
Utilisation du logiciel d'administration automatique Cfengine

Ronan.Keryell@enst-bretagne.fr

—

Laboratoire Informatique & Télécommunications

Département Informatique

École Nationale Supérieure des Télécommunications de Bretagne

0-1

- Frustration
 - ▶ Installer une machine quand on sait le faire
 - ▶ Temps ↗ lorsque nombre de machines à installer ↗
- Processus naturel en informatique : appliquer les concepts à l'outil lui-même (« *boot-straper* »)

~> Installation et administration système automatique



- Méthode déployée au
 - ▶ Centre de Recherche en Informatique de l'École Nationale Supérieure des Mines de Paris
 - ▶ Laboratoire Informatique et Télécommunication de l'École Nationale Supérieure des Télécommunications de Bretagne
- Besoins d'installation et d'administration
 - ▶ Ordinateurs de recherche UNIX (parallélisation, distribution, compilation, optimisation de programme,...)
 - ▶ Ordinateurs d'élèves (mastère IAR2M SOLARIS, LINUX, NT)
 - ▶ Machines de télétravail à la maison
 - ▶ Ordinateurs parallèle (RÉACTIVE)
- Environnement système commun



Pour favoriser la portabilité

- Utiliser méthode d'installation automatique (JumpStart, FAI, KickStart, Replicator,...) de manière minimale
- Terminer avec une méthode portable
- Maintenir le système fonctionnel avec une méthode portable



Nécessite un système d'installation minimal



- CFENGINE
- Exemples
- PCFENGINE

Version étendue de l'article sur

<http://www.cri.ensmp.fr/~keryell/publications/conf/2001/JRES2001/cfengine>



- Logiciel développé depuis 1993 principalement par Mark BURGESS
- Projet de recherche concernant l'administration système distribuée et automatisée
- Utilisé de par le monde sur $\approx 10^5$ machines (UNIX & NT)
- Idées
 - ▶ Politique établie sous formes de règles de haut niveau plutôt que de détailler chaque machine
 - ▶ Langage déclaratif « ce qu'on veut » « *how it should be* »
 - ▶ Configuration (éventuellement) centralisée
 - ▶ Philosophie de Mark BURGESS : système immunitaire où le système réagit par une série d'actions lorsqu'il rencontre telle ou telle situation anormale



- ▶ Progressivement le système doit revenir vers l'état stable pleinement fonctionnel
- Intérêts multiples indiscutables
 - ▶ Faire du down-sizing managérial dans le back-office du SI conformément aux needs des share-holders
 - ▶ Mettre tous les ingénieurs système au chômage
 - ▶ Simplifier organisation JRES2003



- Bonne nouvelle pour administrateurs système dans la salle : informatique théorique prouve que la stabilité est indécidable dans le cas général ☹
- Essayer d'écrire les règles afin de favoriser l'attracteur étrange « ça marche » plutôt que « c'est planté »
- Mauvaise nouvelle pour les organisateurs de JRES2003... ☺



- Système de base :
 - ▶ Ensemble des fichiers de configuration définissant le comportement à adopter
 - Typiquement localisés dans le répertoire `/usr/local/share/cfengine` (reflété par la valeur de la variable d'environnement `CFINPUTS`)
 - Configuration stockée dans le fichier `cfengine.conf`
 - ▶ Exécutant de CFENGINE `cfagent` doit être lancé régulièrement pour effectuer le travail
- Systèmes optionnels :
 - ▶ Serveur sécurisé de configurations `cfserverd`
 - Fournit à des `cfagents` distants leur configuration (s'ils ne peuvent pas y accéder par d'autres moyens)



- Exécutions à distance de `cfagents`
- ▶ Démon centralisant l'état global du système pour faire des statistiques sur le fonctionnement du système
- ▶ un outil de représentation graphique de l'état du système



- Configuration d'une machine dépend de nombreux aspects
 - ▶ Rôle dans l'entreprise
 - ▶ Localisation géographique
 - ▶ Réseau qui la contient
 - ▶ Structure matérielle :
 - Architecture
 - Système d'exploitation
 - Disques disponibles
 - Type de réseau local
 - Écran disponible
 - ...
- Simplification combinatoire : caractéristiques abstraites par des « classes »



Classification lors de l'exécution par

- Identité de la machine (rodomouls_enst_bretagne_fr, enst_bretagne_fr, rodomouls), adresses (192_44_75_24), réseau (192_44_75)
- Système d'exploitation et architecture matérielle (sunos_5_9, sunos_sun4u, sparc, 32_bit,...)
- Temps et la date (Sunday, Hr18, Min59, Min55_00, Day9, December, Yr2001)
~> Changer de comportement au cours du temps



Besoin de définir des classes de plus haut niveau à partir des précédentes

- Algèbre booléenne . | ! ()
- Déclaration explicite

classes:

```
apache_hosts = ( +@n_web www.enstb.org -gavotte.enst-bretagne.fr)
cri_sun = ( +@n_cri_sun )
sun_sans_serveur_WWW = ( +@n_cri_sun -@n_web )
```

- Arguments ligne de commande -D ou -N

```
cfagent -DInstallationTime
```

- Succès d'une commande

classes:

```
have_cc = ( "/bin/test -x /usr/ucb/cc"
            "/bin/test -x /usr/local/bin/gnu/cc" )
```



- Par retour d'action

`define=liste-de-classes`

Concept moteur principal de CFENGINE

- ↪ Déclenche des cascades d'actions
- Sortie de l'exécution d'un module externe à CFENGINE

`+ma-classe`



Utilisation avec syntaxe $\$(variable)$

- Variables prédéfinies contenant
 - ▶ Éléments de nommage de la machine : `host`, `fqhost`, `ipaddress`, `domain`, `site`,...
 - ▶ Indications temporelles : `date`, `year`, `timezone`
 - ▶ Adresse électronique de l'administrateur système `sysadm`
 - ▶ Liste des classes : `AllClasses` contient toutes les classes auquel appartient l'instance de CFENGINE à un instant donnée et `class` contient la liste des classes prédéfinies
 - ▶ Variables syntaxiques contenant des constantes textuelles de type caractère `cr`, `lf`, `tab`, `quote`, `dblquote`, `spc`, `dollar`,...



- Variables utilisateur
 - ▶ Syntaxe *variable* = (*contenu*)
 - ▶ Déclarée par un module en sortant *=variable* = (*contenu*)



Découpage de tâches CFENGINE en sous-tâches rangées par actions thématiques

thème :

classe ::

action1

action2

...



links:

```
solaris.apache_hosts::
```

```
# To have apache starting at boot time:
```

```
/etc/rc2.d/K15apachectl -> /etc/init.d/apachectl
```

```
/etc/rc3.d/S85apachectl -> /etc/init.d/apachectl
```



Pas d'action concrète mais influe comportement global

- Inclut des fichiers avec action import

```
import:
```

```
$(cf_directory)/main.cf
```

```
$(cf_directory)/accounting.cf
```

- Auberge espagnole de CFENGINE : control avec les déclarations de variables, des déclarations de classes, des motifs d'exclusion,...

```
control:
```

```
cf_directory = ( /usr/local/share/cfengine/cf )
```

```
LIT::
```

```
site = ( LIT )
```

```
domain = ( enst-bretagne.fr )
```

```
sysadm = ( Ronan.Keryell@enst-bretagne.fr )
```

```
any::
```

```
timezone = ( MET )
```



- Sous Unix tout est un fichier ~> majorité des actions orientées fichier
- Vérifier et corriger la présence et les droits de fichiers et éventuellement de les créer avec `files`

`files:`

`solaris::`

`# Create this file to log the login failures:`

`/var/adm/loginlog mode=600 owner=root group=sys action=touch`

`any::`

`home mode=o-w r=inf act=fixall`

`home/public_html mode=a+r fixall`

- Cas particuliers des répertoires avec `directories`

`directories:`

`# Create the local mount points per machines:`

`LIT.rodomouls::`



```
/export/burette  
/export/dinette  
/export/pipette  
LIT.gavotte::  
/export/interne  
/export/calice1  
/export/calice2  
/export/calice3
```

- Lors d'une installation, tâche fastidieuse d'édition de fichiers sous-traitée à edit

```
editfiles:  
solaris::  
{  
# Log all the login failures:  
/etc/default/login  
AppendIfNoSuchLine "SYSLOG_FAILED_LOGINS=0"
```



```
}  
{  
# Add accounting jobs to the adm crontab:  
/var/spool/cron/crontabs/adm  
AutoCreate  
AppendIfNoSuchLine "# Accounting stuff:"  
AppendIfNoSuchLine "0 * * * * /usr/lib/acct/ckpacct"  
AppendIfNoSuchLine  
    "30 2 * * * /usr/lib/acct/runacct 2> /var/adm/acct/nite/fd2log"  
AppendIfNoSuchLine "30 7 1 * * /usr/lib/acct/monacct"  
DefineClasses "StartAccounting"  
DefineClasses "RestartCron"  
}  
# To mount the file systems with logging enabled to eradicate fsck.  
{ /etc/vfstab  
    # To use logging ufs file systems:
```



```
ReplaceAll '^(/dev/.*[ $(tab)]ufs[ $(tab)].*)-$' With '\1logging'
}
solaris.LIT::
# Use DNS and files :
{ /etc/nsswitch.conf
  SetCommentStart '#'
  CommentLinesStarting 'hosts:      nis [NOTFOUND=return] files'
  CommentLinesStarting 'hosts:      files'
  CommentLinesStarting 'hosts:      files dns'
  AppendIfNoSuchLine '# Put the DNS in first place to have FQHN. RK.'
  AppendIfNoSuchLine 'hosts:      dns files'
}
```

Nombreuses directives spécialisées dans les éditions
incrémentales orientées administration système

- copy copie fichier ou arborescence, éventuellement depuis un
cfserverd



copy:

UserDiskServer::

```
/local/masterfiles/.cshrc  dest=home/.cshrc mode=0600
```

solaris.OpenSSH::

```
$(shared_conf)/OpenSSH/etc/openssh/ssh_config
```

```
dest=/etc/openssh/ssh_config
```

```
type=byte
```

```
define=InstallSsh
```

- Liens symboliques ou durs avec links

links:

```
# Add the entry to launch pppd at boot time:
```

solaris.pppd_hosts::

```
/etc/rc3.d/S90pppd ->! /etc/init.d/pppd
```

- Disques jamais trop grands ~> nettoyage avec tidy

tidy:

AllHomeServers::



```
home      pattern=core      R=inf age=0
home      pattern=*~        R=inf age=7
home      pattern=#*        R=inf age=30
any::
/tmp/     pat=*              R=inf  age=1
/         pat=core          R=2    age=0
/etc      pat=hosts.equiv    r=0    age=0
```

- Changement de nom en lieu de suppression

```
disable:
```

```
any::
```

```
    /etc/hosts.equiv
```

```
WWW.(Sunday|Wednesday)::
```

```
    /usr/local/httpd/logs/access_log rotate=10
```

- Certains fichiers ou répertoires devant échapper aux copies ou aux nettoyages sont précisés avec l'action ignore :

```
ignore:
```



```
any::  
  # Prevent tidying .X11 directories in /tmp  
  .X11  
  # Don't tidy emacs locks  
  !*  
  /local/lib/gnu/emacs/lock/
```



- shellcommands pour exécuter des commandes depuis CFENGINE :

shellcommands:

```
AllBinaryServers.sun4.Saturday::
```

```
    "/usr/etc/catman -w -M /usr/local/man"
```

```
    "/usr/etc/catman -w -M /usr/local/X11R5/man"
```

```
solaris.LaunchExportfs::
```

```
    "/usr/sbin/shareall"
```

- Contrôle des processus en train de tourner avec processes :

processes:

```
# At least one httpd process should run,
```

```
# except during installation of course...
```

```
solaris.apache_hosts.!InstallationTime::
```



```
    "/usr/local/apache/bin/httpd"
```

```
    matches=>0
```



```
restart "/etc/init.d/apachectl start"  
RestartSyslogd::  
# Tell syslogd to read again its configuration:  
"/usr/sbin/syslogd" signal=hup
```



- `classes` ou `groups` déclarent de nouvelles classes
- `acl` déclare des ACL portables utilisables dans d'autres actions
- `filters` déclare des ensembles de paramètres utilisables par d'autres classes   modularité



Actions de haut niveau

- broadcast spécifie adresses de diffusion
- interfaces précise le masque réseau
- defaultroute vérifier la route par défaut
- resolve configure le client DNS



- disks ou required déclenchent des actions s'il n'y a plus assez de place ou que des points de montage ont disparu
- Montages explicites généraux avec miscmounts

```
miscmounts:
```

```
  physics::
```

```
    libraryserver:/${(site)}/libraryserver/data2
```

```
    /${(site)}/libraryserver/data2 mode=ro
```

- Actions pour réaliser le schéma d'organisation dans l'université de l'auteur de CFENGINE. Auto-monteur probablement préférable



Respect d'une certaine causalité avec actionsequence dans control

```
control:
```

```
  any::
```

```
    actionsequence = (
```

```
      netconfig
```

```
      resolve
```

```
      checktimezone
```

```
      directories
```

```
      files
```

```
      copy
```

```
      editfiles
```

```
      links
```

```
      tidy
```

```
      module:mytests.class1.class2.class3 arg1 arg2
```

```
      shellcommands
```



```
processes
# At least for the Minitel access installation:
copy.minitel
editfiles.minitel
)
```



Déploiement du système au sein du CRI et du LIT

- Simplicité d'administration, même sans compétence
- Portabilité du point de vue
 - ▶ Système d'exploitation (SOLARIS, GNU/LINUX/DEBIAN, GNU/LINUX/REDHAT,...) et du modèle d'ordinateur (SUN, PC,...)
 - ▶ Localisation et entité administrative, laboratoire, entreprise, maison
 - ▶ Utilisation variée des machines
 - En réseau ou pas
 - Machine utilisateur ou plutôt de type serveur
 - Spécialisée comme des nœuds d'une machine parallèle, embarquée comme pour un pare-feu ou un nœud de réseau actif



- Serveurs www stockés chez un hébergeur et sur lesquels il est difficile d'intervenir physiquement
- Référentiel centralisé
 - ▶ Vision cohérente du système
 - ▶ Facilite l'installation du système au départ ou en cas de gros dégâts
 - ▶ Mise à jour à plusieurs de ce référentiel pour partager et mettre en commun les expériences des administrateurs distribué
- Tolérance aux pannes en ayant un nombre arbitraire d'instances du système d'installation
- Suppose confiance mutuelle entre administrateurs des différents sites mais intérêt à factoriser les efforts



- Avoir un espace de nommage unique
- Exploiter toutes les ressources matérielles disponibles (disques durs, pour améliorer les capacités et augmenter la tolérance aux pannes)
- Supprimer maximum de points uniques de panne possibles (plusieurs routeurs de courrier électronique, quitte à utiliser de la place disque et des machines en plus pour le faire)
- Distribuer le plus possible les services sur les différentes machines pour une meilleure tolérance aux pannes même pour des services n'existant qu'à un exemplaire : si une machine tombe en panne, seul le compte d'un ou de quelques utilisateurs sont indisponibles jusqu'au transfert ou restauration sur une autre machine par exemple
- Préférer des approches logicielles pour assurer la tolérance aux

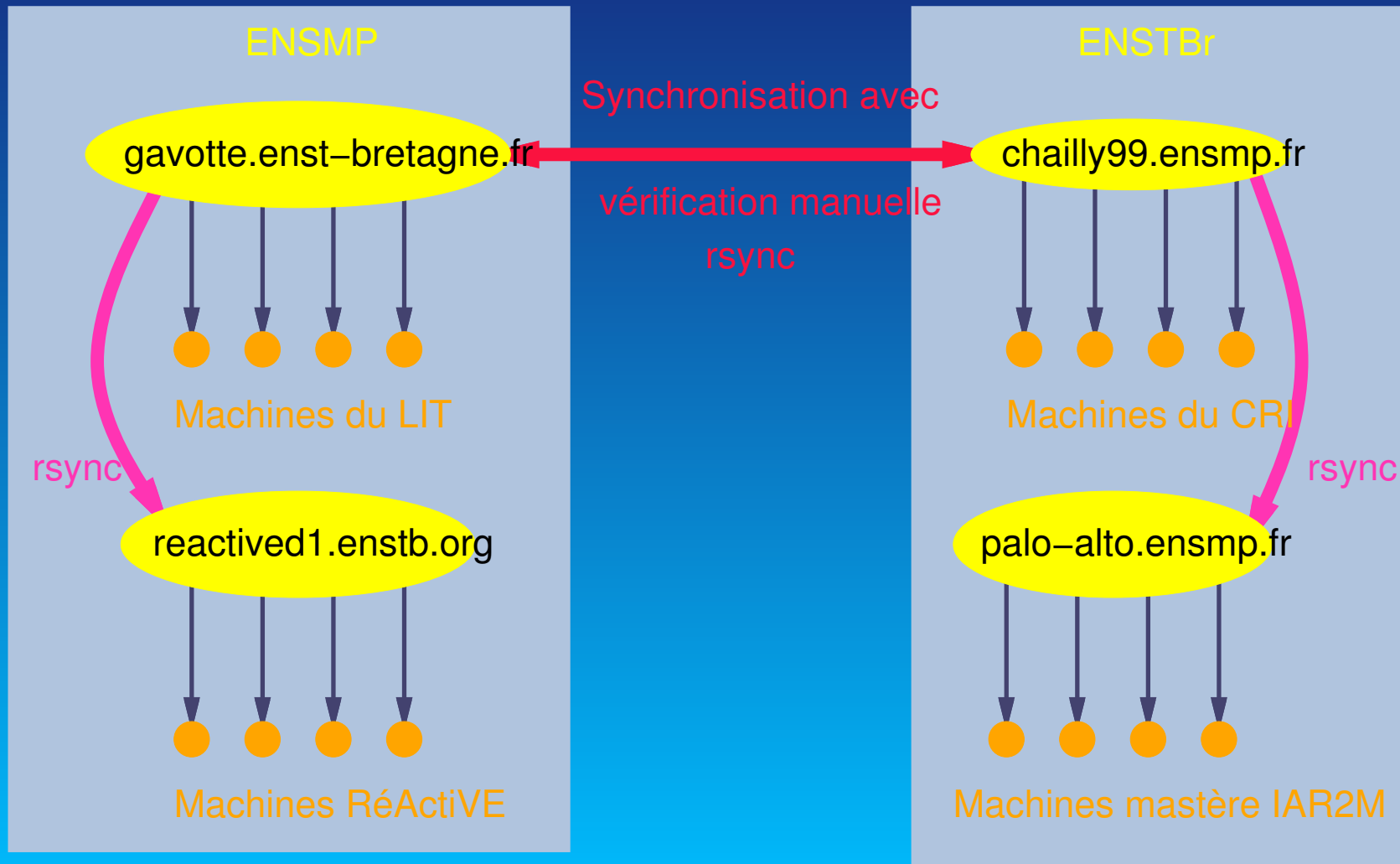


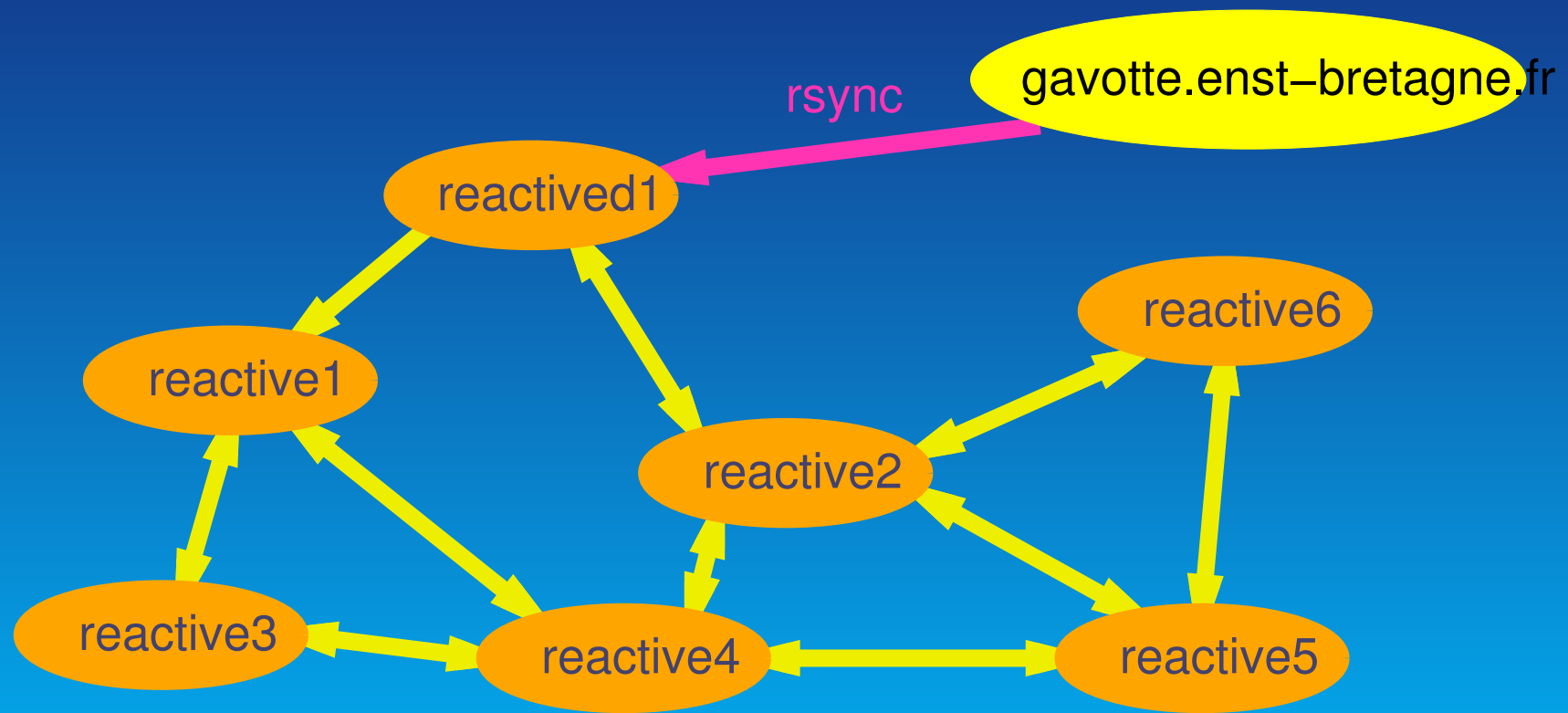
pannes (ne pas utiliser par exemple de RAID matériel si on peut mettre plusieurs machines pour faire un serveur NFS redondant) car cela permet de tirer profit du seul matériel existant

- utiliser un système de sauvegarde en réseau pour sauvegarder chaque nuit toutes les informations sensibles (en utilisant ici le logiciel libre AMANDA pour éviter, entre autres, de payer des licences par machine sauvegardées)

Viable \leadsto Mise en place de l'automatisation du système







Installation par vague



Tout est dans /usr/local/share :

cfengine : configuration de base de CFENGINE

cfengine.conf : se contente en fait d'inclure tous les fichiers du répertoire suivant

control:

```
# Where all the configuration files for cfengine are:
```

```
cf_directory = ( /usr/local/share/cfengine/cf )
```

import:

```
# Split things up to keep things tidy:
```

```
# The main file...
```

```
$(cf_directory)/main.cf
```

```
# and all the other files sorted by function:
```

```
$(cf_directory)/accounting.cf
```

```
$(cf_directory)/accounts.cf
```

```
$(cf_directory)/apache.cf
```

```
$(cf_directory)/automount.cf
```



```
$(cf_directory)/cfengine.cf  
$(cf_directory)/cron.cf  
$(cf_directory)/exportfs.cf  
$(cf_directory)/holidays.cf  
$(cf_directory)/localmounts.cf  
$(cf_directory)/logging.cf  
$(cf_directory)/minitel_access.cf  
$(cf_directory)/naming.cf  
$(cf_directory)/network.cf  
$(cf_directory)/ntp.cf  
$(cf_directory)/patch.cf  
$(cf_directory)/ppp_access.cf  
$(cf_directory)/printing.cf  
$(cf_directory)/sendmail.cf  
$(cf_directory)/solaris.cf  
$(cf_directory)/ssh.cf
```



`cfengine/cf` : fichiers de configurations rangés par fonction ou thème

`conf` : contient tous les fichiers de référence nécessaire à configurer correctement le système : description des imprimantes, fichiers réseaux, tables gérant le courrier,...

Rangement des choses par ordre d'application importante, puis par site, par système d'exploitation et enfin par répertoire de destination des fichiers à installer

`CRI` : fichiers généraux spécifiques au CRI

`etc` : ce qui va génériquement dans `/etc` ;

`linux` : spécifique à l'installation de LINUX, autre que les configurations d'application importante

`etc` : hiérarchie `/etc` spécifique à LINUX ;

`LIT` : fichiers généraux spécifiques au LIT ;



log : contient les informations sur les transferts multi-site du référentiel de configuration ou d'autres hiérarchies

- ▶ Améliore la traçabilité
- ▶ Permet aux administrateurs des différents sites de se tenir au courant des choses modifiées par l

mail : le nécessaire au bon fonctionnement du courrier électronique

ppp : fichiers spécifiques à un accès PPP ;

ssh : fichiers spécifiques à l'installation de ssh ;

Solaris : fichiers spécifiques à l'installation des machines sous SOLARIS hormis les configurations d'application importante ;

etc : hiérarchie /etc spécifique à SOLARIS ;

jumpstart : fichiers impliqués dans la procédure d'installation automatique de SOLARIS



fai : hiérarchie spécifique à l'installation de LINUX

Tout est géré via RCS pour laisser des traces (facile avec EMACS)

Pas CVS car importance des droits



```
# Sendmail installation and configuration.
```

```
# $Header: /usr/local/share/cfengine/cf/RCS/sendmail.cf,v 1.4 2001/11/14
```

```
groups:
```

```
mail_servers = ( gavotte.enstb.org smtp-cri.ensmp.fr )
```

```
copy:
```

```
solaris::
```

```
# Install directly the files from the server since
```

```
# sendmail is launched before automount.
```

```
# This adds also better fault tolerance.
```

```
/usr/local/sbin/sendmail
```

```
dest=/usr/lib/sendmail
```



```
type=byte  
define=RelaunchSendmail
```

```
/usr/local/sbin/editmap  
dest=/usr/sbin/editmap  
type=byte
```

```
/usr/local/sbin/makemap  
dest=/usr/sbin/makemap  
type=byte
```

```
/usr/local/sbin/mailstats  
dest=/usr/sbin/mailstats  
type=byte
```

```
/usr/local/sbin/praliases
```



```
dest=/usr/sbin/praliases  
type=byte
```

```
$(shared_conf)/mail/generic/helpfile  
dest=/etc/mail/helpfile  
owner=root group=root  
type=byte
```

```
$(shared_conf)/mail/generic/cf/cf/submit.cf  
dest=/etc/mail/submit.cf  
owner=root group=root  
type=byte
```

```
# The anti-spam database:  
$(shared_conf)/mail/$(site)/access.dir  
dest=/etc/mail/access.dir
```




```
owner=root group=root  
type=byte
```

```
$(shared_conf)/mail/$(site)/access.pag  
dest=/etc/mail/access.pag  
owner=root group=root  
type=byte
```

```
mail_servers::
```

```
$(shared_conf)/mail/$(site)/local-host-names  
dest=/etc/mail/local-host-names  
type=byte  
define=RelaunchSendmail
```

```
$(shared_conf)/mail/$(site)/server-$(os).cf  
dest=/etc/mail/sendmail.cf
```



```
type=byte
define=RelaunchSendmail

# Specific database to a full-fledged mail router:
$(shared_conf)/mail/$(site)/domaintable.dir
    dest=/etc/mail/domaintable.dir
    owner=root group=root
    type=byte

$(shared_conf)/mail/$(site)/domaintable.pag
    dest=/etc/mail/domaintable.pag
    owner=root group=root
    type=byte

$(shared_conf)/mail/$(site)/genericstable.dir
    dest=/etc/mail/genericstable.dir
```



```
owner=root group=root  
type=byte
```

```
$(shared_conf)/mail/$(site)/genericstable.pag  
dest=/etc/mail/genericstable.pag  
owner=root group=root  
type=byte
```

```
$(shared_conf)/mail/$(site)/mailertable.dir  
dest=/etc/mail/mailertable.dir  
owner=root group=root  
type=byte
```

```
$(shared_conf)/mail/$(site)/mailertable.pag  
dest=/etc/mail/mailertable.pag  
owner=root group=root
```



```
type=byte
```

```
$(shared_conf)/mail/$(site)/virtusertable.dir
```

```
dest=/etc/mail/virtusertable.dir
```

```
owner=root group=root
```

```
type=byte
```

```
$(shared_conf)/mail/$(site)/virtusertable.pag
```

```
dest=/etc/mail/virtusertable.pag
```

```
owner=root group=root
```

```
type=byte
```

```
!mail_servers::
```

```
$(shared_conf)/mail/$(site)/leaf-$(os).cf
```

```
dest=/etc/mail/sendmail.cf
```

```
type=byte
```

```
define=RelaunchSendmail
```



files:

solaris::

```
# The statistics file for sendmail:  
/etc/mail/statistics  
mode=644 owner=root group=bin  
action=touch
```

links:

solaris::

```
# Links for sendmail pseudo-commands:  
/usr/bin/hoststat ->! /usr/lib/sendmail  
/usr/bin/mailq ->! /usr/lib/sendmail  
/usr/bin/newaliases ->! /usr/lib/sendmail  
/usr/bin/purgetat ->! /usr/lib/sendmail
```



directories:

```
# Set sendmail mode and owner properly for security:
```

```
any::
```

```
  / owner=root mode=go-w
```

```
  /etc owner=root mode=go-w
```

```
  /etc/mail owner=root mode=go-w
```

```
  /usr owner=root mode=go-w
```

```
  /var owner=root mode=go-w
```

```
  /var/spool owner=root mode=go-w
```

```
  /var/spool/mqueue owner=root mode=go-w
```

```
  /var/spool/clientmqueue owner=smmssp group=smmssp mode=770
```

shellcommands:

```
RelaunchSendmail.solaris::
```



```
"/etc/init.d/sendmail stop"  
"/etc/init.d/sendmail start"
```

```
processes:
```

```
solaris::
```

```
# Start it anyway. More than 0 instance should run:
```

```
"sendmail"
```

```
matches=>0
```

```
restart "/etc/init.d/sendmail start"
```



- Centraliser des ressources de type fichiers (tables)
- Propagation à toutes les machines d'une entité
- Possibilité de changer un mot de passe
- Économie d'espace disque
- NIS, NIS+, LDAP, FNS,...
- Possibilité de modifier son mot de passe
- Tolérance aux pannes ?



- $\lim_{t \rightarrow \infty} \text{Prix du disque} = 0$
- CFENGINE a déjà l'infrastructure pour copier des fichiers \rightsquigarrow gratuit !
- Fichiers toujours locaux
 - ▶ Insensible à la coupure réseau
 - ▶ Éventuellement encapsulation d'un autre système de nommage sur la référence CFENGINE
 - ▶ Changements des systèmes de nommage ou des serveurs en douceur
 - ▶ \rightsquigarrow / tolérance aux pannes
 - ▶ Fin des problèmes pénibles
- Possibilité de changer un mot de passe ?
 - ▶ Se connecter au serveur de référence



- ▶ Emballer passwd, chsh, chfn,... :

```
ssh gros-server passwd
```

pour modifier le fichier de référence sur le serveur



- Propager systématiquement depuis la référence

copy:

solaris::

Set up the host file :

\$(shared_conf)/\$(site)/etc/hosts

dest=/etc/inet/hosts

type=byte

linux::

Set up the host file :

\$(shared_conf)/\$(site)/etc/hosts

dest=/etc/hosts

type=byte

any::



```
# Set up the ethers file :
$(shared_conf)/$(site)/etc/ethers
    dest=/etc/ethers
    type=byte

# Set up the netgroup file :
$(shared_conf)/$(site)/etc/netgroup
    dest=/etc/netgroup
    type=byte

$(shared_conf)/$(site)/$(os)/etc/passwd
    dest=/etc/passwd
    type=byte

$(shared_conf)/$(site)/$(os)/etc/shadow
    dest=/etc/shadow
```



```
type=byte
```

```
$(shared_conf)/$(site)/$(os)/etc/group
```

```
dest=/etc/group
```

```
type=byte
```



- Différencier temps installation et régime stationnaire

copy:

```
InstallationTime|!reference_server:
```

```
$(shared_conf)/$(site)/$(os)/etc/passwd
```

```
dest=/etc/passwd
```

```
type=byte
```

```
!InstallationTime.reference_server:
```

```
/etc/passwd
```

```
dest=$(shared_conf)/$(site)/$(os)/etc/passwd
```

```
type=byte
```

```
InstallationTime|!reference_server:
```

```
$(shared_conf)/$(site)/$(os)/etc/shadow
```

```
dest=/etc/shadow
```



```
type=byte
```

```
!InstallationTime.reference_server:
```

```
$(shared_conf)/$(site)/$(os)/etc/shadow
```

```
dest=/etc/shadow
```

```
type=byte
```

- Mais comment combiner ça avec un système de gestion de version ?

Cf. PCFENGINE



```
#!/bin/sh -vx
```

```
# Apply the normal cfengine config during FAI.
```

```
# $Header: /CVS/libre-intra/reactive/src/fai/client-config/scripts/LIT,v
```

```
# Run in verbose mode:
```

```
set -v -x
```

```
TARGET=/tmp/target
```

```
# At the end of the install, the future / is indeed in $TARGET,
```

```
# and / is only temporary during the installation.
```

```
UsrLocal=/usr/local
```

```
TempUsrLocal=$TARGET$UsrLocal
```




```
# Since there is no running automount yet, no NIS, no DNS,...:
mkdir -p $TempUsrLocal/share/cfengine $TempUsrLocal/share/conf
# Use the copy from reactived1 :
mount -t nfs 192.168.70.12:/usr/local/share/cfengine \
    $TempUsrLocal/share/cfengine
mount -t nfs 192.168.70.12:/usr/local/share/conf \
    $TempUsrLocal/share/conf

cp /usr/bin/cfengine $TARGET/usr/bin/cfengine
# Make cfengine believe it is really in / instead of $TARGET:
chroot $TARGET cfengine -v -DInstallationTime \
    -f $UsrLocal/share/cfengine/cfengine.conf

# Clean up the mounting points since it will be recreated
# by autofs anyway:
umount $TempUsrLocal/share/cfengine $TempUsrLocal/share/conf
```



```
# Run in verbose mode:
set -v -x
# At the end of the install, the future / is indeed in /a,
# and / is only temporary during the installation.
UsrLocal=/usr/local
TempUsrLocal=/a$UsrLocal
# Since there is no running automount yet, no NIS, no DNS,...:
/bin/mkdir -p $TempUsrLocal
/usr/sbin/mount -F nfs 192.44.75.87:/export/calice1/local $TempUsrLocal
# Disable the autoshutdown:
/usr/bin/touch /a/noautoshutdown
# Make cfengine believe it is really in / instead of /a:
/usr/sbin/chroot /a $UsrLocal/sbin/cfagent -v -DInstallationTime \
    -f $UsrLocal/share/cfengine/cfengine.conf
# Clean up the mounting point since it will be recreated by autofs anyway:
```



```
/usr/sbin/umount $TempUsrLocal  
rmdir $TempUsrLocal
```



Actuellement

- Langage avec syntaxe spécifique
- Pas un langage dans le sens de la programmation
- Peu extensible (nouvelles actions ?)
- Choses complexes : `shellcommands` extérieurs ou modules



- Projet de recherche au LIT dans le cadre de RÉACTIVE, 2 élèves 3A à partir de janvier 2002
- Faire un CFENGINE directement dans un vrai langage orienté objet interprété
 - ▶ Fichier de paramétrage directement écrit dans ce langage
 - ▶ Structures de données du langage \equiv structures de données de PCFENGINE
 - ▶ Utilisation de l'héritage multiple pour construire de nouvelles actions
 - ▶ `copyedit`
 - ▶ Copie depuis plusieurs répertoire (du plus précis au moins précis)
 - ▶ Gestion directe de la distribution auto-montage, exportation NFS, redondance distribuée et `rsync`



- ▶ Améliorer d'ancienne (`resolve` à partir d'`edit`)
- ▶ Gérer les fichiers modifiés par un système de gestion de versions
- ▶ ...
- ▶ Itération sur des configurations (points-fixes), générations d'actions à la volée,... \rightsquigarrow configuration de plus haut niveau, plus compacte
- ▶ Portabilité intrinsèque assurée par le langage de haut niveau
- Utilise un langage existant courant adapté au système : `perl` ou `Python` \rightsquigarrow `Python CFENGINE`

¿ Encore un autre langage à apprendre ?



- Instrumentation du code CFENGINE par patch pour en faire un compilateur vers du PCFENGINE (économie de l'analyseur lexical et grammatical)
- Parties pénibles de CFENGINE et non fondamentales : sous-traitance par PCFENGINE avec traduction en CFENGINE et mise à jour des classes avant et après
- Possibilité aussi d'utiliser PCFENGINE comme un module de CFENGINE



- Automatisation administration système (installation et routine)
- Fichiers de configuration centralisés
- Excellents concepts : classes de machines, règles simples
- Logiciel libre GNU
- Existe sous UNIX et NT
- J'attends vos contributions pour PCFENGINE ☺

<http://www.cfengine.org>



Liste des transparents

Introduction

- 1 Introduction
- 2 Cadre
- 3 Installation automatique
- 4 Plan
- 5 Cfengine

Cfengine

- 8 Composants constituant Cfengine
- 10 La classe !

La classe !

- 11 Classes « matérielles »
- 12 Classes « utilisateur »
- 14 Variables

Variables

- 16 Actions

Actions

- 17 Exemple d'action
- 18 Actions de contrôle
- 19 Actions contrôlant les fichiers
- 26 Actions contrôlant les processus
- 28 Actions de type macros
- 29 Actions de configuration de réseau
- 30 Actions de configuration des disques
- 31 Chef d'orchestre :séquence d'actions
- 33 Hypothèses

Mise en 1œuvre

- 35 Autres hypothèses liées à l'usage du système
- 37 Réplication des référentiels
- 38 Architecture du réseau RéActiVE

De l'utilisation de CFENGINE —PCFengine—



39 Structure du référentiel

44 Installation de sendmail 8.12

54 Système de nommage

Système de nommage

55 NIS, NIS+, LDAP, FNS,... cfengine !

57 Propagation des fichiers

60 Mise à jour depuis fichiers classiques

62 Inclusion dans la FAI GNU/Linux/Debian

Bootstrap du système

64 Inclusion dans le Solaris JumpStart

66 Existe-t-il une vie après Cfengine ?

PCFengine

67 PCFengine

69 Compatibilité avec Cfengine

70 Conclusion

71 Table des matières

