Pour le CRC, cela a éliminé un travail fastidieux et sans valeur ajoutée. Pour les correspondants, la satisfaction de faire les modifications soi-même, en totale autonomie et avec des résultats rapides est un réel gain. Le bilan est donc largement encourageant, et nous incite à développer de plus en plus la délégation de gestion, partout où la valeur ajoutée du CRC n'apparaît pas clairement.

Parmi les évolutions futures, il faut en noter trois qui nous tiennent particulièrement à cœur :
– la gestion des adresses IPv6 (qui dépend essentiellement du support de ce type de données avec PostgreSQL, disponible à partir de la version 7.4 actuellement en bêta) ;
– la possibilité pour les correspondants de créer eux-mêmes des « sous-correspondants » et de leur affecter des droits ;
– le couplage avec d'autres réalisations en cours (système d'information réseau) au CRC.