GSP - Gestion supervision de parc

Introduction

Fabien Rico (fabien.rico@univ-lyon1.fr)

Univ. Claude Bernard Lyon 1

Séance 1

Introduction

- Contexte
  - parc important ;
  - plusieurs *type* d'installation ;
  - matériel hétérogène.
- Besoins :
  - installation de base : *provisionnement* ;
  - suivit et configuration : *orchestration* ;
  - surveillance : *supervision*.

Intervenants

- Christopher J. Lee : orchestration (puppet)
- Emmanuel Reuter : supervision

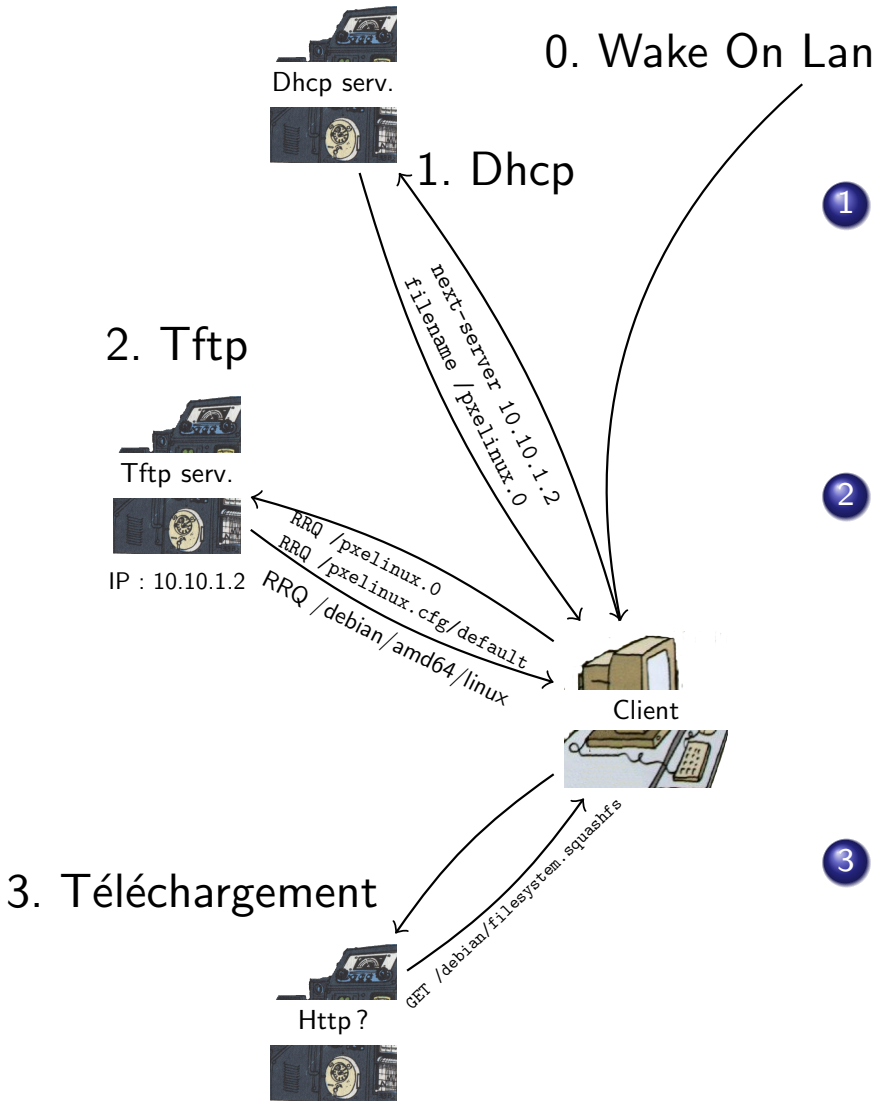
Démarrage réseau

C'est un outil de base pour commencer :

- machines sans aucun système ;
- machines à tester (démarrer sur un système de test) ;
- machines à réinstaller
- démarrage sans disque

Les outils d'installation centralisée sont souvent une interface graphique de configuration du démarrage réseau et des installeurs sans assistance (*unattended*).

Démarrage réseau



1. le serveur dhcp en plus des configurations réseaux fourni :
   - le nom du serveur tftp ;
   - le nom du fichier de boot à utiliser.
2. le client télécharge via TFTP :
   - l'image de *préboot* PXE ou EFI ;
   - la configuration de démarrage ;
   - le noyaux correspondant au choix de l'utilisateur.
3. le client télécharge le reste via un protocole plus évolué

Outils

Pour configurer le démarrage réseau, il faut :

- un serveur DHCP :
  - `isc-dhcp` ;
  - `dnsmasq`.
- un serveur TFTP :
  - `atftpd` ;
  - `tftpd-hpa` ;
  - `dnsmasq`.

dnsmasq

C'est un logiciel capable de fournir les services `DNS`, `tftp` et `dhcp`.

- demande peu de ressources,
- configuration simple et souple,
- dévellopé pour un petit réseau interne.

Il est utilisé par exemple :

- en salle TP réseau ;
- par `NetworkManager` sous ubuntu ;
- par `virtmanager` pour gérer les réseaux de machines virtuelles.

dnsmasq (configuration)

Le fichier /etc/dnsmasq.conf donne un exemple des configurations avec leur sens.
À chaque option du fichiers correspond une option. Par exemple

```
# fichier /etc/dnsmasq.conf
address=/machine.detournee.fr/127.0.0.1
# commande
dnsmasq ... --address "/machine.detournee.fr/127.0.0.1"
```

Attention, la popularité de dnsmasq fait qu'il y a souvent une instance exécutée sur votre machine, cela peut provoquer des conflit d'accès au port par exemple.

Options dnsmasq

- no−resolv : ne transfert pas les requêtes vers les serveurs dns du fichier resolv .conf
- server =/domain.fr/192.168.0.1 : transfert les requètes pour un domain particulier.
- address=/www.mondomain.fr/10.11.10.1 : un champs A
- bind−interfaces : n'ouvre de socket en écoute que sur certaines interfaces
- interface =eth0 ajoute eth0 aux interfaces écoutées
- dhcp−range=10.250.100.200,10.250.100.250,255.255.255.0,5m un ensemble d'adresses distribuables en dhcp
- dhcp−host=50:9a:4c:14:ef:4c, 10.250.100.90, prv3−a una adresse précise
- dhcp−boot=pxelinux.0 non du fichier à télécharger (le serveur est lui même par défaut)
- enable−tftp : ajoute le service tftp
- tftp −root=/var/tftp/ : la racine tftp

Options
tt dnsmasq

Lorsque dnsmasq gère plusieurs réseau, il faut utiliser les tag :

```
# définition d'une range sur le réseau privé
dhcp-range=set:prive,10.250.100.200,10.250.100.250,\
           255.255.255.0,5m
# définition d'un host sur le réseau privé
# et géré par FOG
dhcp-host=set:fogguee,set:prive,50:9a:4c:14:ef:4c,\
          10.250.100.90,prv3-a
#
# définition d'une route pour le réseau privé
dhcp-option=tag:prive,121,10.250.0.0/16,10.250.100.1
# définition d'une route par défaut
# uniquement pour les machines gérées
# par FOG
dhcp-option=tag:fogguee,option:router,10.250.100.3
```

Boot PXE

C'est la vielle version de boot, elle n'est pas compatible UEFI et il faut donc désactiver l'UEFI dans les configurations de démarrage.
Le système est proche de l'ancien bootloader *lilo*, on définie des labels correspondant à un démarrage possible :

```
label mybootentry1
  kernel rescue32
  append initrd=initram.igz ethx=192.168.157.100 \
         netboot=http://192.168.157.1:8080/sysrcd.dat

label mybootentry2
  kernel rescue64
  append initrd=initram.igz dodhcp \
                netboot=nbd://192.168.157.1:2000
```

le noyaux doit être trouvé dans les fichiers PXE du système qui vous intéresse et les options dépendent du noyau. Il est donc important de suivre le tutoriel propre à la distribution visée.

Exemple pris sur `http://www.system-rescue-cd.org/manual/PXE_network_booting/`

Démarrag UEFI

Nouvelle version compatible UEFI, la configuration du bootloader est proche de celle de grub

```
function load_video {
insmod efi_gop
insmod efi_uga
insmod video_bochs
insmod video_cirrus
insmod all_video
}

load_video
set gfxpayload=keep
insmod gzio

menuentry 'Install Fedora 64-bit' --class fedora --class gnu-linux \
  --class gnu --class os {
   linuxefi f26/vmlinuz ip=dhcp \
   inst.repo=http://mon.serveur.fr/x86_64/os/
   initrdefi f26/initrd.img
}
```

Exemple pris sur

https://docs-old.fedoraproject.org/en-US/Fedora/26/html/Installation_Guide/pxe-bootloader.html

Installation unnattended

C'est une installation sans intervention humaine :

- une véritable installation
- les réponses au questions sont préremplient dans un fichier ou une base de données.

A cause de cela :

- C'est long.
- C'est difficile à tester.
- L'évolution est difficile.
+ C'est souple d'utilisation.
+ Cela s'adapte sur tous les matériel.

L'intéret de tel système est d'installer sur une machine neuve un système de base stable, utilisable dans le réseau.

Outils unnatended

Chaque système/distribution gère ses propres outils de déploiement :

- RedHat/Fedora utilise *kickstart*.
- Debian/Ubuntu utilise *preseed*.
- Windows semble utiliser *ADK*.

Fichier kickstart

```
#platform=x86, AMD64, ou Intel EM64T
#version=DEVEL
# Install OS instead of upgrade
install
# Keyboard layouts
keyboard 'fr'
# Root password
rootpw --plaintext toto
# Use network installation
url --url="http://mon.serveur.fr/distrib/"
# System language
lang fr_FR
# Firewall configuration
firewall --disabled
# Reboot after installation
reboot
# System timezone
timezone Europe/Paris
# Network information
network  --bootproto=dhcp --device=eth0
# System authorization information
auth  --useshadow  --passalgo=sha512
# Use graphical install
graphical
firstboot --disable
# SELinux configuration
selinux --disabled

# System bootloader configuration
bootloader --location=mbr
# Partition clearing information
clearpart --linux

%packages
@gnome-desktop

%end
```

Fichier preseed

```
#### Network configuration.
d-i   netcfg/choose_interface            select auto
d-i   netcfg/get_hostname                string host1
d-i   netcfg/get_domain                  string mondomain.fr
#### Mirror settings.
d-i   mirror/country                     string enter information manually
d-i   mirror/http/hostname               string ftp.de.debian.org
d-i   mirror/http/directory              string /debian
d-i   mirror/suite                       string sarge
d-i   mirror/http/proxy                  string http://mainframe.athome:3128/
### Partitioning.
# If the system has free space you can choose to only partition that space.
d-i partman-auto/init_automatically_partition \
    select Use the largest continuous free space
# You can choose from any of the predefined partitioning recipes:
d-i partman-auto/choose_recipe          select Desktop machine
d-i partman/confirm_write_new_label      boolean true
d-i partman/choose_partition             select \
    Finish partitioning and write changes to disk
d-i partman/confirm                      boolean true
#### Boot loader installation.
d-i   grub-installer/only_debian         boolean true
d-i   grub-installer/with_other_os       boolean true
##### Finishing up the first stage install.
# Avoid that last message about the install being complete.
d-i   prebaseconfig/reboot_in_progress   note
##### Preseeding base-config.
base-config   base-config/intro          note
base-config   base-config/login          note
###### Account setup.
# To preseed the root password, you have to put it in the clear in this file
passwd passwd/root-password              password r00tme
passwd passwd/root-password-again        password r00tme
# Alternatively, you can preseed the user's name and login.
passwd passwd/user-fullname              string Holger Levsen
passwd passwd/username                   string hl
passwd passwd/user-password              password insecure
passwd passwd/user-password-again        password insecure
###### Apt setup.
base-config   apt-setup/uri_type         select http
base-config   apt-setup/country          select enter information manually
base-config   apt-setup/hostname         string ftp.de.debian.org
base-config   apt-setup/directory        string /debian
base-config   apt-setup/another          boolean false
ase-config apt-setup/non-free          boolean true
base-config apt-setup/contrib           boolean true
base-config   apt-setup/security-updates boolean true
###### Package selection.
# You can choose to install any combination of tasks that are available.
tasksel       tasksel/first    multiselect Desktop environment
```

Méthodes d'installation

- Clonages de disque
  - \+ simple ;
  - \+ rapide ;
  - \- créent des clones.
- Installations *unattended*
  - \- complexe ;
  - \- lent ;
  - \+ c'est une installation.

Clonage de dique

- Méthode
  - Installation d'un système modèle.
  - Récupération de l'image du disque.
  - Déployement du système sur tous les postes.
- Logiciel :
  - Norton Ghost (historique)
  - Clonezilla
  - FOG
- Une source et N clients : possibilité de multicast.

Fonctionnalité des logiciels de clonage

- Démarrage sur le réseau.
- Inventaire.
- Gestion des images en fonction de groupes.
- Modification mineur du système installé (licences, carte réseau...).
- Installation en multicast.
- Capable de lire les partitions.
- Gestion totalement à distance :
  - *Wake on Lan*.
  - Utilisation de système live pour les tests.
  - ...

Intéret du clonage

Toute la technique est dans l'installation d'une seule machine.

- Installation de base.
- Correstion des problèmes.
- Test.
- Réplication.

Exemple des cartes réseau en salle TPR.

Coût du clonage

Les système de clonage demande des postes identiques :

- Difficulté de gestion des « exception » :
  - pas de remplacement de pièces par un équivalent ;
  - pas de remplacement d'un seul poste.
- Achat en lot.
- Nécessité de *spare*.
- Durée de vie limitée.

Cela demande des achat réguliers et importants.

Un exemple de clonage : les images de Machines Virtuelles

Les machines virtuelles sont très adaptée au clonage :

- Le matériel est toujours identique.
- Il est difficile de gérer les installation (console à distance...).
- Il est facile de cloner les disques.
- Le clonage permet le Copy on Write.

Les images de machines virtuelles sont des copie de disques avec (parfois) un script de démarrage pour adapter la nouvelle machine à sont environnement :

- expansion des disques ;
- effacement des mots de passe ;
- récupération du nom, de clef d'accès ...

Installation automatique

Logiciels capables de configurer les différents services pour gérer l'installation *unattended*

- démarrage réseau ;
- gestion des distributions ;
- modèles de fichiers *unattended*

Tout est paramétrable à partir des modèles et de variables. Mais :

- il faut maitriser la configuration des fichiers *unattended* ;
- comme c'est une installation les tests sont longs ;

Foreman

C'est un logiciel web permettant l'installation

- Il peut être associé à des logiciels d'orchestration pour gérer les configurations (puppet, ansible, ...)
- Il dispose d'une interface de supervision.
- Propose de nombreux *plugins* :
  - gestion d'interface cloud (Amazon EC2, openstack, ...)
  - faire l'inventaire des postes
  - ...

Fonctionnement

Il a 2 grandes partie :

- Le cœur avec l'interface web, la base de données...
- Le ou les *smart proxy* qui sont les agents distants capables de récolter et transférer des informations au postes administrés.
  - Ils fournissent les services de base (DNS, DHCP, TFTP, ...)
  - Ils peuvent utiliser différents logiciels (isc-dhcp, dnsmasq ...)
  - Ils doivent être proche des machines administrées.
  - Ils sont authentifié par des certificat X509.

Attention, qui dit certificat dit importance du nommage des machines. *Si on change le nom du serveur, il est plus simple de réinstaller complètement foreman*.