

Serveur DNS et DHCP couplé à LDAP

Debian GNU/Linux



Matthieu Vogelweith
10 juillet 2008

Résumé

L'objectif de ce document est de détailler l'installation d'un serveur d'infrastructure (DNS et DHCP) complet basé sur des briques libres dont la réputation n'est plus à faire : BIND [1] (Berkeley Internet Name Domain), DHCPD [2] (Dynamic Host Configuration Protocol) et OpenLDAP [3].

Afin de centraliser les informations relatives aux machines du réseau et de permettre un déploiement à grande échelle, les deux services utiliseront OpenLDAP pour stocker les informations. Tous les enregistrements DNS et toute la configuration du(des) serveur(s) DHCP sera donc enregistrée dans l'annuaire.

Pour faciliter l'administration de ces services, ce document détaillera l'utilisation du module Network du MDS (**M**andriva **D**irectory **S**erver [4]). Enfin ce document présente de nombreux outils et astuces permettant de tester et évaluer le serveur mis en place.

Ce document a été rédigé en LaTeX en utilisant l'excellent Vim sous Debian GNU/Linux. Il est disponible aux formats XHTML et PDF. Les sources LaTeX sont disponibles ici : [L^AT_EX](#)

Licence

Copyright ©2008 Matthieu VOGELWEITH <matthieu@vogelweith.com>.

Vous avez le droit de copier, distribuer et/ou modifier ce document selon les termes de la GNU Free Documentation License, Version 1.2 ou ultérieure publiée par la Free Software Foundation ; avec aucune section inaltérable, aucun texte de première page de couverture, et aucun texte de dernière page de couverture. Une copie de la licence est disponible dans la page [GNU Free Documentation License](#).

Table des matières

Table des matières	3
1 Préparation	4
1.1 Pré requis	4
1.2 Configuration du gestionnaire de paquets	4
1.3 Annuaire OpenLDAP & MDS	4
1.4 Plugin Network du MDS	4
2 Serveur Bind 9	7
2.1 Installation des paquets	7
2.2 Configuration de base	7
2.3 Configuration LDAP	7
3 Serveur DHCP	8
3.1 Installation des paquets	8
3.2 Configuration du service	8
3.3 Configuration avancée	8
4 Références	9

Chapitre 1

Préparation

1.1 Pré requis

Ce document suppose que le serveur est déjà installé avec une Debian Etch [5] propre. Pour plus d'informations sur l'installation et la configuration du système de base, voir ma page dédiée à l'installation du système.

1.2 Configuration du gestionnaire de paquets

Comme indiqué précédemment, l'administration courante du serveur se fera avec le module Network du MDS. Pour obtenir les paquets, ajouter simplement les lignes suivantes dans le fichier `/etc/apt/sources.list` :

```
# Mandriva Directory Server
deb http://mds.mandriva.org/pub/mds/debian etch main
```

Notons que ce dépôt contient également les paquets pour BIND et DHCP recompilés avec le support LDAP. Ce support n'est pas encore intégré dans les archives officielles fournies par l'ISC mais est disponible avec les patch réalisés par FIXME [?].

Reste maintenant à mettre à jour la liste des paquets disponibles avec la commande suivante :

```
# aptitude update
```

1.3 Annuaire OpenLDAP & MDS

L'installation du serveur LDAP et la configuration de base du MDS faisant l'objet d'un document dédié [6], elles ne seront pas détaillées ici. L'installation et la configuration du plugin Network du MDS sont cependant expliquées dans le paragraphe suivant.

1.4 Plugin Network du MDS

- Gestion de zones de plusieurs réseaux distants à partir de la même interface.
- > Plus besoin de faire quarante SSH pour modifier l'infrastructure des sites distants.

Le MDS possède un plugin permettant de gérer les champs LDAP relatifs aux zones DNS et aux sous-réseaux DHCP. Notons que cette page propose d'utiliser le MDS pour la gestion de l'annuaire mais il est tout à fait possible de suivre cette documentation en éditant l'annuaire en utilisant d'autres outils.

```
# aptitude install mmc-agent mmc-web-base mmc-web-network python-mmc-network slapd ldap-  
utils
```

Les schémas proposés de base avec OpenLDAP ne permette pas de gérer les services DNS et DHCP. Les schémas nécessaires sont donc fournis avec les paquets du MDS. Pour utiliser ces schémas, il faut dans un premier temps les copier dans le répertoire dédié à cet effet :

```
# cp /usr/share/doc/python-mmc-base/contrib/ldap/mmc.schema /etc/ldap/schema/  
# cp /usr/share/doc/python-mmc-base/contrib/ldap/dnszone.schema /etc/ldap/schema/  
# cp /usr/share/doc/python-mmc-base/contrib/ldap/dhcp.schema /etc/ldap/schema/
```

Il faut maintenant configurer slapd pour qu'il utilise ces nouveaux schémas. Ajouter les lignes suivantes dans `/etc/ldap/slapd.conf` :

```
include /etc/ldap/schema/mmc.schema  
include /etc/ldap/schema/dnszone.schema  
include /etc/ldap/schema/dhcp.schema
```

Et enfin re-démarrer le service pour que les modifications soient prises en compte :

```
# /etc/init.d/slapd restart
```

Le serveur LDAP est maintenant prêt pour fournir les différents champs nécessaires aux serveurs DNS et DHCP, il reste maintenant à configurer le plugin Network du MDS. Toute la configuration se fait dans `/etc/mmc/plugins/network.ini` :

```
[main]  
disable = 0  
  
[dhcp]  
dn = ou=DHCP,dc=example,dc=org  
pidfile = /var/run/dhcpd.pid  
init = /etc/init.d/dhcp3-server  
logfile = /var/log/syslog  
leases = /var/lib/dhcp3/dhcpd.leases  
  
[dns]  
dn = ou=DNS,dc=example,dc=org  
pidfile = /var/run/bind/run/named.pid  
init = /etc/init.d/bind9  
logfile = /var/log/daemon.log  
bindroot = /etc/bind/  
bindgroup = bind  
# dnsreader = DNS Reader  
# dnsreaderpassword = DNSReaderPassword
```

Pour appliquer les modifications et vérifier que la structure de l'annuaire est correcte, il faut simplement redémarrer l'agent MMC :

```
# /etc/init.d/mmc-agent restart
```

Toutes les branches LDAP nécessaires au fonctionnement du MDS sont automatiquement créées lors du redémarrage de l'agent.

Chapitre 2

Serveur Bind 9

2.1 Installation des paquets

```
# aptitude install bind9 resolvconf
```

2.2 Configuration de base

- Utilisation du fichier auto-généré par resolvconf pour gérer les forwarders. Dans `/etc/bind/named.conf` :

```
# include "/etc/bind/named.conf.options";  
include "/var/run/bind/named.options";
```

2.3 Configuration LDAP

Tous les fichiers de configuration nécessaires à la connexion avec OpenLDAP sont générés automatiquement par le MDS. Il suffit simplement d'inclure le fichier principal dans le fichier `/etc/bind/named.conf` :

```
include "/etc/bind/named.conf.ldap";
```

Chapitre 3

Serveur DHCP

3.1 Installation des paquets

```
# aptitude install dhcp3-server-ldap
```

3.2 Configuration du service

La configuration du service DHCP est très simple, il suffit de lui indiquer les paramètres de connexions à l'annuaire LDAP. On peut par exemple créer un fichier `/etc/dhcp3/dhcpd.conf.ldap` contenant les lignes suivantes :

```
ldap-server "localhost";  
ldap-port 389;  
ldap-base-dn "dc=example,dc=org";  
ldap-method dynamic;  
ldap-debug-file "/var/log/dhcp-ldap-startup.log";
```

Il suffit ensuite d'inclure ce fichier dans le fichier `/etc/dhcp3/dhcpd.conf` :

```
include "/etc/dhcp3/dhcpd.conf.ldap";
```

3.3 Configuration avancée

Utilisation d'un utilisateur dédié pour la connexion à l'annuaire :

```
ldap-username "cn=DHCPmaster,dc=example,dc=org";  
ldap-password "mypassword";
```

Utilisation forcée d'un hostname pour l'identification :

```
ldap-dhcp-server-cn "dhcpserver";
```

Chapitre 4

Références

- [1] Site officiel de bind. www.isc.org/bind/.
- [2] Site officiel de dhcpd. www.isc.org/dhcpd/.
- [3] Site officiel de openldap. www.openldap.org.
- [4] Site du mandriva directory server. mds.mandriva.org.
- [5] Site officiel du projet debian. www.debian.org.
- [6] Document ldap - mds. www.vogelweith.com/debian_server/050_openldap.php.