

Mutualisation de la configuration de postes de travail GNU/Linux dans un environnement multi départements

Manuel Sabban

JRES

Sommaire

- 1 Motivation et besoins des usagers
 - Présentation de Télécom ParisTech
 - Missions et contraintes
- 2 Bcfg2
 - Installation du système d'exploitation
 - Choix de bcfg2
 - Configuration de bcfg2
- 3 Virtualisation
 - Motivations
 - Distribution pair-à-pair
- 4 Conclusion

Sommaire

- 1 Motivation et besoins des usagers
 - Présentation de Télécom ParisTech
 - Missions et contraintes
- 2 Bcfg2
 - Installation du système d'exploitation
 - Choix de bcfg2
 - Configuration de bcfg2
- 3 Virtualisation
 - Motivations
 - Distribution pair-à-pair
- 4 Conclusion

Télécom ParisTech, école d'ingénieurs

Télécom ParisTech

- Quatre départements scientifiques
- Une division des systèmes d'information
- Personnel informatique des départements scientifiques en cours d'intégration à la DSI
- 1400 élèves
- Environ 250 postes sous GNU/Linux répartis en 15 salles de TP équipées en ordinateurs
- Environ 120 stations de travail sous GNU/Linux

Sommaire

- 1 Motivation et besoins des usagers
 - Présentation de Télécom ParisTech
 - Missions et contraintes
- 2 Bcfg2
 - Installation du système d'exploitation
 - Choix de bcfg2
 - Configuration de bcfg2
- 3 Virtualisation
 - Motivations
 - Distribution pair-à-pair
- 4 Conclusion

Missions et contraintes

Mission

- Gestion de station de salle de TP
- Gestion station de travail pour les personnels
- Répondre aux évolutions des besoins

État initial

Configuration logicielle hétérogène

Objectifs

- environnement stable pour ne pas dérouter les utilisateurs
- minimisation des coûts d'exploitation
- matériel hétérogène

Sommaire

- 1 Motivation et besoins des usagers
 - Présentation de Télécom ParisTech
 - Missions et contraintes
- 2 Bcfg2
 - Installation du système d'exploitation
 - Choix de bcfg2
 - Configuration de bcfg2
- 3 Virtualisation
 - Motivations
 - Distribution pair-à-pair
- 4 Conclusion

Procédure d'installation

Boot en PXE

Utilisation de l'installeur Debian en mode non interactif

Configuration des postes en utilisant bcfg2

Procédure d'installation

Boot en PXE

Utilisation de l'installeur Debian en mode non interactif

Configuration des postes en utilisant bcfg2

Procédure d'installation

Boot en PXE

Utilisation de l'installeur Debian en mode non interactif

Configuration des postes en utilisant bcfg2

Sommaire

- 1 Motivation et besoins des usagers
 - Présentation de Télécom ParisTech
 - Missions et contraintes
- 2 Bcfg2
 - Installation du système d'exploitation
 - Choix de bcfg2
 - Configuration de bcfg2
- 3 Virtualisation
 - Motivations
 - Distribution pair-à-pair
- 4 Conclusion

Choix de bcfg2

Choix effectué en juin 2006 à l'échelle d'un département

- python (compétences disponibles)
- XML simple

Solution généralisée en 2010 à la DSI

Choix de bcfg2

Choix effectué en juin 2006 à l'échelle d'un département

- python (compétences disponibles)
- XML simple

Solution généralisée en 2010 à la DSI

Bcfg2 et les autres logiciels majeurs de gestion de configuration

FAI

Logiciel d'installation automatisé

- Gestion de la procédure de boot
- Partitionnement et formatage
- Installation des paquetages
- Personnalisations

Pas de gestion des mises à jour à l'époque, cela ne correspondait pas à notre besoin

Bcfg2 et les autres logiciels majeurs de gestion de configuration

Puppet

- fonctionnalités similaires
- Gère aussi la configuration de windows (pas à l'époque)
- Ruby, mais pas de compétence
- Problème de stabilité (à l'époque)

cfengine2

- fonctionnalités similaires
- configuration jugée compliquée (à l'époque)

Bcfg2 et les autres logiciels majeurs de gestion de configuration

Puppet

- fonctionnalités similaires
- Gère aussi la configuration de windows (pas à l'époque)
- Ruby, mais pas de compétence
- Problème de stabilité (à l'époque)

cfengine2

- fonctionnalités similaires
- configuration jugée compliquée (à l'époque)

Sommaire

- 1 Motivation et besoins des usagers
 - Présentation de Télécom ParisTech
 - Missions et contraintes
- 2 Bcfg2
 - Installation du système d'exploitation
 - Choix de bcfg2
 - Configuration de bcfg2
- 3 Virtualisation
 - Motivations
 - Distribution pair-à-pair
- 4 Conclusion

Bcfg2 : Généralités

Principe

La philosophie de Bcfg2 est de décrire précisément l'état souhaité pour chaque machine et d'effectuer les opérations nécessaires pour arriver à cet état. La spécification se découpe en trois parties utilisant une syntaxe XML simple.

Architecture

Une installation de Bcfg2 consiste en :

- un serveur comprenant une description de tous les clients
- un ensemble de postes utilisant le client Bcfg2

Les communications entre le client et le serveur sont chiffrées et le serveur authentifié.

Bcfg2 : Généralités

Principe

La philosophie de Bcfg2 est de décrire précisément l'état souhaité pour chaque machine et d'effectuer les opérations nécessaires pour arriver à cet état. La spécification se découpe en trois parties utilisant une syntaxe XML simple.

Architecture

Une installation de Bcfg2 consiste en :

- un serveur comprenant une description de tous les clients
- un ensemble de postes utilisant le client Bcfg2

Les communications entre le client et le serveur sont chiffrées et le serveur authentifié.

Bcfg2 : Généralités

Principe

La philosophie de Bcfg2 est de décrire précisément l'état souhaité pour chaque machine et d'effectuer les opérations nécessaires pour arriver à cet état. La spécification se découpe en trois parties utilisant une syntaxe XML simple.

Architecture

Une installation de Bcfg2 consiste en :

- un serveur comprenant une description de tous les clients
- un ensemble de postes utilisant le client Bcfg2

Les communications entre le client et le serveur sont chiffrées et le serveur authentifié.

Bcfg2 : Le serveur

Le serveur bcfg2

- un fichier de configuration (certificats, activations des plugins)
- une « arborescence » de configuration, /srv/bcfg2 versionnée par mercurial pour nous.

Ressource utilisée

Il s'agit d'une machine virtuelle OpenVZ.

Bcfg2 : Le client

Le client bcfg2 se compose de :

- un fichier de configuration `/etc/bcfg2.conf` ;
- un exécutable.

Le client bcfg2

Il existe les modes interactifs, build, verbeux et déboguage.

Invocation

Nous l'exécutons une fois par jour par un cron (anacron) au même moment que la mise à jour quotidienne.

Bcfg2 : Généralités

La configuration se découpe en trois catégories :

Configuration

- Définition des méta-données
- Description formelle
- Description littérale

Bcfg2 : Généralités

La configuration se découpe en trois catégories :

Configuration

- Définition des méta-données
Définitions de profils et de groupes
- Description formelle
- Description littérale

Bcfg2 : Généralités

La configuration se découpe en trois catégories :

Configuration

- Définition des méta-données
- Description formelle
- Description littérale

Bcfg2 : Généralités

La configuration se découpe en trois catégories :

Configuration

- Définition des méta-données
- Description formelle
Définit ce qui compose la configuration
- Description littérale

Bcfg2 : Généralités

La configuration se découpe en trois catégories :

Configuration

- Définition des méta-données
- Description formelle
- Description littérale

Bcfg2 : Généralités

La configuration se découpe en trois catégories :

Configuration

- Définition des méta-données
- Description formelle
- Description littérale
Précise le contenu de la configuration

Définition des méta-données

Définition d'un bundle

Un ensemble cohérent et interdépendant de programmes, de services et de fichiers de configurations.

Définition d'un groupe

Un groupe est un ensemble hiérarchisé de groupes et de bundles.

Définition des méta-données

Un profil est associé à chaque machine.

Clients.xml

```
<Clients version="3.0">  
  <Client profile="tp_fc" name="fcmobile02.enst.fr"/>  
  <Client profile="tp" name="c124-03.enst.fr"/>  
  [...]  
</Clients>
```

Définition des méta-données

Un profil est associé à chaque machine.

Clients.xml

```
<Clients version="3.0">  
  <Client profile="tp_fc" name="fcmobile02.enst.fr"/>  
  <Client profile="tp" name="c124-03.enst.fr"/>  
  [...]  
</Clients>
```

Les groupes

Définition d'un groupe

```
<Group name="tp_fc" profile="true">  
  <Group name="basic"/>  
  <Bundle name="X11"/>  
  [...]  
</Group>
```

profil

On associe à chaque profil :

- Un ou plusieurs groupes
- Un ou plusieurs bundles

Les bundles

Bundle

```
<Bundle name='postfix' version='2.0'>  
  <Path name='/etc/postfix/main.cf' />  
  <Path name='/etc/postfix/generic' />  
  <Package name='postfix' />  
  <Action name='postmapalias' />  
  <Service name='postfix' />  
</Bundle>
```

Les probes

Les probes

C'est une affectation dynamique à un groupe.

Les probes

Ce sont des scripts qui renvoient `group:<nom du groupe dynamique>`

Les probes

Nous nous en servons pour tenir compte des spécificités matérielles

Les probes

Les probes

C'est une affectation dynamique à un groupe.

Les probes

Ce sont des scripts qui renvoient `group:<nom du groupe dynamique>`

Les probes

Nous nous en servons pour tenir compte des spécificités matérielles

Les probes

Les probes

C'est une affectation dynamique à un groupe.

Les probes

Ce sont des scripts qui renvoient `group:<nom du groupe dynamique>`

Les probes

Nous nous en servons pour tenir compte des spécificités matérielles

Les probes

Exemple de probe

```
#!/bin/sh
if which lspci >/dev/null 2>&1; then
    lspci -nmmd 10de: | uniq -f6 | \
    awk '($2=="\"0300\"" || $2=="\"0302\"")\
    {print "group:probe_nvidia"}'
fi
```

Utilisation des probes

Nous nous en servons pour détecter et prendre en compte le hardware

Exemple d'utilisation de probes

```
<Bundle name="X11" version='2.0'>  
  <Service name="mdm"/>  
  <Group name="probe_nvidia">  
    <Package name="nvidia-kernel-dkms"/>  
    [...]   
    <Path name="/etc/modprobe.d/nvidia.conf"/>  
  </Group>  
</Bundle>
```

Configuration formelle

Quatre types d'objets :

- Installation d'un paquet
- Chemin ou système de fichier (répertoire, lien, fichier ou permission)
- Démarrage d'un service
- Exécution d'une commande

Configuration formelle

Quatre types d'objets :

- Installation d'un paquet
- Chemin ou système de fichier (répertoire, lien, fichier ou permission)
- Démarrage d'un service
- Exécution d'une commande

Configuration formelle

Quatre types d'objets :

- Installation d'un paquet
- Chemin ou système de fichier (répertoire, lien, fichier ou permission)
- Démarrage d'un service
- Exécution d'une commande

Configuration formelle

Quatre types d'objets :

- Installation d'un paquet
- Chemin ou système de fichier (répertoire, lien, fichier ou permission)
- Démarrage d'un service
- Exécution d'une commande

Configuration littérale

Différents plugins que nous utilisons pour définir les actions associées à la configuration formelle

- Cfg
- Deb
- Rules
- SSHBase

Configuration littérale

Différents plugins que nous utilisons pour définir les actions associées à la configuration formelle

- Cfg
- Deb
- Rules
- SSHBase

Extension Cfg

Chaque fichier se trouve dans un répertoire qui porte son propre nom

Ce même répertoire est placé dans une arborescence analogue au système final

Exemple

Par exemple, pour le fichier `xorg.conf`. Cette configuration se trouve définie dans le répertoire `<config_dir>/Cfg/etc/X11/xorg.conf`

Extension Cfg

Chaque fichier se trouve dans un répertoire qui porte son propre nom

Ce même répertoire est placé dans une arborescence analogue au système final

Exemple

Par exemple, pour le fichier `xorg.conf`. Cette configuration se trouve définie dans le répertoire `<config_dir>/Cfg/etc/X11/xorg.conf`

Extension Cfg : exceptions

Exceptions

Des exceptions sont possibles :

- par groupes
- par machine identifiée par son nom FQDN

Il suffit de suffixer le fichier concerné correctement.

Extension Cfg : Génération par template

Template

Deux langages de templates sont possibles :

- cheetah (<http://cheetahtemplate.org/>)
- genshi (<http://genshi.edgewall.org/>)

Il suffit de suffixer le fichier concerné correctement.

Extension Cfg : Exemple

Exemple

```
$ pwd
/srv/bcfg2/Cfg/etc/X11/xorg.conf
$ ls
xorg.conf.H_c130-01.enst.fr
xorg.conf.H_c124-05.enst.fr
xorg.conf.G50_probe_nvidia
xorg.conf.cheetah
[...]
```

Gestion des paquets

Nous utilisons le driver apt car nous avons des machines debian.

Bcfg2 sait gérer de multiple distributions ou systèmes d'exploitations

```
[...]  
<Package name="nvidia-kernel-dkms" />  
[...]
```

Pas besoin de numéro de version sur les paquets

Gestion des paquets

Nous utilisons le driver apt car nous avons des machines debian.

Bcfg2 sait gérer de multiple distributions ou systèmes d'exploitations

```
[...]  
<Package name="nvidia-kernel-dkms" />  
[...]
```

Pas besoin de numéro de version sur les paquets

Gestion des paquets

Nous utilisons le driver apt car nous avons des machines debian.

Bcfg2 sait gérer de multiple distributions ou systèmes d'exploitations

```
[...]  
<Package name="nvidia-kernel-dkms" />  
[...]
```

Pas besoin de numéro de version sur les paquets

Rules

Tous les fichiers xml du répertoire `<config dir>/Rules` sont interprétés.

Quatre types de règles

- Répertoire
- Lien symbolique
- Permissions
- Service

Rules

Tous les fichiers xml du répertoire `<config dir>/Rules` sont interprétés.

Quatre types de règles

- Répertoire
- Lien symbolique
- Permissions
- Service

Rules

Exemple de «Rules»

```
<Rules priority="0">  
  <Path type='permissions' name="/usr/bin/pmount"  
    perms="4755" owner="root" group="plugdev"/>  
  <Service name="mdm" type="deb" status="on"  
    mode="default" target="reload"/>  
  <Action name='updategrub' timing='post'  
    when='modified' command='update-grub'  
    status='check'/>  
  <Path type='symlink' name="/usr/local/bin/tcsh"  
    to="/usr/bin/tcsh"/>  
</Rules>
```

SSHBBase

Deux utilités

- Maintenir `/etc/ssh_known_hosts`
- Générer un clef privée pour les nouvelles installations

Possibilité de renseigner `ssh_known_hosts` avec des clefs appartenant à des machines non gérés par bcfg2

Sommaire

- 1 Motivation et besoins des usagers
 - Présentation de Télécom ParisTech
 - Missions et contraintes
- 2 Bcfg2
 - Installation du système d'exploitation
 - Choix de bcfg2
 - Configuration de bcfg2
- 3 Virtualisation
 - Motivations
 - Distribution pair-à-pair
- 4 Conclusion

Windows et machines virtuelles

Besoins

- Windows pour des besoins pédagogiques
- Droits administrateur pour des besoins pédagogiques.

Cahier des charges

- Pas de solution à double démarrage
- Pas de répartition Windows et GNU/Linux des salles de TP
- Solution «user friendly»
- Licence assez permissive

Solution de virtualisation

Nous avons choisi VirtualBox

Windows et machines virtuelles

Besoins

- Windows pour des besoins pédagogiques
- Droits administrateur pour des besoins pédagogiques.

Cahier des charges

- Pas de solution à double démarrage
- Pas de répartition Windows et GNU/Linux des salles de TP
- Solution «user friendly»
- Licence assez permissive

Solution de virtualisation

Nous avons choisi VirtualBox

Windows et machines virtuelles

Besoins

- Windows pour des besoins pédagogiques
- Droits administrateur pour des besoins pédagogiques.

Cahier des charges

- Pas de solution à double démarrage
- Pas de répartition Windows et GNU/Linux des salles de TP
- Solution «user friendly»
- Licence assez permissive

Solution de virtualisation

Nous avons choisi VirtualBox

Sommaire

- 1 Motivation et besoins des usagers
 - Présentation de Télécom ParisTech
 - Missions et contraintes
- 2 Bcfg2
 - Installation du système d'exploitation
 - Choix de bcfg2
 - Configuration de bcfg2
- 3 Virtualisation
 - Motivations
 - Distribution pair-à-pair
- 4 Conclusion

Diffusion des images

Les images de machines virtuelles sont des fichiers binaires volumineux.

Bcfg2 n'est pas adapté pour répondre à ce besoin.

Solution

Nous utilisons donc bittorent.

Diffusion des images

Les images de machines virtuelles sont des fichiers binaires volumineux.

Bcfg2 n'est pas adapté pour répondre à ce besoin.

Solution

Nous utilisons donc bittorent.

Diffusion des images

Les images de machines virtuelles sont des fichiers binaires volumineux.

Bcfg2 n'est pas adapté pour répondre à ce besoin.

Solution

Nous utilisons donc bittorent.

Utilisation de bcfg2 pour .torrent

La mise à jour des machines virtuelles se fait donc automatiquement par bittorrent.

Serveur

```
cd /srv/vms/archives/VMcatalog/  
btmakemetabase.bittornado \  
http://nfs-vms.enst.fr:6969/announce <Dossier>
```

Client

Le fichier et le service torrent est lui géré par bcfg2.

Utilisation de bcfg2 pour .torrent

La mise à jour des machines virtuelles se fait donc automatiquement par bittorrent.

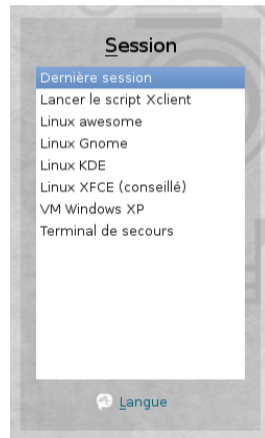
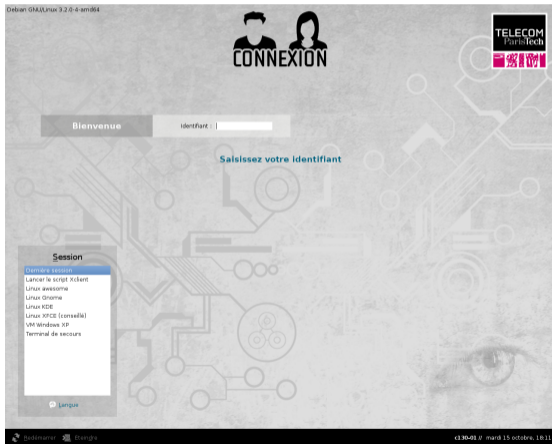
Serveur

```
cd /srv/vms/archives/VMcatalog/  
btmakemetafile.bittornado \  
http://nfs-vms.enst.fr:6969/announce <Dossier>
```

Client

Le fichier et le service torrent est lui géré par bcfg2.

Facilité d'utilisation



Conclusion

- configuration personnalisée des postes clients adaptée à leur utilisation (poste de bureau, poste de salles de travaux pratiques et postes pilotes d'instrumentation)
- possibilité d'utilisation de machines virtuelles en tant qu'administrateur
- possibilité d'utilisation de Windows en mode virtualisé
- facilement administrable et adaptable à un environnement avec beaucoup de besoins différents.
- la solution déployée est facilement transposable dans d'autres environnements dans la mesure où les personnalisations fines ne se font que dans les machines virtuelles.

Conclusion

- configuration personnalisée des postes clients adaptée à leur utilisation (poste de bureau, poste de salles de travaux pratiques et postes pilotes d'instrumentation)
- possibilité d'utilisation de machines virtuelles en tant qu'administrateur
- possibilité d'utilisation de Windows en mode virtualisé
- facilement administrable et adaptable à un environnement avec beaucoup de besoins différents.
- la solution déployée est facilement transposable dans d'autres environnements dans la mesure où les personnalisations fines ne se font que dans les machines virtuelles.

Conclusion

- configuration personnalisée des postes clients adaptée à leur utilisation (poste de bureau, poste de salles de travaux pratiques et postes pilotes d'instrumentation)
- possibilité d'utilisation de machines virtuelles en tant qu'administrateur
- possibilité d'utilisation de Windows en mode virtualisé
- facilement administrable et adaptable à un environnement avec beaucoup de besoins différents.
- la solution déployée est facilement transposable dans d'autres environnements dans la mesure où les personnalisations fines ne se font que dans les machines virtuelles.

Conclusion

- configuration personnalisée des postes clients adaptée à leur utilisation (poste de bureau, poste de salles de travaux pratiques et postes pilotes d'instrumentation)
- possibilité d'utilisation de machines virtuelles en tant qu'administrateur
- possibilité d'utilisation de Windows en mode virtualisé
- facilement administrable et adaptable à un environnement avec beaucoup de besoins différents.
- la solution déployée est facilement transposable dans d'autres environnements dans la mesure où les personnalisations fines ne se font que dans les machines virtuelles.

Conclusion

- configuration personnalisée des postes clients adaptée à leur utilisation (poste de bureau, poste de salles de travaux pratiques et postes pilotes d'instrumentation)
- possibilité d'utilisation de machines virtuelles en tant qu'administrateur
- possibilité d'utilisation de Windows en mode virtualisé
- facilement administrable et adaptable à un environnement avec beaucoup de besoins différents.
- la solution déployée est facilement transposable dans d'autres environnements dans la mesure où les personnalisations fines ne se font que dans les machines virtuelles.