

Debian Lenny - Gestion centralisée avec Cfengine

Debian GNU/Linux



Matthieu Vogelweith
10 mars 2009

Résumé

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 ©2009 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 1.3 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 Présentation	4
1.1 Les différents composants	4
1.2 Scénario	4
2 Mise en place du serveur Cfengine	5
2.1 Installation	5
2.2 Configuration de cfserverd	5
2.3 Démarrage automatique	6
3 Mise en place des clients Cfengine	7
3.1 Installation	7
3.2 Configuration des mises à jour	7
3.3 Copie de la clé publique	8
3.4 Démarrage automatique	8
4 Quelques scripts d'actions	9
4.1 Organisation	9
4.2 Maintenance du mot de passe root	9
4.3 Maintenance du fichier sources.list	9
5 Références	11

Chapitre 1

Présentation

1.1 Les différents composants

- Sur le serveur, cfservd (permet de gérer les connexions entrantes et de diffuser les différents fichiers.
- Sur le client, plusieurs possibilités :
 - cfagent lancé en crontab
 - cfexecd en mode "wrapper" lancé en crontab
 - cfexecd en mode démon

1.2 Scénario

- Installation et configuration du serveur.
- Installation et configuration des clients.
- Les clients vont chercher les fichiers de configuration sur le serveur en utilisant cfexecd et update.conf.
- Les clients exécutent les actions décrites dans cfagent.conf localement.

Chapitre 2

Mise en place du serveur Cfengine

2.1 Installation

```
# aptitude install cfengine2
```

2.2 Configuration de cfserverd

- Dans /etc/cfengine/cfserverd.conf

```
control:
    # Domaine ID
    domain = ( example.com )

    # Allow root user
    AllowUsers = ( root )

    # Elapsed time before starting again an action
    IfElapsed = ( 5 )
    ExpireAfter = ( 15 )

    # Max connections allowed to this cfserverd
    MaxConnections = ( 50 )

    # Allow multiple connections from one client
    MultipleConnections = ( true )

    # Trust keys from local network
    TrustKeysFrom = ( 192.168.101.0/24 )

admit:
    /etc/cfengine          192.168.101.0/24
    /usr/sbin/cfagent      192.168.101.0/24
```

- Dans /etc/cfengine/cfagent.conf

```
control:
    actionsequence = ( processes editfiles )
    domain         = ( example.com )
    access         = ( root )
```

```

# Where cfexecd sends reports
smtpserver      = ( 127.0.0.1 )
sysadm          = ( root )

# Run twice an hour
schedule        = ( Min00_05 Min30_35 )

# Variables
cf_server       = ( cfengine.example.com )
cf_dir          = ( /etc/cfengine )

processes:
# Make sure these processes are always running
"cfengine2" restart "/etc/init.d/cfengine2 restart"

editfiles:

linux::
# Make sure cfexecd runs at boot time and daily.
{
    /etc/cron.d/cfengine
    AutoCreate
    Backup "false"
    EmptyEntireFilePlease
    InsertLine '# /etc/cron.d/cfengine: crontab entries for cfengine'
    InsertLine ''
    InsertLine '@reboot          root    [ -x /usr/sbin/cfexecd ] && /usr/sbin/
cfexecd -F -1 || exit 1'
    InsertLine '0 2 * * *          root    [ -x /usr/sbin/cfexecd ] && /usr/sbin/
cfexecd -F -1 || exit 1'
}

```

2.3 Démarrage automatique

Pour que les différents démons démarrent automatiquement au boot de la machine, il suffit de modifier les variables suivantes dans le fichier `/etc/default/cfengine2` :

```

RUN_CFSERVD=1
RUN_CFEEXEC=1
RUN_CFENVD=1

```

Il est en suite possible de démarrer tous les démons avec la commande suivante :

```

# /etc/init.d/cfengine2 restart

```

Chapitre 3

Mise en place des clients Cfengine

3.1 Installation

L'installation des clients se fait exactement comme sur le serveur, en installant le paquet **cfengine**. La seule différence se situera au niveau des démons démarrés au boot de la machine.

```
# aptitude install cfengine2
```

3.2 Configuration des mises à jour

Le fichier `/etc/cfengine/update.conf` est utilisé par `cfagent` ou `cfexecd` pour se connecter au serveur `cfserverd` et mettre à jour les différents fichiers de configuration. Ce fichier est le seul qu'il est indispensable de diffuser manuellement sur les différents clients `cfengine`.

```
control:

    actionsequence = ( copy tidy ) # Keep this simple and constant
    domain         = ( example.com ) # Needed for remote copy

    policyhost     = ( cfengine.example.com )

    master_cfinput = ( /etc/cfengine )
    workdir        = ( /etc/cfengine )

    SplayTime     = ( 0 )

copy:

    $(master_cfinput)    dest=$(workdir)
                        r=inf
                        mode=700
                        type=binary
                        include=cfagent.conf
                        include=update.conf
                        include=cf.*
                        purge=true
                        server=$(policyhost)

# Cfexecd stores output in this directory.
# Make sure we don't build up files and choke on our own words!
tidy:
    $(workdir)/outputs pattern=* age=7
```

La configuration décrite ci-dessus permet donc de peupler le répertoire `/etc/cfengine` des clients à partir du répertoire `/etc/cfengine` du serveur. Notons que la copie est récursive (`r=inf`), que les fichiers non présents sur le serveurs sont supprimés (`purge=true`) et que seuls les fichiers suivants sont copiés :

- `cfagent.conf` : le fichier de configuration de base de l'agent.
- `update.conf` : de cette façon il sera possible de modifier ce fichier sur le serveur pour modifier le comportement des mises à jour sur les clients.
- `cf.*` : tous les fichiers de configurations permettant de spécifier les actions à exécuter sur les clients.

3.3 Copie de la clé publique

```
# scp root@cfengine:/var/lib/cfengine2/ppkeys/localhost.pub /var/lib/cfengine2/ppkeys/  
root@xx.xx.xx.xx.pub
```

3.4 Démarrage automatique

Pour que le démon `cfexecd` démarre automatiquement au boot de la machine, il suffit de modifier la variable suivante dans le fichier `/etc/default/cfengine2` :

```
RUN_CFEEXEC=1  
RUN_CFENVD=1
```

Il est en suite possible de démarrer le démon avec la commande suivante :

```
# /etc/init.d/cfengine2 restart
```

Lors du premier démarrage, `cfexecd` va établir la connexion avec le serveur, envoyer sa clé publique et copier tous les fichiers de configuration (notamment `cfagent.conf`). Il sera ensuite exécuté périodiquement en suivant la politique définie par la variable **schedule** du fichier `cfagent.conf`. Dans la configuration décrite précédemment, l'agent sera exécuté toute les 30 minutes.

Chapitre 4

Quelques scripts d'actions

4.1 Organisation

Afin de conserver une installation facilement maintenable il est très important d'organiser les différents fichiers de configuration de manière réfléchie. Un bon point de départ est sans doute d'utiliser un fichier de configuration distinct pour chaque action. Tous ces fichiers doivent ensuite être "importés" dans le fichier principal cfagent.conf.

Ce chapitre présente 2 fichiers de configuration permettant de changer le mot de passe root et de maintenir le fichier **sources.list** sur les clients. Ces deux fichiers seront nommés respectivement cf.rootpasswd et cf.sources.list. Pour qu'ils soient analysés lors de la prochaine exécution de l'agent, il suffit de les importer en ajoutant les lignes suivantes à la fin du fichier /etc/cfengine/cfagent.conf :

```
import:
  linux::
    cf.rootpassword
    cf.sources.list
```

Ainsi, toutes les machines qui sont dans la classe **linux** exécuteront les actions définies dans ces deux fichiers.

4.2 Maintenance du mot de passe root

- Dans /etc/cfengine/cf.rootpassword

4.3 Maintenance du fichier sources.list

- Dans /etc/cfengine/cf.sources.list

```
control:
  actionsequence = ( editfiles )
editfiles:
```

```

debian_5::

# Sources.list
{
    /etc/apt/sources.list
    AutoCreate
    Backup "false"
    EmptyEntireFilePlease

    # Insert debian repos
    InsertLine '# Generated by Cfengine : Do not edit this file by hand'
    InsertLine ''
    InsertLine '# Debian 5.0 (Lenny)'
    InsertLine 'deb http://ftp.fr.debian.org/debian/ lenny main non-free contrib'
    InsertLine ''
    InsertLine '# Security Updates'
    InsertLine 'deb http://security.debian.org/ lenny/updates main contrib non-
    free'
    InsertLine ''
    InsertLine '# Debian Volatile'
    InsertLine 'deb http://volatile.debian.org/debian-volatile lenny/volatile
    main'
}

# Proxy Setup
{
    /etc/apt/apt.conf.d/99proxy
    AutoCreate
    Backup "false"
    EmptyEntireFilePlease
    InsertLine '# Generated by Cfengine : Do not edit this file by hand'
    InsertLine ''
    InsertLine '# APT-Cacher proxy'
    InsertLine 'Acquire::http::Proxy "http://192.168.101.254:3142";'
}

debian_5.davical::

{
    /etc/apt/sources.list
    AutoCreate
    InsertLine ''
    AppendIfNoSuchLine '# Davical'
    AppendIfNoSuchLine 'deb http://debian.mcmillan.net.nz/debian lenny awm'
}

```

Chapitre 5

Références

[1] Site officiel du projet debian. www.debian.org.

[2] Site du projet cfengine. www.cfengine.org.