

Administration système en réseau : Domain Name System

Philippe Latu

philippe.latu(at)linux-france.org

<http://www.linux-france.org/prj/inetdoc/>

Historique des versions

\$Revision: 1401 \$ \$Date: 2009-06-03 20:23:24 +0200 (mer 03 jun 2009) \$ \$Author: latu \$

Année universitaire 2008-2009

Résumé

Ce support de travaux pratiques sur le Domain Name System s'appuie sur le logiciel BIND. Côté client ou resolver, il illustre les différents tests de fonctionnement du service à l'aide de la dig. Côté serveur, il présente l'utilisation du service suivant 3 modes : cache seulement (cache-only), maître (primary|master) et esclave (secondary|slave).

Table des matières

1. Copyright et Licence	2
1.1. Meta-information	2
2. Adressage IP des postes de travail	2
3. Installation du service DNS <i>cache-only</i>	3
4. Requêtes DNS et tests sur les types de <i>Resource Records</i> (RRs)	3
5. Serveur primaire de la zone zone(i).lan-213.stri	4
6. Serveur secondaire de la zone zone(i).lan-213.stri	5
7. Délégation des zones zone(i).lan-213.stri	6
8. Documents de référence	6

1. Copyright et Licence

Copyright (c) 2000,2009 Philippe Latu.
 Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

Copyright (c) 2000,2009 Philippe Latu.
 Permission est accordée de copier, distribuer et/ou modifier ce document selon les termes de la Licence de Documentation Libre GNU (GNU Free Documentation License), version 1.2 ou toute version ultérieure publiée par la Free Software Foundation ; sans Sections Invariables ; sans Texte de Première de Couverture, et sans Texte de Quatrième de Couverture. Une copie de la présente Licence est incluse dans la section intitulée « Licence de Documentation Libre GNU ».

1.1. Meta-information

Cet article est écrit avec *DocBook*¹ XML sur un système *Debian GNU/Linux*². Il est disponible en version imprimable aux formats PDF et Postscript : [admin.reseau.dns.pdf](#)³ | [admin.reseau.dns.ps.gz](#)⁴.

Toutes les commandes utilisées dans ce document ne sont pas spécifiques à une version particulière des systèmes UNIX ou GNU/Linux. C'est la distribution *Debian GNU/Linux* qui est utilisée pour les tests présentés. Voici une liste des paquets contenant les commandes :

- dnstools - Clients provided with BIND
- bind9-host - Version of 'host' bundled with BIND 9.X
- bind9 - Internet Domain Name Server
- bind9-doc - Documentation for BIND

2. Adressage IP des postes de travail

Tableau 1. Adressage IP des postes et attribution des zones DNS

Poste 1 : serveur primaire	Adresse IP	Poste 2 : serveur secondaire	Passerelle par défaut	zone DNS
Alderaan	192.168.126.66/28	Bespin	192.168.126.65/28	zone1.lan-213.stri
Centares	172.19.115.194/26	Coruscant	172.19.115.193/26	zone2.lan-213.stri
Dagobah	192.168.109.2/25	Endor	192.168.109.1/25	zone3.lan-213.stri
Felucia	10.7.10.2/23	Geonosis	10.7.10.1/23	zone4.lan-213.stri
Hoth	10.5.6.2/23	Mustafar	10.5.6.1/23	zone5.lan-213.stri
Naboo	172.19.114.130/26	Tatooine	172.19.114.129/26	zone6.lan-213.stri

Toutes les questions doivent être traitées avec les documentations de référence listées dans la [Section 8, « Documents de référence »](#).

Pour les documents qui ne sont pas fournis avec les paquets *Debian GNU/Linux*, il faut faire la correspondance entre les différentes possibilités d'organisation des fichiers de configuration et de leurs contenus.

¹ <http://www.docbook.org>

² <http://www.debian.org>

³ <http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.dns.pdf>

⁴ <http://www.linux-france.org/prj/inetdoc/telechargement/admin.reseau.dns.ps.gz>

3. Installation du service DNS *cache-only*

Avant d'aborder la configuration du service DNS, il faut passer par l'étape rituelle de sélection et d'installation des paquets contenant les outils logiciels de ce service.

1. Quels sont les paquets Debian correspondant au service DNS ?

Reprendre les différentes possibilités d'interrogation de la base de données des paquets vues lors des travaux pratiques précédents. On ne retient que les paquets relatifs à la version 9.x.x du logiciel BIND (*Berkeley Internet Name Domain*).

2. Une fois le paquet du serveur de noms de domaines installé quelles sont les commandes qui permettent de valider son exécution ?

Reprendre les différentes possibilités de visualisation des processus actifs, des services réseau ouverts et des messages systèmes disponibles.

3. À partir de la liste des fichiers du paquet bind9, comment identifier les répertoires contenant les fichiers de configuration et de données du service ?

Quelque soit le service étudié, les fichiers de configuration sont toujours placés sous le même répertoire. Il en est de même pour les données d'un service.

4. Pourquoi cette installation du paquet bind9 correspond à un service de type *cache-only* ?

En listant les déclarations dans les fichiers de configuration, on identifie les zones sur lesquelles le service a autorité.

5. Quelle est l'opération à effectuer sur le poste pour que le service DNS installé soit utilisé directement ?

Éditer le fichier de configuration du client ou *resolver* en désignant le service DNS exécuté localement.

6. À quel paquet appartient la commande **dig** ?

Utiliser l'option du gestionnaire de paquet dpkg pour rechercher un fichier dans la base des paquets Debian.

4. Requêtes DNS et tests sur les types de *Resource Records* (RRs)

Avant d'aborder la déclaration de nouvelles zones, il faut installer et valider le fonctionnement du service. La phase de validation passe par une batterie de tests d'interrogation des différents champs du service DNS.

Cette section est basée sur la commande **dig**. Les pages de manuels de cette commande doivent servir de base de réponse aux questions suivantes.



Pourquoi abandonner nslookup ?

La commande **nslookup** est la commande historique liée aux requêtes du service DNS. Le principal reproche fait à cette commande vient de ses réponses inadéquates en cas d'erreurs. Malheureusement, ce comportement non conforme a été utilisé dans de très nombreux développements de *shell scripts*. Pour ne pas entraîner des problèmes en cascade, les développeurs ont décidé d'initier un nouveau développement avec les versions 8.x puis 9.x de BIND : la commande **dig**. Comme ces travaux pratiques utilisent une version 9.x de BIND, il est logique de s'appuyer sur cette nouvelle commande **dig**.

1. Comment reconnaître le serveur DNS utilisé lors d'une requête avec la commande **dig** ?

Lire attentivement les résultats d'une exécution de la commande **dig** sur un nom de domaine quelconque.

2. Comment peut-on visualiser l'utilisation du cache du service DNS à l'aide de la commande **dig** ?

Partant d'un exemple de nom de domaine qui n'a pas encore été «sollicité», on lance 2 fois la même requête avec **dig** et on relève les temps de réponse. Normalement, la première requête récursive est prise en charge par le serveur et demande un temps de traitement beaucoup plus important que la seconde pour laquelle, seul le cache est consulté.

3. Quelles sont les options de la commande **dig** à utiliser pour émettre des requêtes des types suivants : NS, A, PTR, et MX ? Donner un exemple de chaque type.

Consulter les pages de manuels de la commande **dig**.

4. Quelle est l'option de la commande **dig** à utiliser pour émettre des requêtes itératives ? Donner un exemple.

Consulter les pages de manuels de la commande **dig** à la recherche du traçage des étapes d'une requête.

5. Quelle est la syntaxe de la commande **dig** à utiliser pour interroger la classe CHAOS ? Donner deux exemples de requêtes sur les champs `version.bind` et `authors.bind`.

Consulter les pages de manuels de la commande **dig** à la recherche des définitions de classes.

5. Serveur primaire de la zone `zone(i).lan-213.stri`

Il s'agit ici de configurer un serveur maître pour une nouvelle branche ou zone de l'arborescence DNS de travaux pratiques. On part de l'installation du service *cache-only* et on complète les fichiers de configuration.

La syntaxe des fichiers de zone n'est pas facile à maîtriser au premier abord. Il est donc nécessaire de faire appel à des patrons de fichiers de configuration. Un premier jeu de ces fichiers est disponible dans le guide *DNS HOWTO*. Un second jeu, pour une configuration sécurisée, est disponible à partir du site *Secure BIND Template*.

Le fichier `/usr/share/doc/bind9/README.Debian.gz` contient des informations importantes sur l'organisation des fichiers de configuration du service. Il faut retenir les éléments suivants :

- Les fichiers `db.*` qui contiennent les enregistrements sur les serveurs racine et l'interface de boucle locale sont fournis directement avec le paquet Debian. Ils sont donc susceptibles d'être mis à jour à chaque nouvelle version du paquet.
- Le fichier de configuration principal `named.conf` a été éclaté en trois parties.

`named.conf`

Déclarations d'autorité sur le `localhost` et la diffusion en résolution directe et inverse. Liste des fichiers `db.*`.

Ce fichier *appartient* au paquet `bind9` et est susceptible d'être mis à jour. Il ne faut donc pas éditer ce fichier ou y insérer des informations de définitions de zones contrôlées par le service DNS.

`named.conf.local`

Déclarations d'autorité sur les zones administrées par le serveur ; qu'il s'agisse d'un serveur primaire ou secondaire. Ce fichier n'est pas modifié lors d'une mise à jour du paquet Debian.

C'est donc le fichier qui doit être édité pour déclarer les zones sous le contrôle du serveur DNS.

`named.conf.options`

Paramétrage des options du service notamment du répertoire contenant les fichiers de déclaration des zones administrées `/var/cache/bind/`. Voir le *BIND 9 Administrator Reference Manual* pour obtenir la liste de ces options.

C'est le fichier qui doit être édité pour sécuriser les accès aux enregistrements des zones sous le contrôle du serveur DNS..

1. Quel est le fichier de configuration à éditer pour que le service DNS installé ait autorité sur la zone `zone(i).lan-213.stri` ?

Établir la correspondance entre l'organisation des fichiers de configuration du paquet Debian et les indications des documents de référence.

2. Quel est le fichier de configuration qui indique le répertoire de stockage des fichiers de déclaration de zone ? Quel est ce répertoire ? Quel est la particularité de son masque de permissions ?

Établir la correspondance entre l'organisation des fichiers de configuration du paquet Debian et les indications des documents de référence. Repérer le propriétaire du processus `named` et relever ses caractéristiques : `uid`, `gid`, répertoire utilisateur, etc.

3. Dans quelles sections du guide *DNS HOWTO* et du *BIND 9 Administrator Reference Manual* peut on trouver des exemples de déclarations de zones ? Créer un fichier de déclaration de la zone `zone(i).lan-213.stri` dans le répertoire adéquat à partir de ces exemples.

Le fichier de zone doit comprendre :

- Deux serveurs de noms : un primaire et un secondaire.
- Un *Mail Exchanger*.
- Trois hôtes avec des adresses IP différentes et quelques *Canonical Names*.

4. Quelles sont les opérations à effectuer pour valider le service DNS sur la nouvelle zone déclarée ?

Passer en revue les étapes classiques de validation d'un service : processus actif, journalisation des messages d'erreurs et tests de requêtes.

6. Serveur secondaire de la zone `zone(i).lan-213.stri`

Il s'agit ici de configurer un serveur secondaire pour la zone de l'arborescence DNS de travaux pratiques mise en place dans la section précédente. Comme dans le cas du serveur primaire, on part de l'installation du service *cache-only* fournie par le paquet Debian et on complète les fichiers de configuration.

Ici, on n'a pas besoin de se préoccuper de la syntaxe des fichiers de zone sachant que les enregistrements sont obtenus par transfert réseau entre les serveurs primaire et secondaire.

Le fichier `/usr/share/doc/bind9/README.Debian.gz` contient des informations importantes sur l'organisation des fichiers de configuration du service. Là encore, il s'agit des mêmes fichiers de configuration que ceux du serveur primaire et ont retrouve les éléments identiques :

- Les fichiers `db.*` qui contiennent les enregistrements sur les serveurs racine et l'interface de boucle locale sont fournis directement avec le paquet Debian. Ils sont donc susceptibles d'être mis à jour à chaque nouvelle version du paquet.
- Le fichier de configuration principal `named.conf` a été éclaté en trois parties.

`named.conf`

Déclarations d'autorité sur le `localhost` et la diffusion en résolution directe et inverse. Liste des fichiers `db.*`.

Ce fichier *appartient* au paquet `bind9` et est susceptible d'être mis à jour. Il ne faut donc pas éditer ce fichier ou y insérer des informations de définitions de zones contrôlées par le service DNS.

`named.conf.local`

Déclarations d'autorité sur les zones administrées par le serveur ; qu'il s'agisse d'un serveur primaire ou secondaire. Ce fichier n'est pas modifié lors d'une mise à jour du paquet Debian.

`named.conf.options`

Paramétrage des options du service notamment du répertoire contenant les fichiers de déclaration des zones administrées `/var/cache/bind/`. Voir le *BIND 9 Administrator Reference Manual* pour obtenir la liste de ces options.

1. Quel est le fichier de configuration à éditer pour que le service DNS installé ait autorité sur la zone `zone(i).lan-213.stri` ?

Établir la correspondance entre l'organisation des fichiers de configuration du paquet Debian et les indications des documents de référence.

2. Quel est le fichier de configuration qui indique le répertoire de stockage des fichiers de déclaration de zone ? Quel est ce répertoire ? Quel est la particularité de son masque de permissions ?

Établir la correspondance entre l'organisation des fichiers de configuration du paquet Debian et les indications des documents de référence. Repérer le propriétaire du processus `named` et relever ses caractéristiques : `uid`, `gid`, répertoire utilisateur, etc.

3. Quelle est la particularité d'un service DNS secondaire en matière de déclaration de zone ? Comment les enregistrements (*Resource Records*) sont ils obtenus ?

Retrouver les informations sur les *transferts de zones* ou sur les requêtes du type AXFR dans la documentation recommandée.

4. Quelles sont les opérations à effectuer pour valider le service DNS sur la nouvelle zone déclarée ?

Passer en revue les étapes classiques de validation d'un service : processus actif, journalisation des messages d'erreurs et tests de requêtes.

7. Délégation des zones `zone(i).lan-213.stri`

Il est évident que la zone `lan-213.stri` n'est pas destinée à être exploitable depuis le réseau public Internet. Le service DNS présenté ici n'est valide que dans l'infrastructure de travaux pratiques de la formation STRI. Pour que le mécanisme de délégation de zone puisse fonctionner correctement entre le niveau `lan-213.stri` et les niveaux inférieurs de l'arborescence, il est nécessaire de diriger les requêtes des serveurs des zones déléguées vers le serveur ayant autorité sur la zone `lan-213.stri`.



Note

Ce contexte de travaux pratiques n'est pas aussi singulier qu'il n'y paraît. En effet, de plus en plus d'opérateurs cherchent à contrôler le trafic DNS issu de leurs réseaux. Il est très facile d'intercepter toutes les requêtes à destination du port `udp/53` et de bloquer ainsi tous les appels directs aux serveurs du niveau racine. À titre d'exemple, voici la syntaxe `iptables` d'une requête d'interception sur une passerelle de filtrage réseau.

```
-A PREROUTING -i eth1+ -p udp --dport 53 -j REDIRECT --to-port 53
```

Dans un tel contexte, la seule solution consiste à rediriger les requêtes émises par le serveur DNS local vers le ou les serveur(s) de l'opérateur. C'est justement l'objet la manipulation ci-dessous.

1. Quel est le fichier de configuration à éditer pour que toutes les requêtes du service DNS installé soient redirigées vers le serveur maître de la zone `lan-213.stri` ?

Identifier le fichier de configuration dédié au paramétrage des options du service DNS à l'aide de la documentation fournie avec le paquet Debian.

2. Quelle est l'option de traitement des redirections ? Pour quelles requêtes cette option est-elle utilisée ?

Repérer le mot clé *forward* dans les documents de référence et le fichier de configuration.

8. Documents de référence

BIND 9 Administrator Reference Manual

*BIND 9 Administrator Reference Manual*⁵ : documentation complète la plus récente sur la syntaxe de configuration du service DNS. Si le paquet `bind9-doc` est installé, ce manuel est placé dans le répertoire `/usr/share/doc/bind9-doc/arm/`.

⁵ <http://www.bind9.net/manuals>

DNS HOWTO

*DNS HOWTO*⁶ : documentation complète sur la configuration serveur et client DNS.

Securing an Internet Name Server

*Securing an Internet Name Server*⁷ : documentation de référence sur la configuration des fonctions de sécurité d'un service DNS.

Secure BIND Template

*Secure BIND Template*⁸ : patrons de fichiers de configuration d'un service DNS.

⁶ <http://www.tldp.org/HOWTO/DNS-HOWTO.html>

⁷ <http://www.cert.org/archive/pdf/dns.pdf>

⁸ <http://www.cymru.com/Documents/secure-bind-template.html>