Min2RIEN

Outils libres pour la gestion d'un parc de machines sous macOS

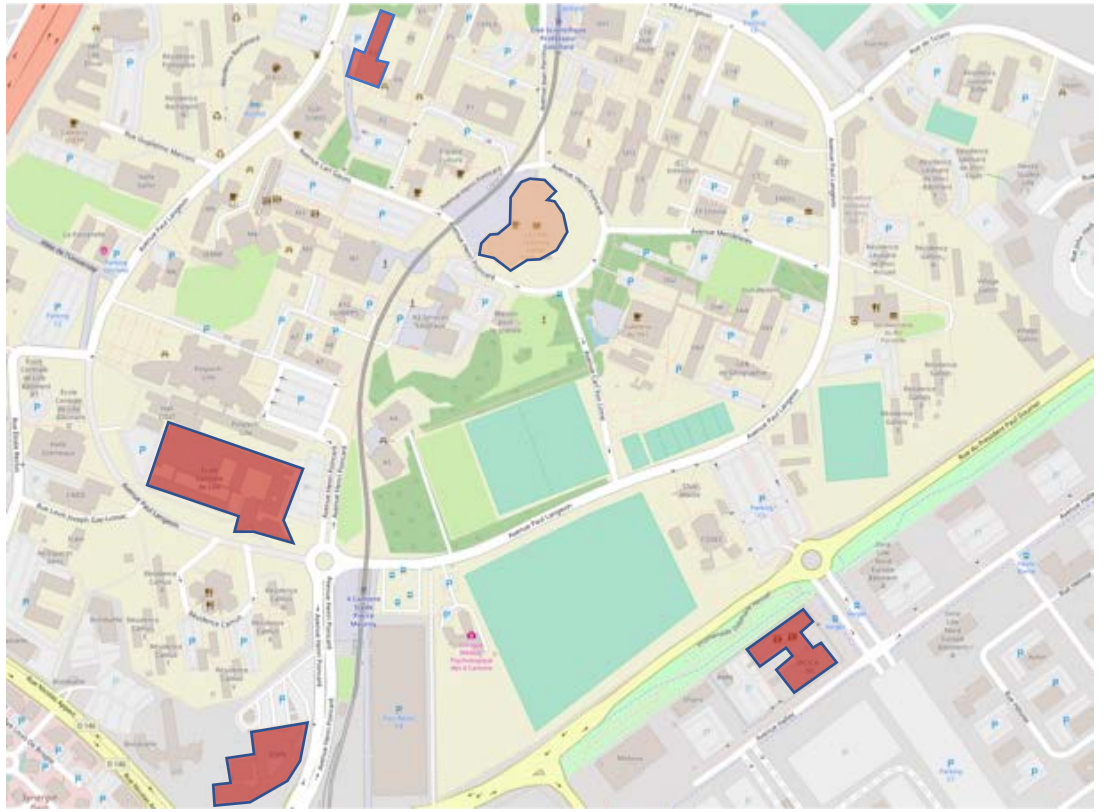
Mickaël Masquelin | iemn

25 Janvier 2018

cnrs ISEN ALL IS DIGITAL! LILLE yncréa Université de Valenciennes et du Hainaut-Cambrésis centralelille ÉCOLE CENTRALE DE LILLE Université de Lille RENATECH

Quelques mots sur le laboratoire …

- Unité Mixte de Recherche
- 5 tutelles :
  - Le CNRS
  - L'Université de Lille
  - L'Université de Valenciennes
  - L'Ecole Centrale
  - Le groupe YNCREA – ISEN
- 6 sites géographiquement distants
- Environ 500 personnes (chercheurs, ingénieurs, administratifs, étudiants, …)



Les environnements des postes clients à l'IEMN

Sur le site du LCI, un peu moins de 1 500 objets connectés au LAN ou au Wi-Fi.

Les objectifs ?

Les objectifs ?

AVOIR UNE VUE D'ENSEMBLE SUR LES SOLUTIONS DE GESTION DE PARC EXISTANTES

L'idée est de voir qu'il existe un tas d'outils, propriétaires ou libres, pour les administrateurs systèmes et réseaux et de vous donner quelques pointeurs sur ces solutions …

Les objectifs ?

AVOIR UNE VUE D'ENSEMBLE SUR LES SOLUTIONS DE GESTION DE PARC EXISTANTES

L'idée est de voir qu'il existe un tas d'outils, propriétaires ou libres, pour les administrateurs systèmes et réseaux et de vous donner quelques pointeurs sur ces solutions …

ESSAYER DE VOUS DONNER QUELQUES PISTES

J'espère que vous repartirez de la journée thématique avec pleins d'idées, des envies de changer la manière dont vous fonctionnez chez vous pour gérer certaines choses vis-à-vis de l'écosystème Apple, …

Les objectifs ?

AVOIR UNE VUE D'ENSEMBLE SUR LES SOLUTIONS DE GESTION DE PARC EXISTANTES

L'idée est de voir qu'il existe un tas d'outils, propriétaires ou libres, pour les administrateurs systèmes et réseaux et de vous donner quelques pointeurs sur ces solutions …

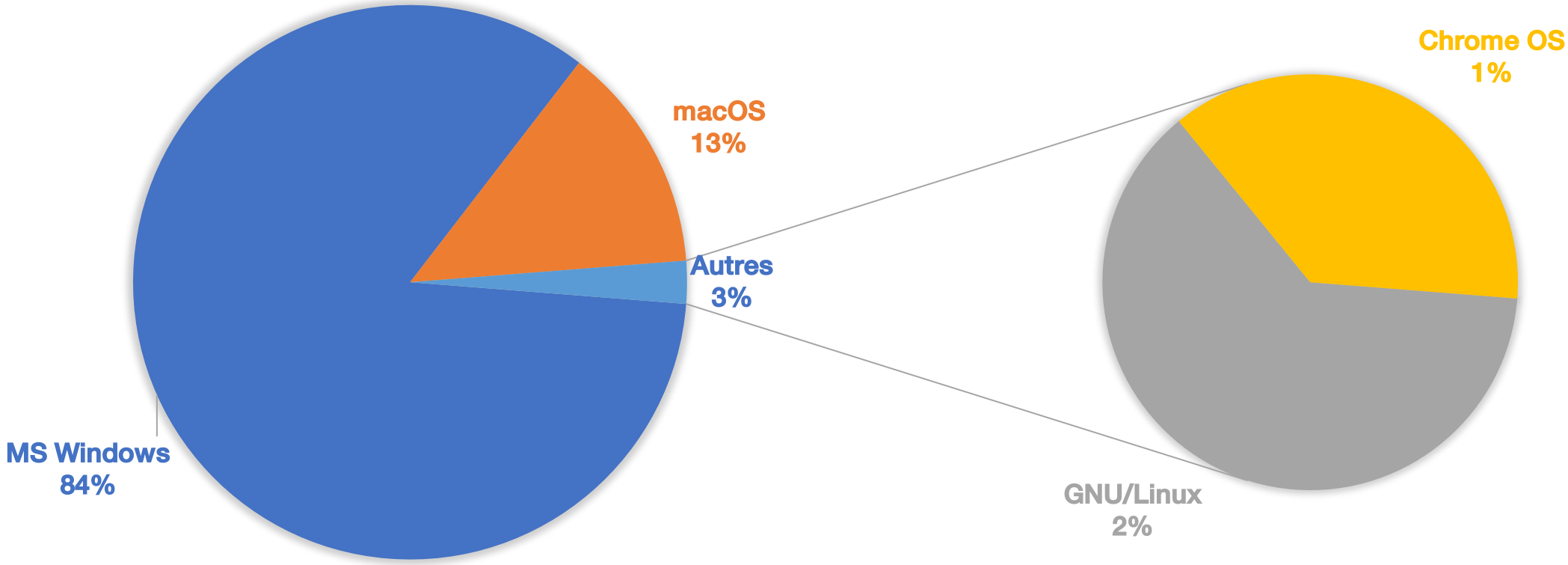
ESSAYER DE VOUS DONNER QUELQUES PISTES

J'espère que vous repartirez de la journée thématique avec pleins d'idées, des envies de changer la manière dont vous fonctionnez chez vous pour gérer certaines choses vis-à-vis de l'écosystème Apple, …

ESSAYER DE VOUS CONVAINCRE QU'UN MAC N'EST PAS FORCEMENT QU'UN OBJET DE LUXE …

On va essayer d'éviter les trolls Apple svp ☺

Le poste de travail en France



Source : étude ZDNet.fr (décembre 2017)

Apple de plus en plus présent dans nos structures

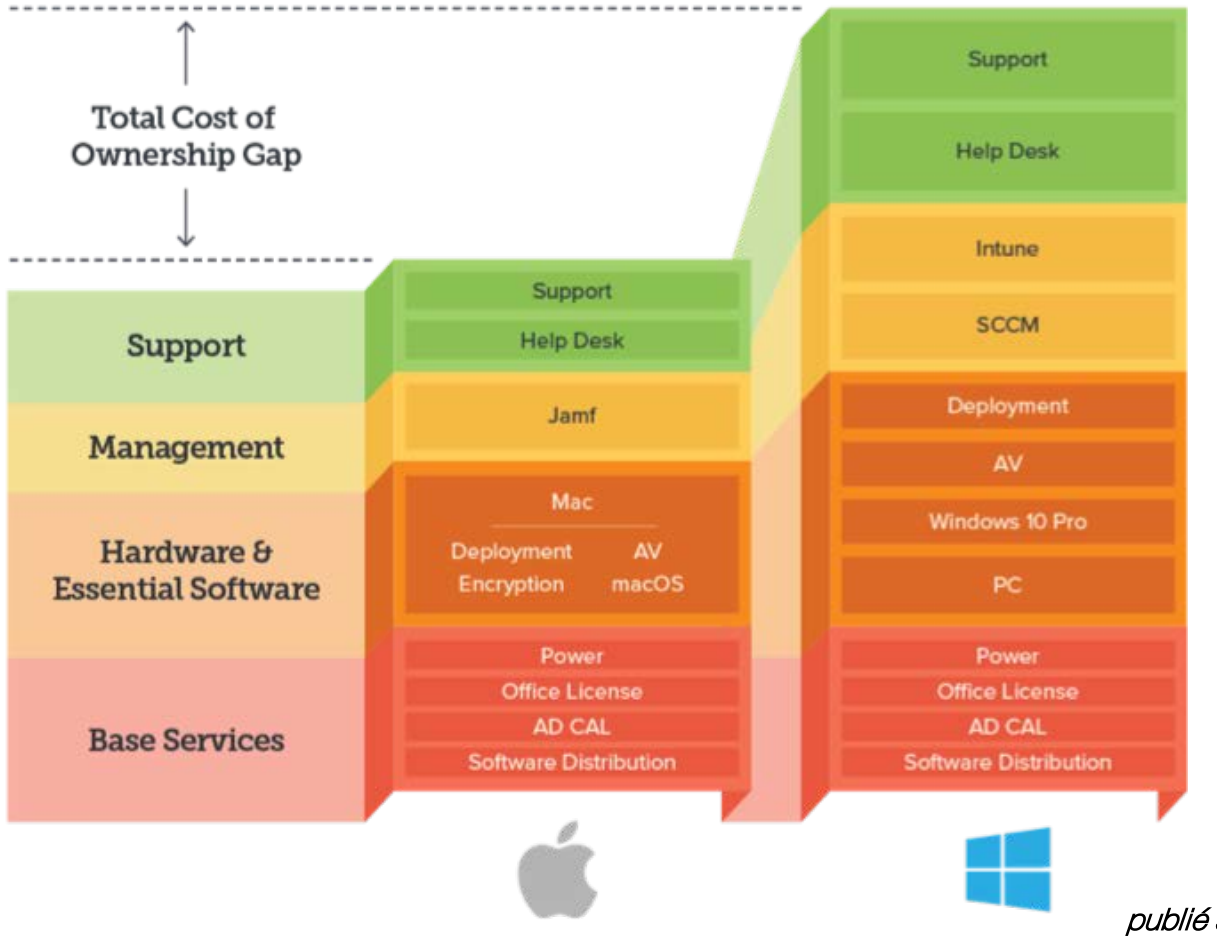
Un ordinateur Apple c'est …

Au départ :

Surcoût à l'achat évalué entre 117$ et 454 $

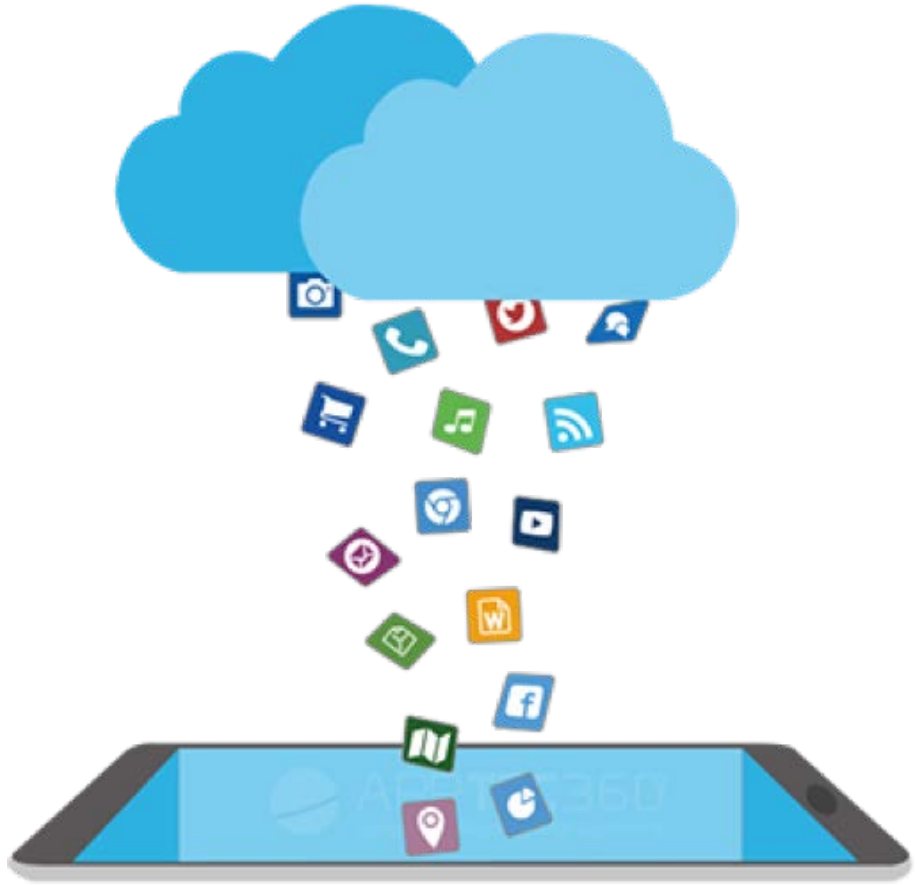
A l'arrivée :

Economie évaluée entre 273$ et 543$ sur 4 ans.



Source : article de Nick Thomson publié sur le blog jamf le 25 janvier 2017

Deux types de solutions pour les environnements Apple



Les solutions de déploiement

- Pour les clients macOS :
  - Outils Apple fourni avec macOS Server (NetInstall, …) ;
  - DeployStudio (gratuit) ;
  - DELL KACE (payant) ;
  - Casper Suite de JAMF Sotfware (payant) ;
  - Client Management Suite de Symantec (payant) ;

… et toutes les solutions de MDM …

La gestion des applications

- Pour les clients macOS / iOS :

  - AppStore d'Apple (payant) ;
  - Suite Symantec (payante) ;
  - JAMF Pro (payant) ;
  - Kiosk de FileWave (payant) ;
  - Ivanti EndPoint Manager (ex-LANDesk) (payant) ;
  - Mobile Application Management de MobileIron ; (payant) ;
  - Munki (gratuit) ; …

La solution retenue à l'IEMN ?

Pourquoi ne pas utiliser des outils payants alors ?

Temps

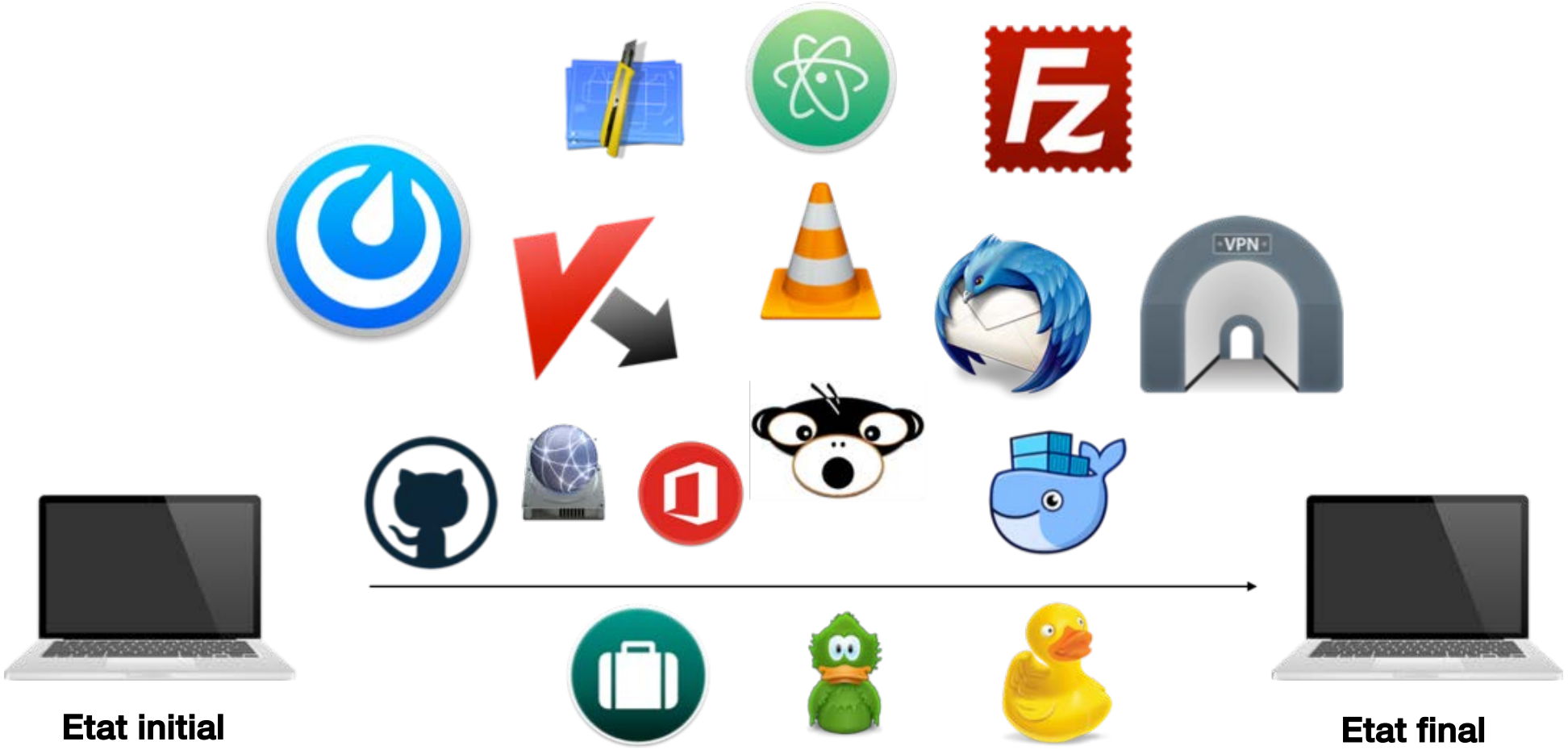
Ouvert vs Propriétaire

Coût

Gérer des postes macOS (pratiquement) **sans** macOS

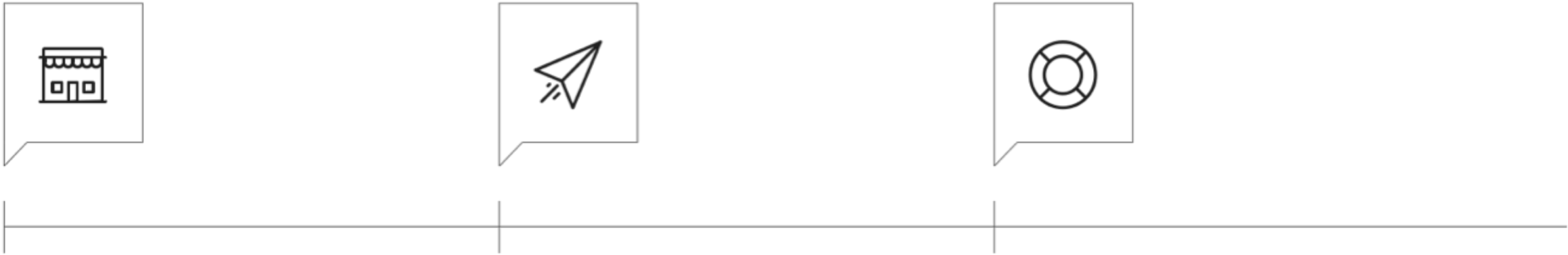
… C’est possible ???

Comment fait-on à l'IEMN ?



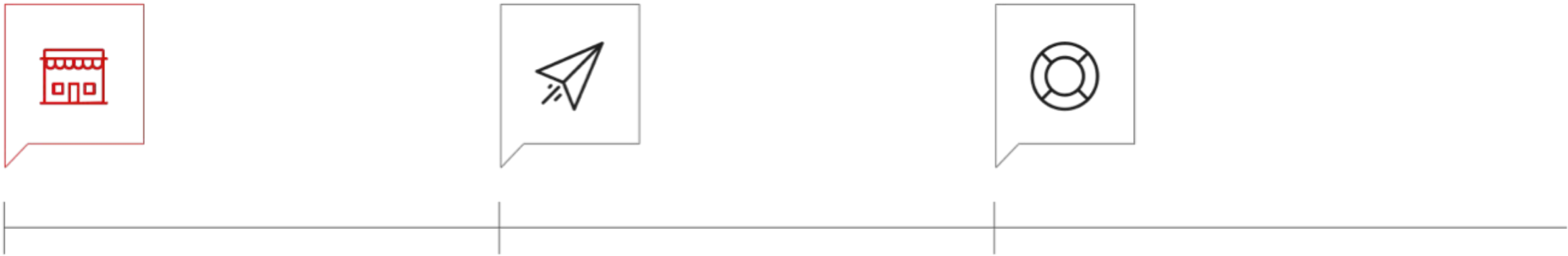
Notre vision du cycle de vie du poste client à l'IEMN

- 3 étapes :



Notre vision du cycle de vie du poste client à l'IEMN

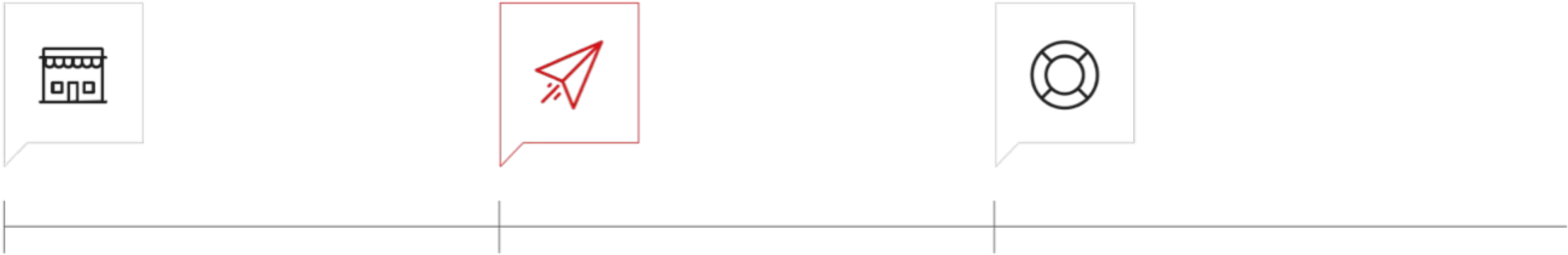
- 3 étapes :



PREPARATION
Une nouvelle machine est achetée ; une nouvelle VM est déployée …

Notre vision du cycle de vie du poste client à l'IEMN

- 3 étapes :

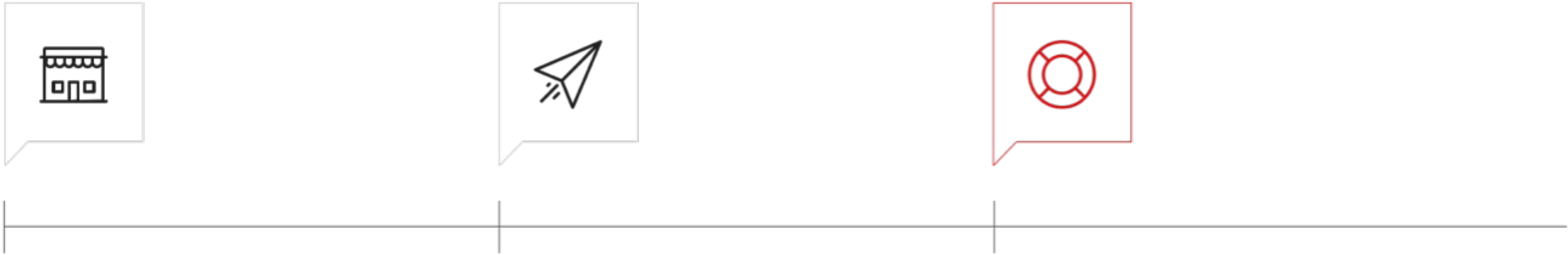


PREPARATION
Une nouvelle machine est achetée ; une nouvelle VM est déployée …

GESTION DES APPLIS, …
La machine est préparée avec tout ce qui nécessaire à l'utilisateur, à minima, pour travailler …

Notre vision du cycle de vie du poste client à l'IEMN

- 3 étapes :



PREPARATION
Une nouvelle machine est achetée ; une nouvelle VM est déployée …

GESTION DES APPLIS, …
La machine est préparée avec tout ce qui nécessaire à l'utilisateur, à minima, pour travailler …

SUPPORT
Ce sont toutes les choses qu'il faut réaliser pour la maintenir à jour, réagir si nécessaire, …

La préparation

« Wouhou !!! un Mac flambant neuf – mais que faire avec ça ? »

Le (re)déploiement du poste de travail (1/2)

- Principe général :

IMAGE NETBOOT

Le serveur contient une image du système cible macOS.

POSTE CLIENT

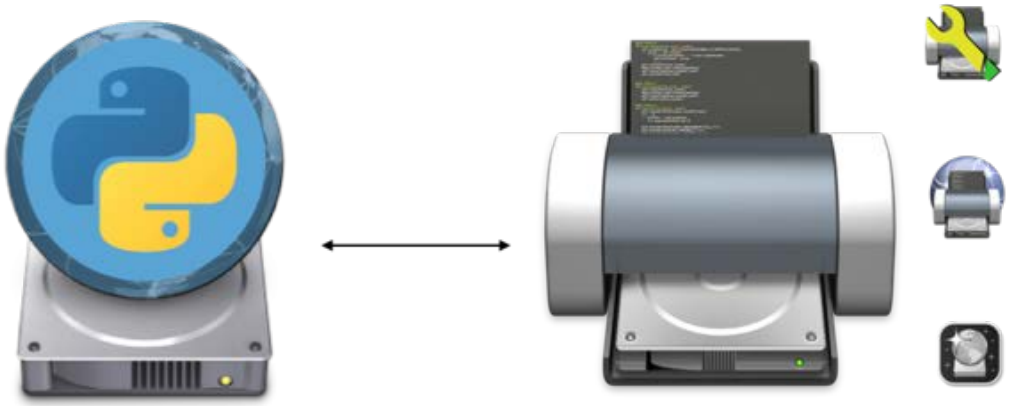
La machine démarre par le réseau et reçoit une image disque préparée préalablement (contient OS + applications) via HTTP.

SERVEUR WEB

Il contient les images disques, les applications à déployer, les profils de configuration, …

Le (re)déploiement du poste de travail (2/2)

- Composants principaux :



BSDpy

Serveur de démarrage sur le réseau (ala PXE), basé sur l'implémentation libre du protocole Apple NetBoot.

Imagr

Application capable de restaurer une image disque et d'installer des applications sur un volume HFS+.

… mais ça, c'était avant …

- Avec l'arrivée d'APFS …
- … et de l'iMac Pro :

Imaging will be dead (soon-ish)

"I don't normally try to foretell the future but there is one change for Mac admins that I'm pretty sure will happen: The coming of Apple File System (APFS) will mark the end of disk imaging on Macs."

Rich Trouton

La parade

- Si on « schématise », globalement, le processus de déploiement c'est :

Hier

Ce vers quoi nous allons

Les orientations d'Apple

Le « nouveau » processus de déploiement de l'OS

- Le provisionnement « léger » :

PAQUET D'INSTALLATION
Contient des applications et des réglages.

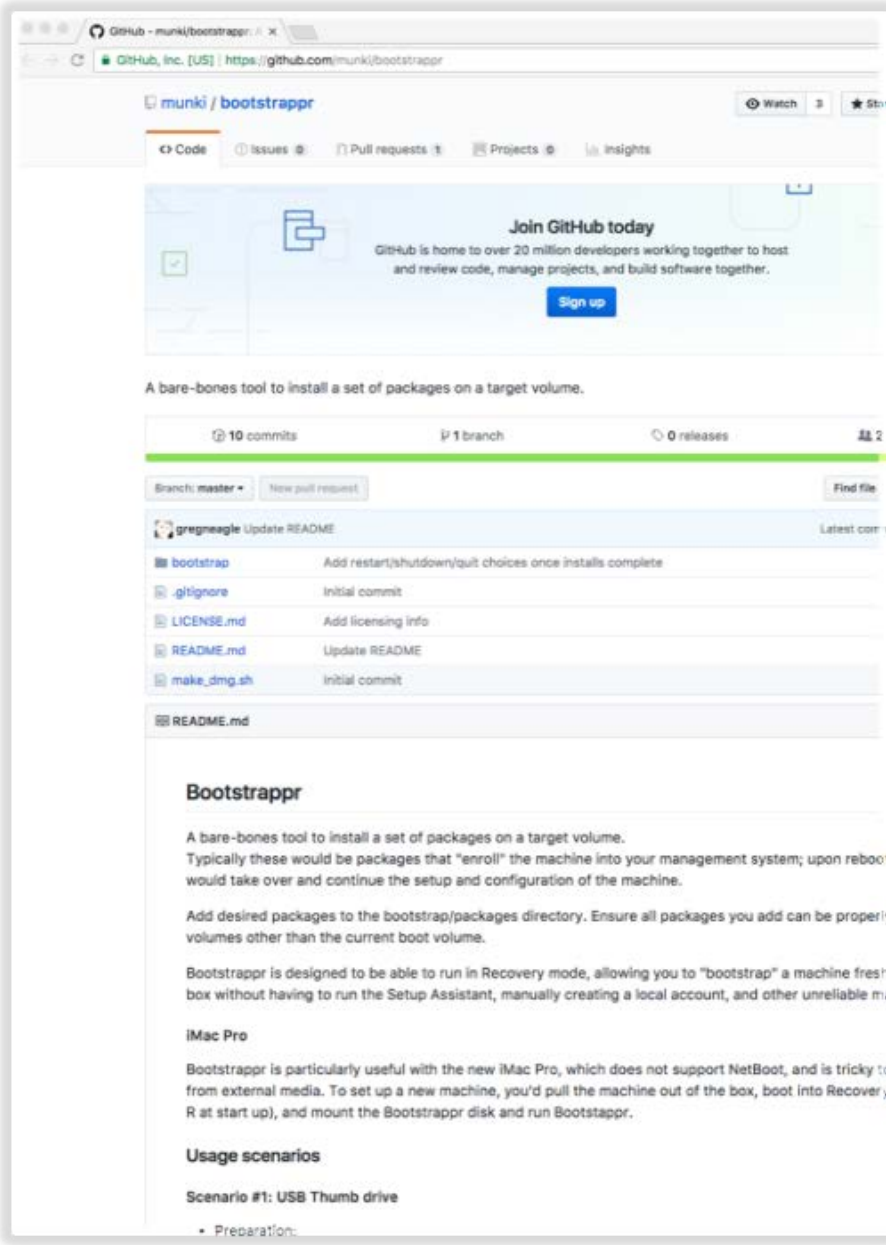
POSTE CLIENT
La machine reçoit les réglages et quelques applications nécessaires à la personnalisation de la machine.

SERVEUR WEB
Il sert les les applications à déployer, les profils de configuration, … Il envoie les infos demandées par le client.

Bootstrapr

Ensemble d'outils en CLI qui permettent de créer une image disque et de la déployer par le biais d'un serveur web.

Cas de l'iMac Pro (chip T2 et Secure Boot) :
Ne « supporte pas » NetBoot ... mais peut booter depuis un lecteur USB. Depuis le recovery mode, on peut lancer Bootstappr ☺



Et pour le futur …

- La transformation est déjà engagée :

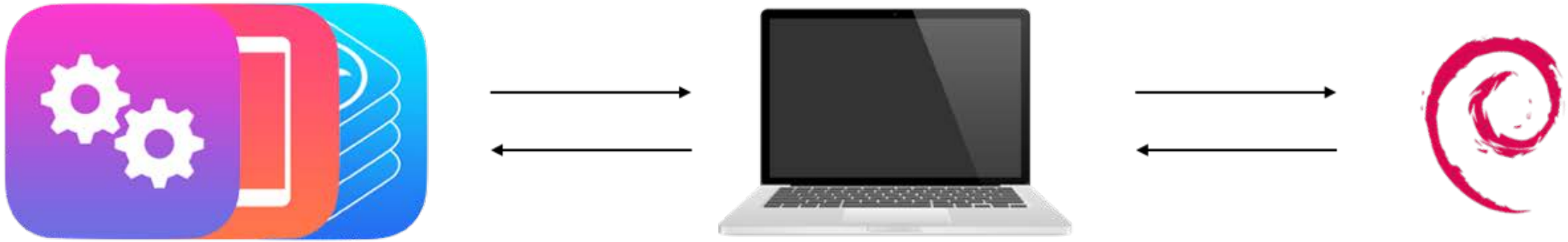
Hier

Ce vers quoi nous allons

Les orientations d'Apple

Et demain ?

- C’est encore plus « simple » :



MDM + DEP + VPP

POSTE CLIENT

La machine reçoit les réglages et les applications nécessaires à sa personnalisation via la solution de MDM.

SERVEUR WEB

Il sert les les applications à déployer, les profils de configuration, … Il envoie les infos demandées par le client.

Et demain ?

- Il existe déjà une solution « libre » pour gérer ce cas :

MicroMDM

POSTE CLIENT

La machine reçoit les réglages et les applications nécessaires à sa personnalisation via MicroMDM.

SERVEUR WEB

Il sert les les applications à déployer, les profils de configuration, … Il envoie les infos demandées par le client.

Min2RIEN

La gestion des applications

Le déploiement de logiciels

Munki

Le déploiement de logiciels

Munki

Ensemble d'outils libres (licence Apache 2), écrits en Python

Catalogue en self-service (ala App Store)

Autorise la gestion du cycle de vie des applications sur les postes clients

Côté « serveur » :

Dépôt d'applications ;

Profils de configuration ; …

Côté client (munkitools) :

Catalogue en self-service ;

Applications gérées ;

Mises à jour logicielles et OS ;

Outils « optionnels » ; …

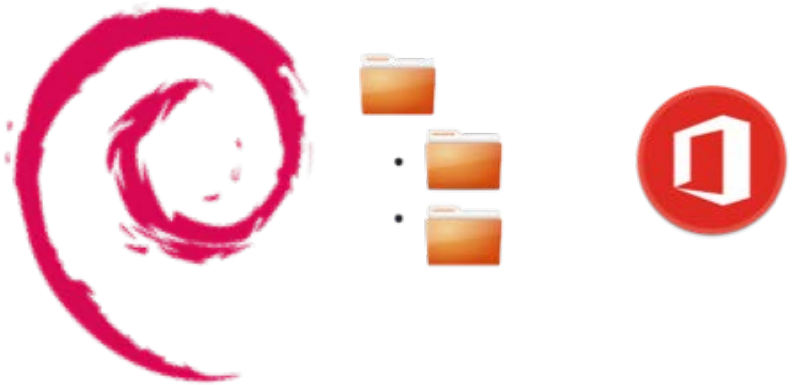
Le déploiement de logiciels dans la pratique …

Munki

Ensemble d'outils libres (licence Apache 2), écrits en Python

Catalogue en self-service (ala App Store)

Autorise la gestion du cycle de vie des applications sur les postes clients



Serveur web (Apache/nginx)

Un dépôt d'applications Munki, c'est 4 répertoires (à minima) :

- /catalogs
- /icons
- /pkgs
- /manifests

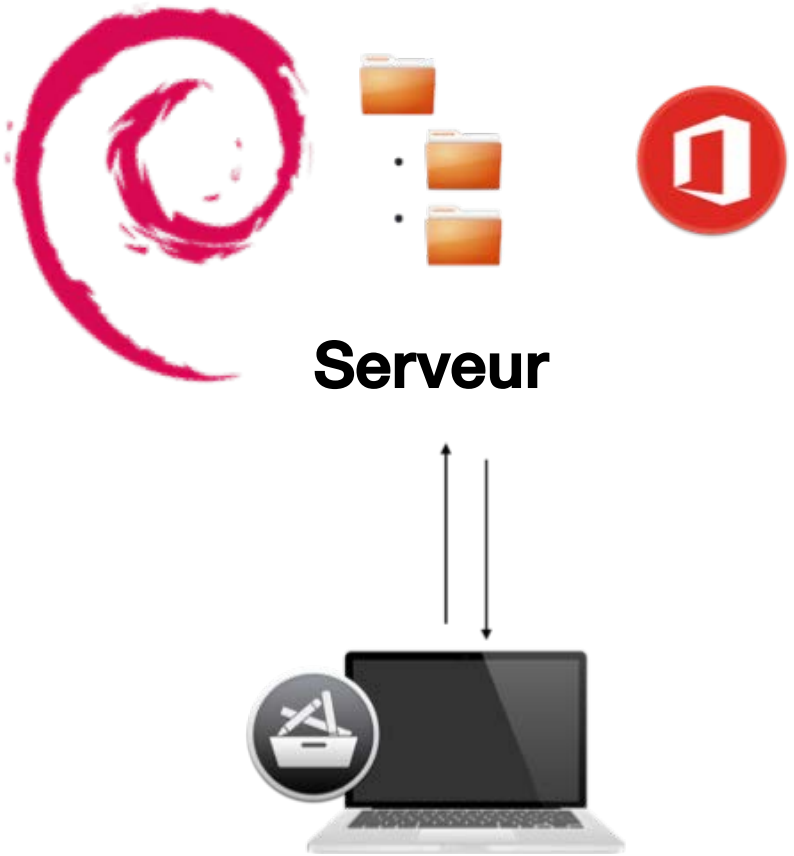
Le déploiement de logiciels dans la pratique …

Munki

Ensemble d'outils libres (licence Apache 2), écrits en Python

Catalogue en self-service (ala App Store)

Autorise la gestion du cycle de vie des applications sur les postes clients



Le déploiement de logiciels dans la pratique …

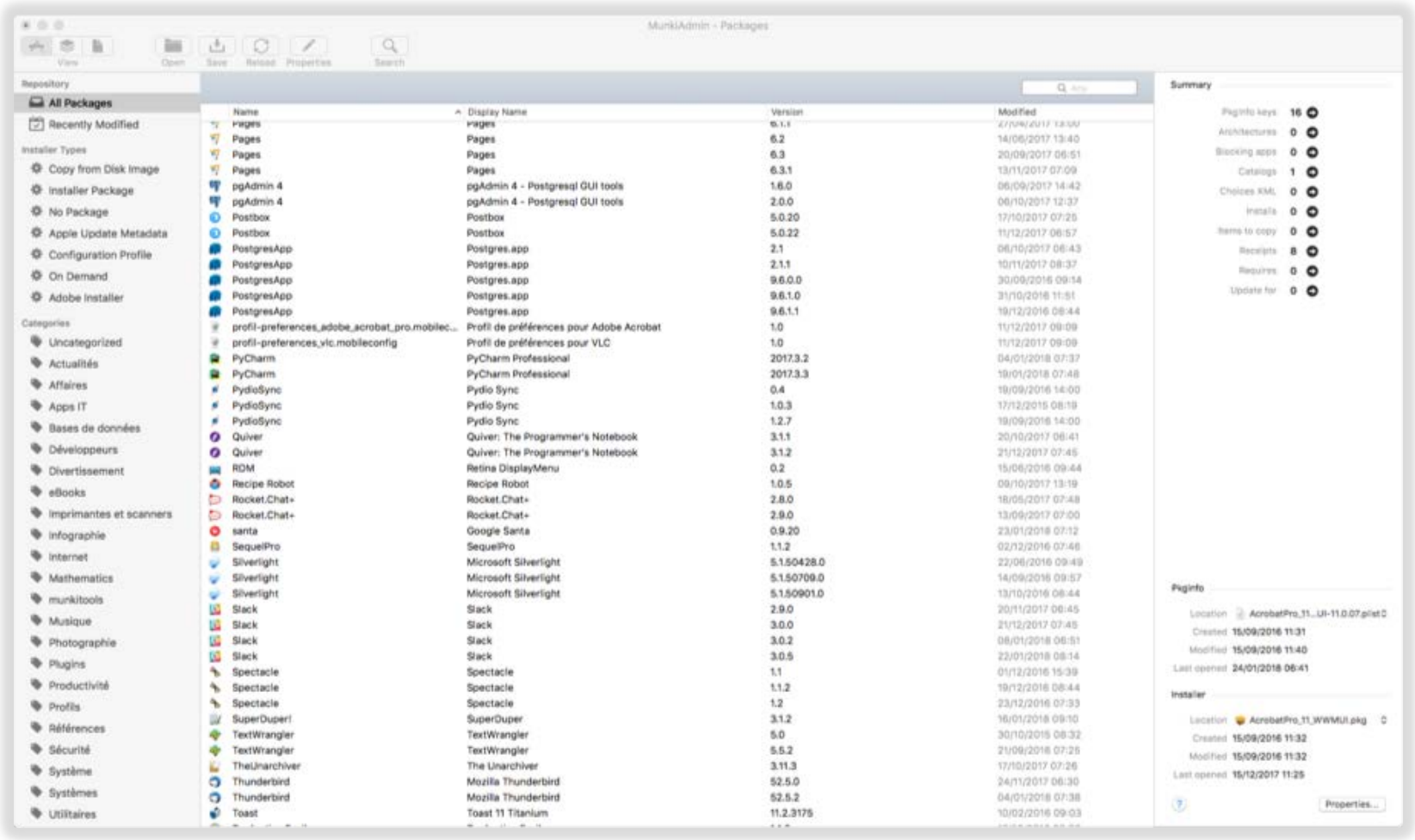
Munki

Ensemble d'outils libres (licence Apache 2), écrits en Python

Catalogue en self-service (ala App Store)

Autorise la gestion du cycle de vie des applications sur les postes clients

Un outil d'administration complet

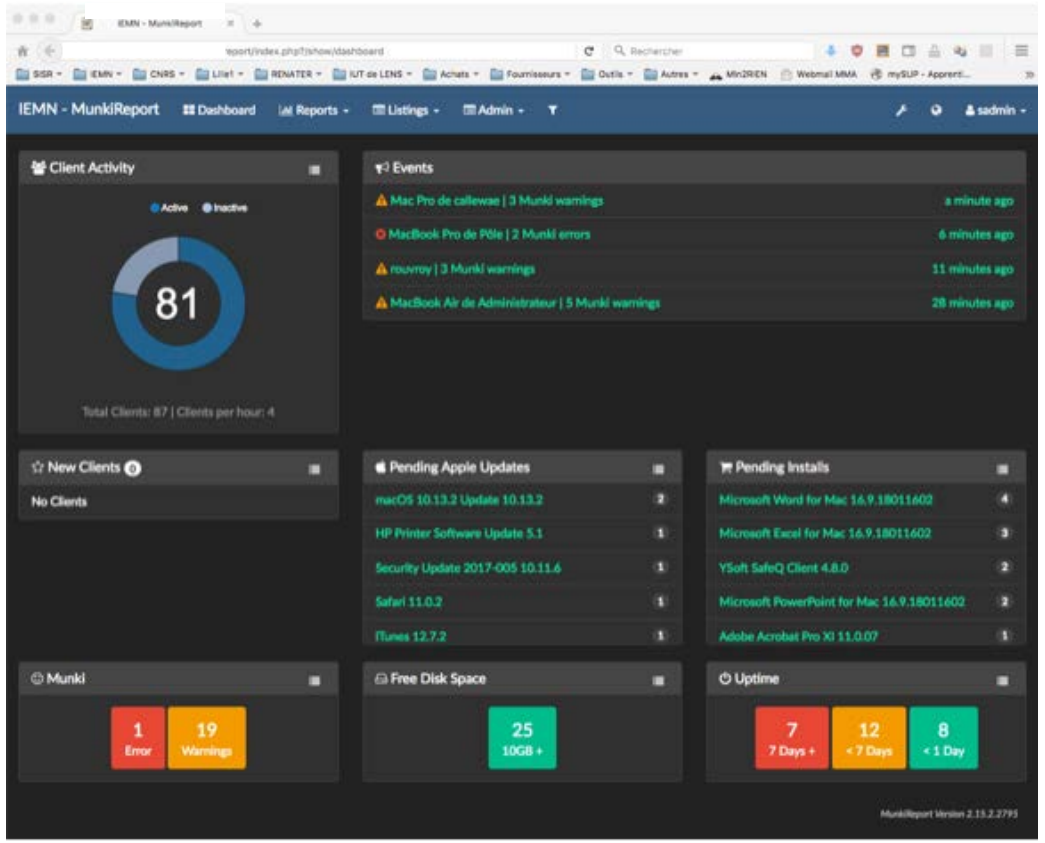


L'inventaire des actifs

munkireport-PHP

Outil de reporting écrit en PHP

Remonte beaucoup d'infos (inventaires, état de conformité de la machine, …)



Les profils de configuration

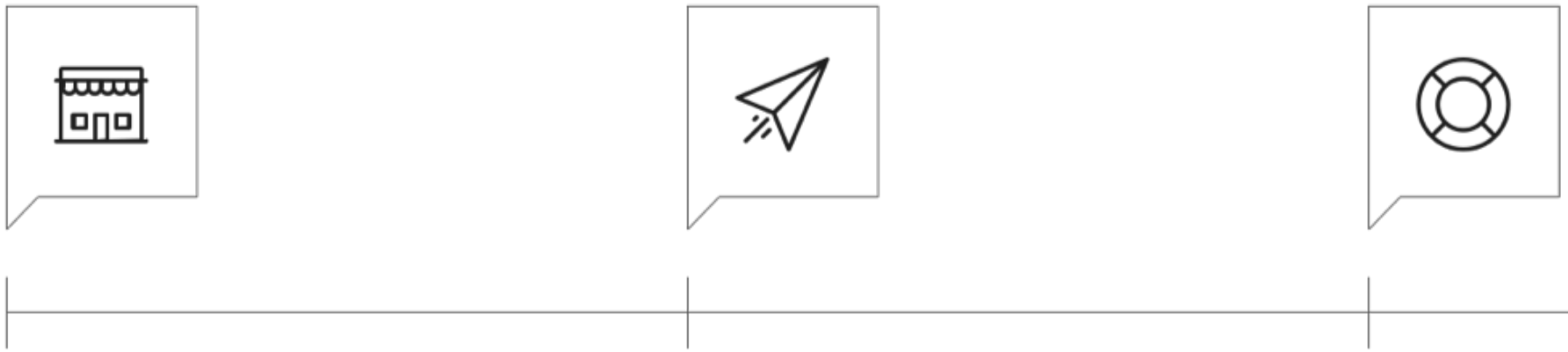
Munki

Stratégies et politiques de sécurité ?

Déployer des profils de configuration (fichiers *.mobileconfig)

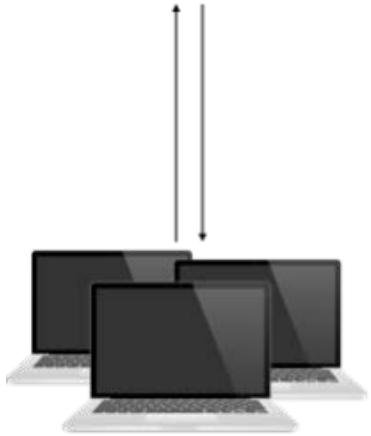

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>PayloadContent</key>
   <array>
      <dict>
         <key>PayloadContent</key>
         <dict>
            <key>com.microsoft.autoupdate2</key>
            <dict>
               <key>Set-Once</key>
               <array>
                  <dict>
                     <key>mcx_preference_settings</key>
                     <dict>
                        <key>HowToCheck</key>
                        <string>Manual</string>
                        <key>LastUpdate</key>
                        <date>2001-01-01T00:00:00Z</date>
                     </dict>
                  </dict>
               </array>
            </dict>
```

Récap' : Le processus pour une machine cliente



Etape initiale …

BSDpy / Imagr

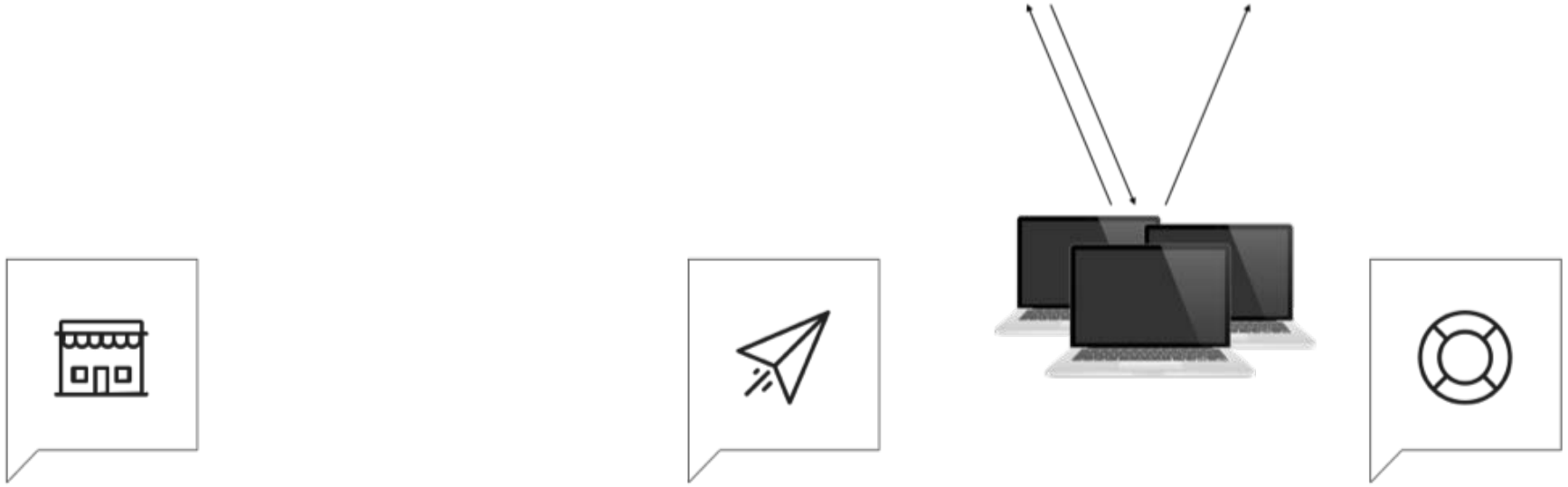


On ajoute les applis, les réglages … et on reporte !

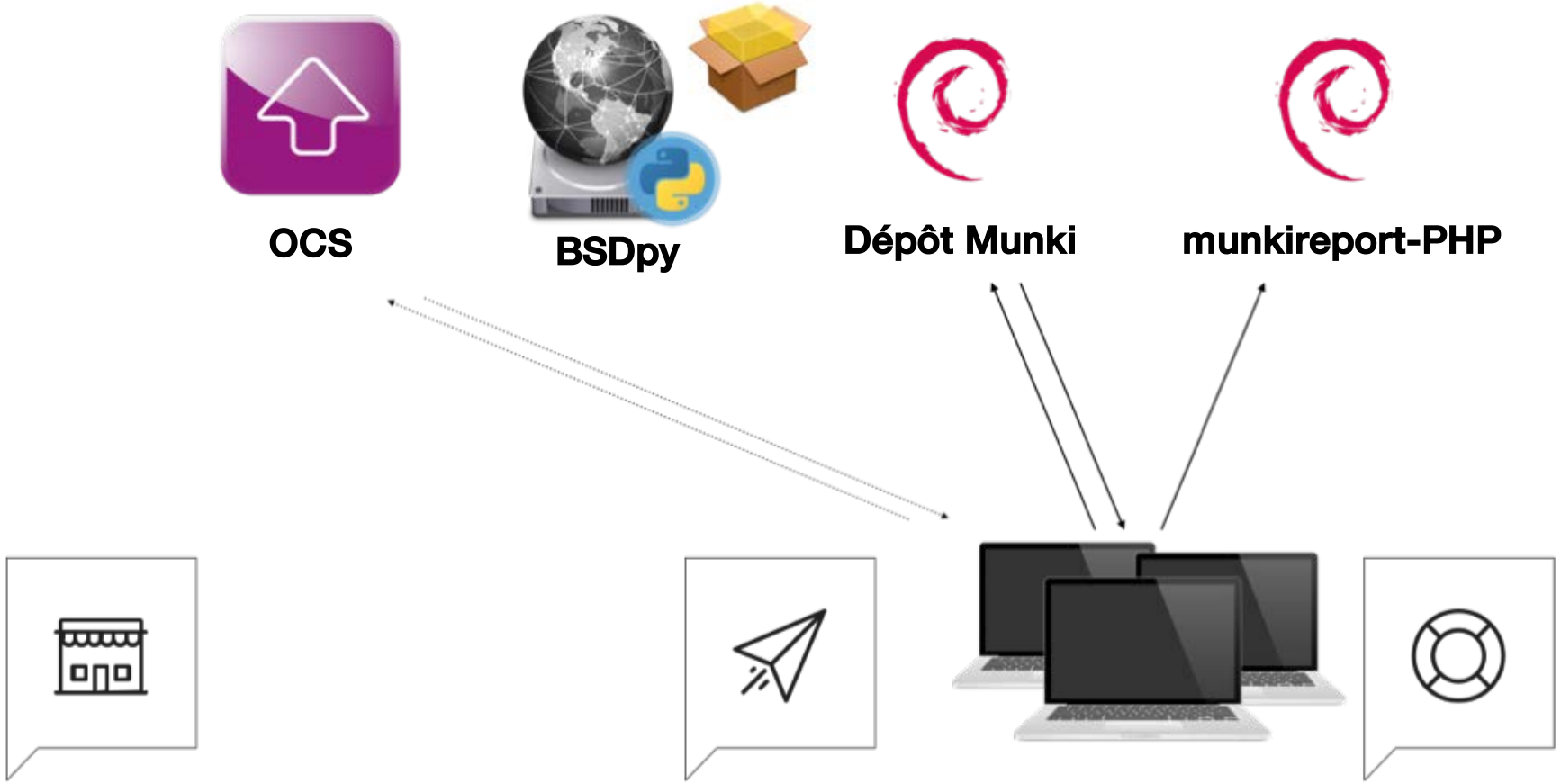
BSDpy / Imagr

Dépôt Munki

munkireport-PHP



On installe OCS sur le client et on donne des infos sur les actifs

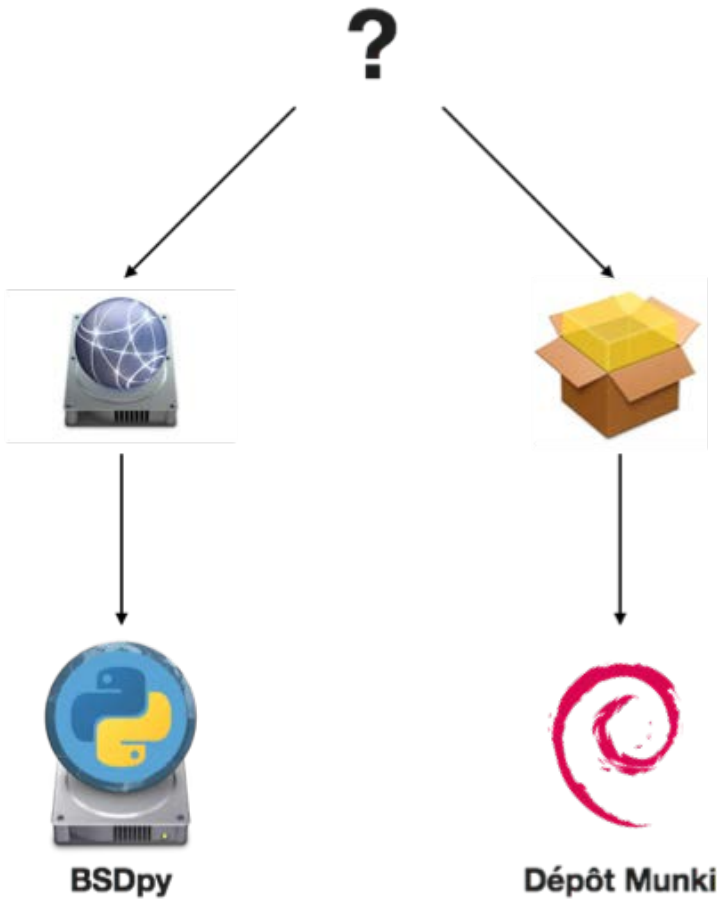


Min2RIEN

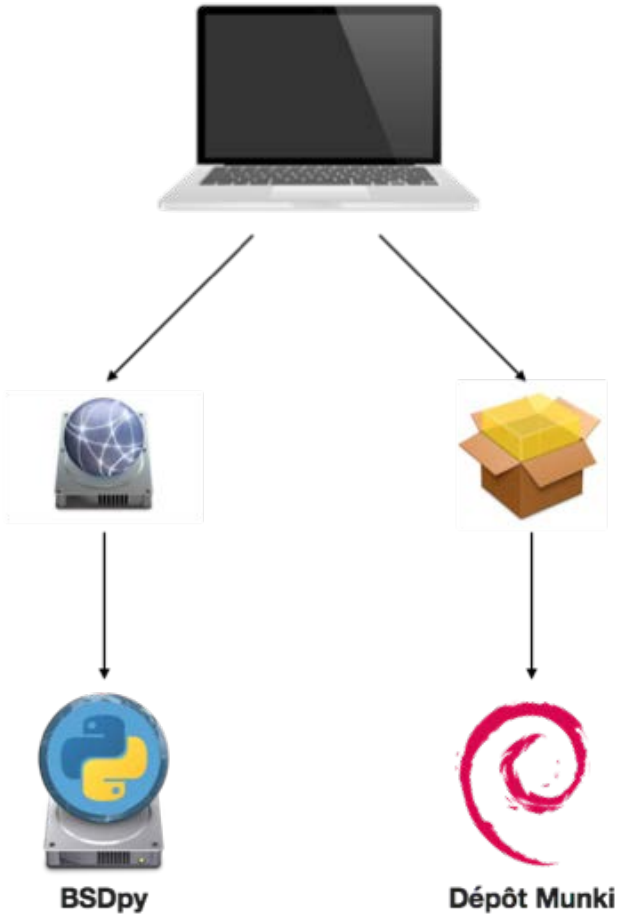
Le support

… Update, update, update …

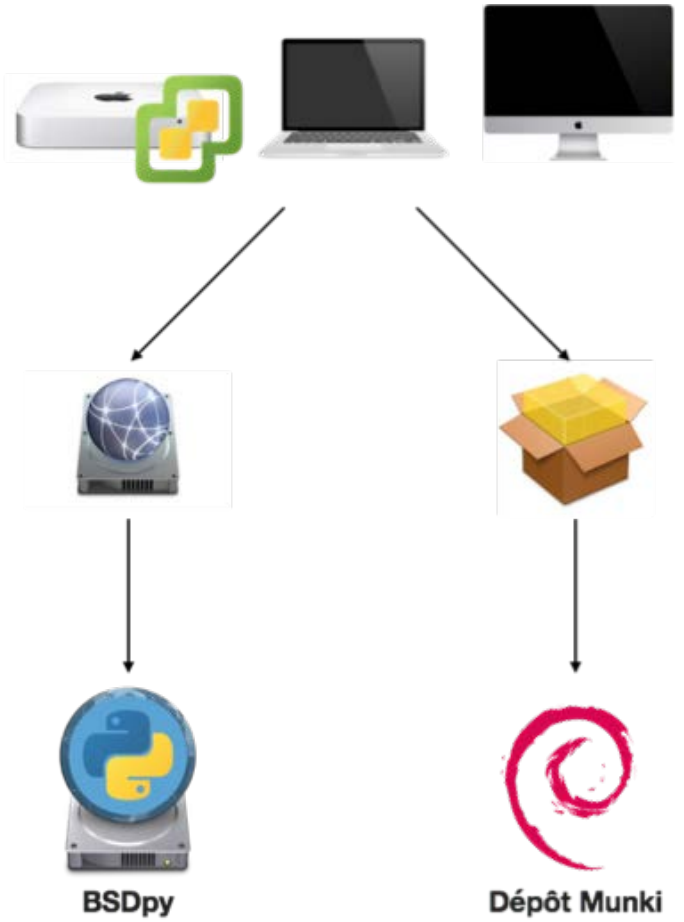
Jusqu'à présent, on a vu quoi ?



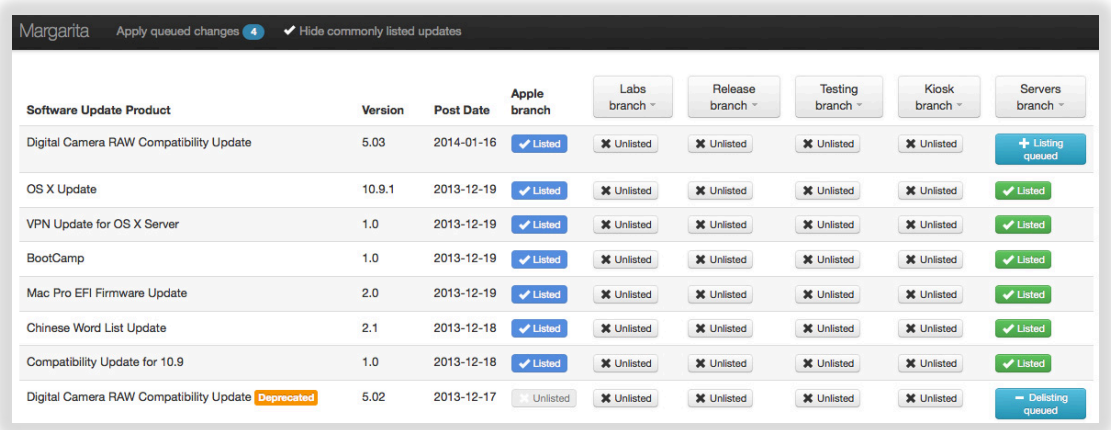
… une solution adaptée à des machines physiques …



… mais aussi à des VMs (ou n'importe quoi d'autre d'ailleurs …)



La gestion des mises à jour de macOS ?



margarita (+ reposado)

Equivalent du SUS Microsoft ou Apple

Outil écrit en Python (avec le framework Flask)

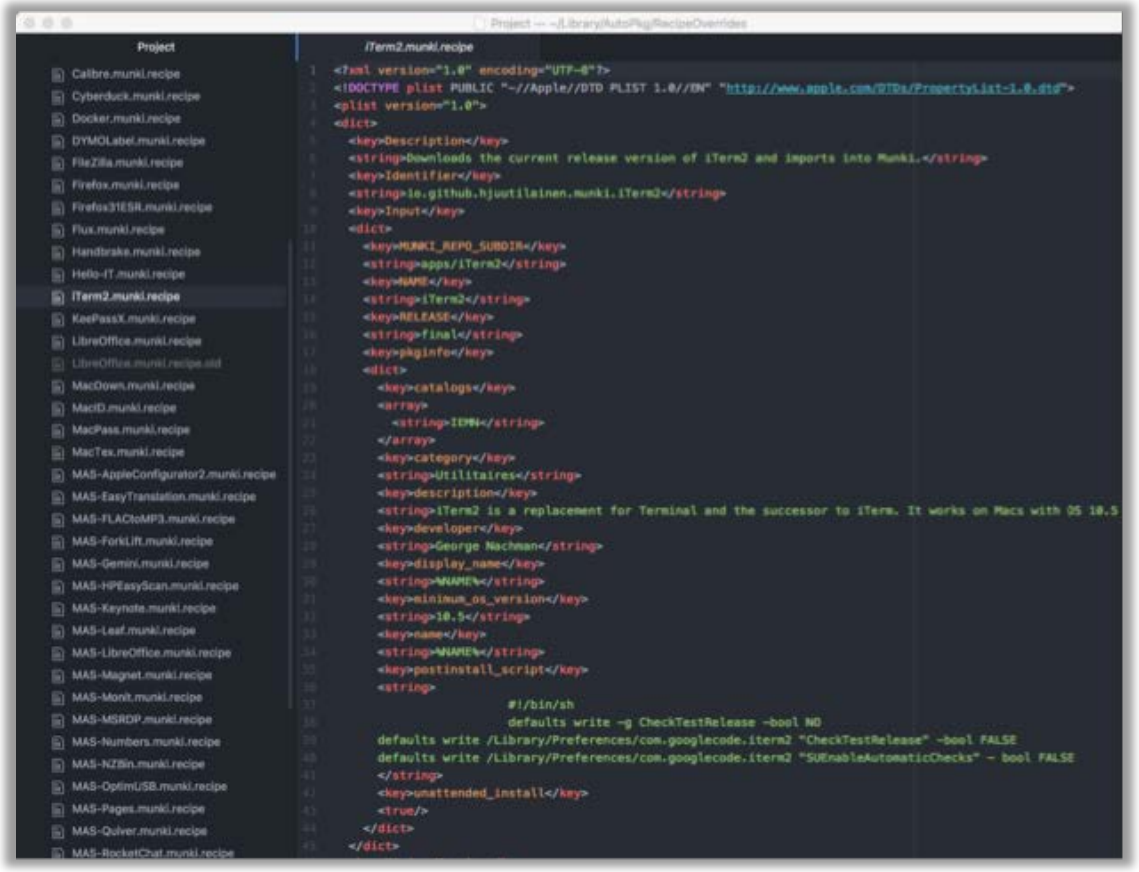
Permet de gérer les mises à jour de macOS

Et pour le processus de mise à jour des logiciels ?

AutoPkgr

Ensemble d'outils libres, interface à Autopkg (licence Apache 2)

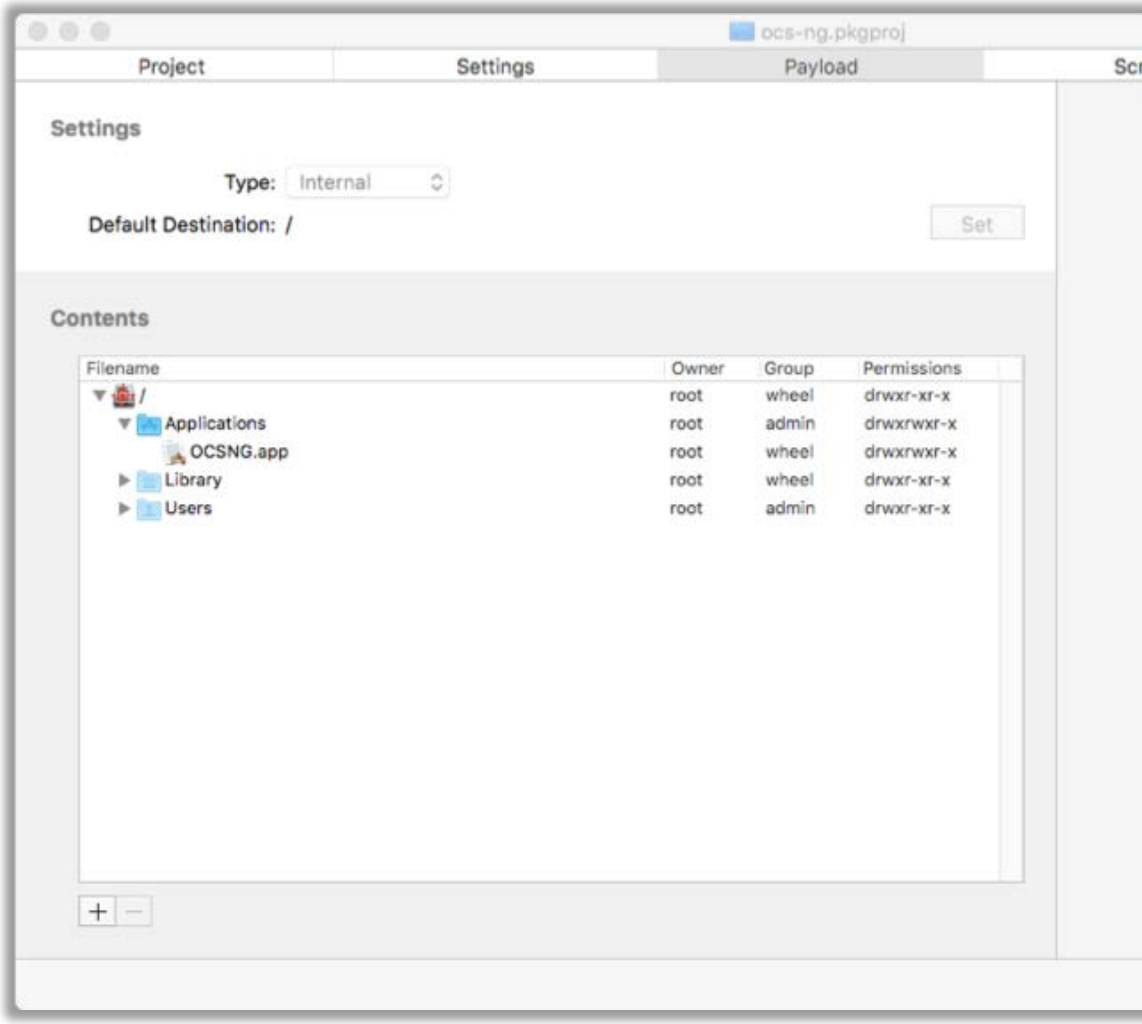
Permet d'automatiser la récupération des mises à jour des applications chez les éditeurs de logiciels (via flux Sparkle, canal de « releases » sur GitHub, RSS, …)



Quelques outils utiles pour le gestionnaire de parc macOS

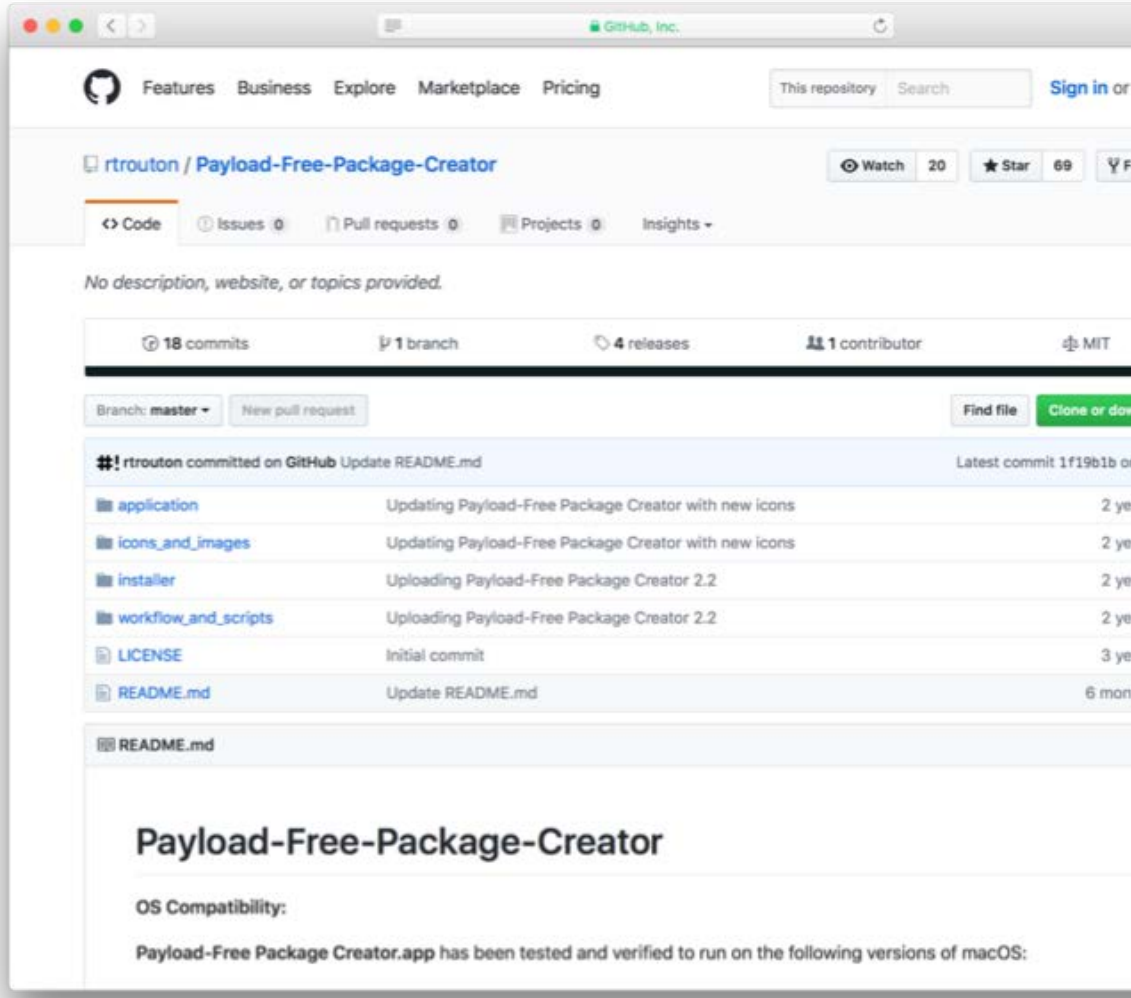
Packages

Application gratuite qui permet de construire des paquets d'installation ou de distribution pour les systèmes à partir de MacOS X 10.5 ou plus



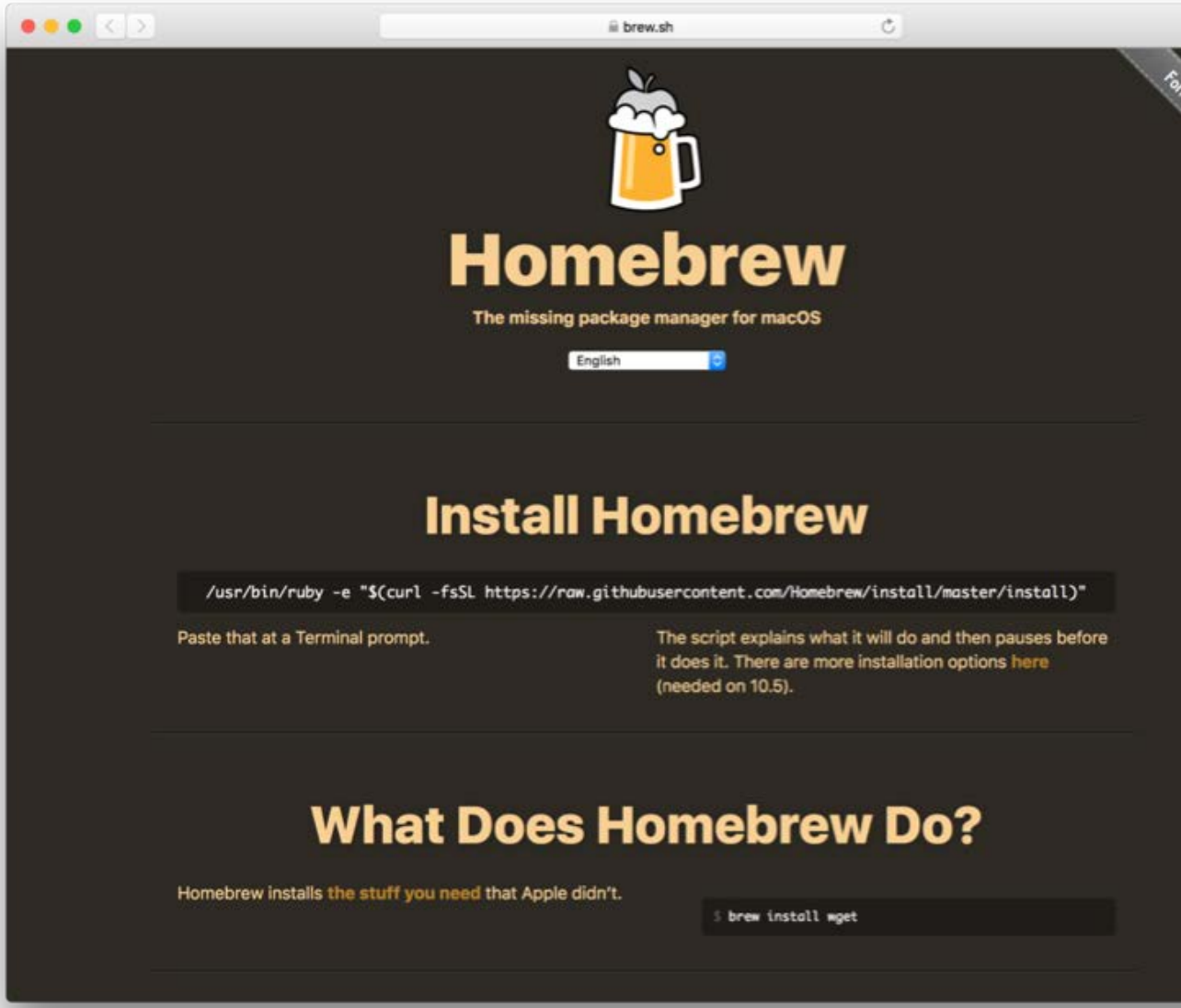
Payload-Free Package Creator

Interface graphique qui s'appuie sur AppleScript, des scripts shell et le binaire pkgbuild pour créer des packages.

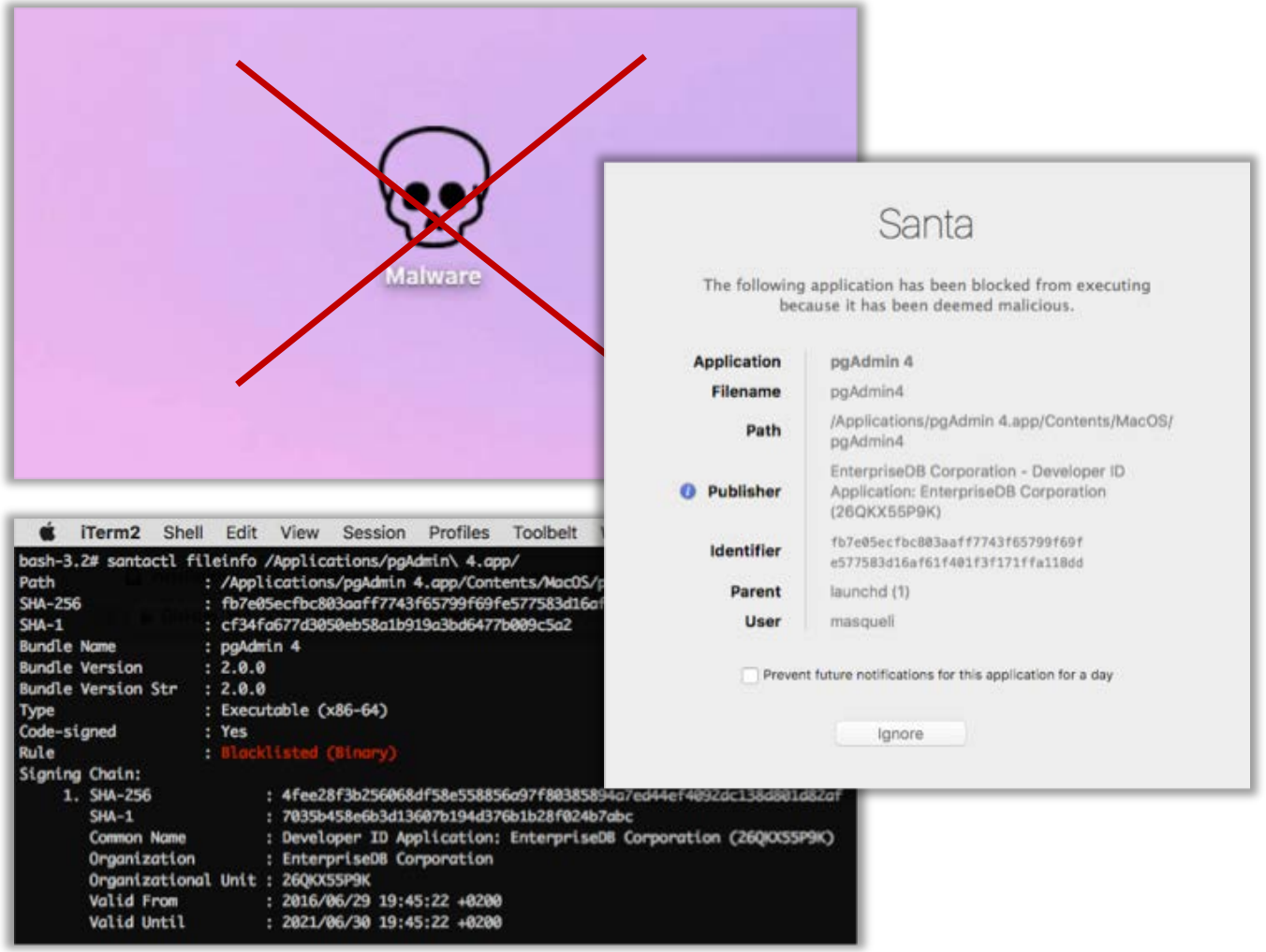


Homebrew

Un gestionnaire de packages (ala apt-get/yum/tdnf pour macOS … (pour ajouter wget facilement par exemple ☺)



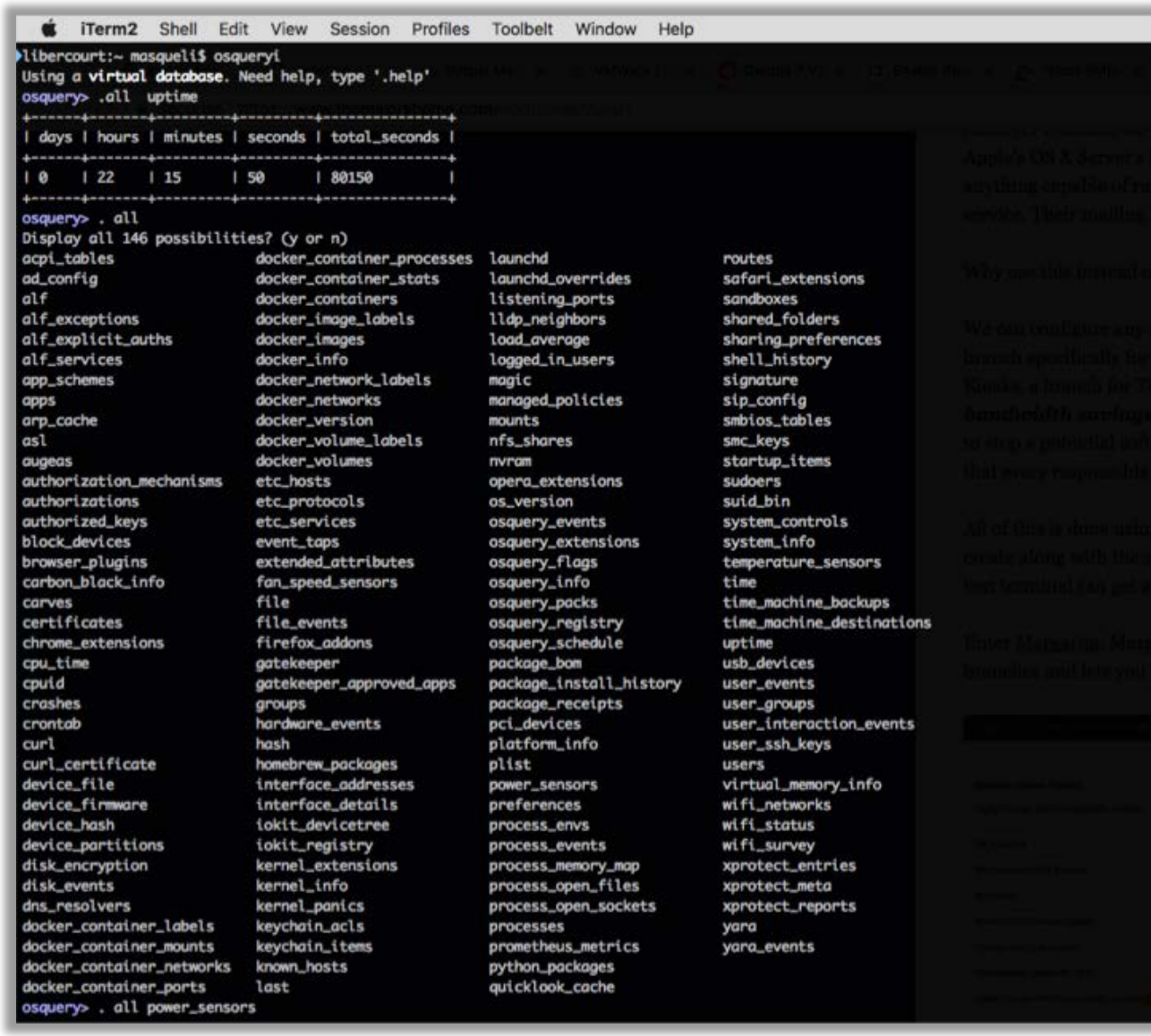
Google Santa



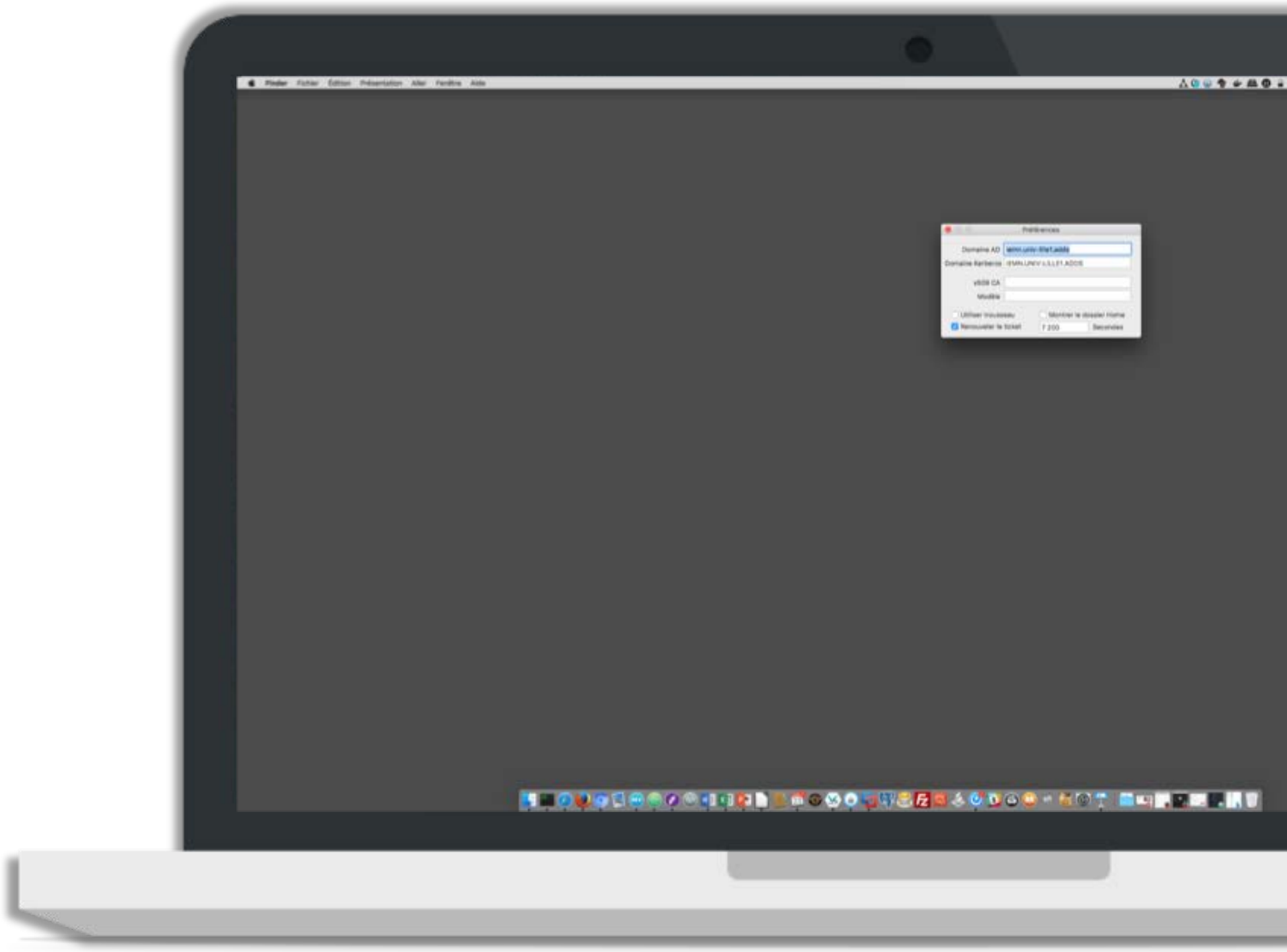
Application développée par Google qui permet de bloquer des binaires malveillants (système de blacklist) pour les machines sous macOS (complément à GateKeeper).

OSQuery

Application en CLI qui vous permet de poser des questions à vos machines Linux, MS Windows et macOS (ala SQL).



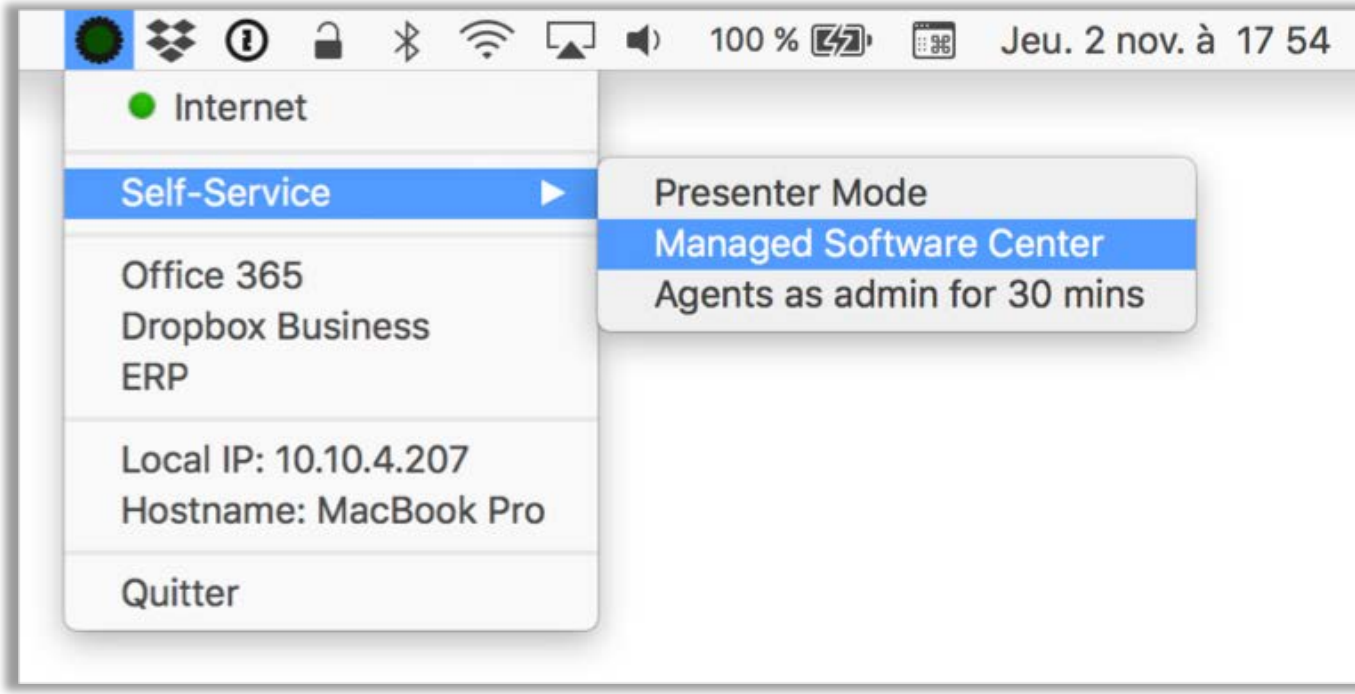
NoMAD



Une application macOS qui permet de se connecter, via un petit menu, à un annuaire Active Directory et d'effectuer plusieurs opérations liées à l'AD (sans être « relié » à l'AD).

Hello-IT

Application qui ajoute un menu entièrement personnalisable sur le poste de travail de l'utilisateur (raccourcis applis, état de la connexion Internet, adresse IPv4, …)



microMDM

Un projet expérimental qui vise à proposer une solution serveur de Mobile Device Management (MDM) pour les terminaux Apple.

Connecting to DEP

Note: Bootstrapping management tools like Munki is probably the reason most of us want an MDM right now, but DEP is not necessary for MicroMDM to work. You can skip to the "Profiles and Applications Section" if you don't have a DEP account.

Got a DEP account? You can set up a virtual server for MicroMDM and sync your devices: https://github.com/micromdm/micromdm/wiki/Connect-MicroMDM-with-DEP

Once you're connected to DEP and can sync devices, you can assign a profile to them:

Sample profile.json. Note the list of serial numbers to assign the profile to.

```
{
   "profile_name": "Test Profile",
   "url":"https://dev.micromdm.io/mdm/enroll",
   "await_device_configured":false,
   "is_mdm_removable":true,
   "department": "IT Department",
   "org_magic": "913FABBB-0032-4E13-9966-D6BBAC900331",
   "support_phone_number": "1-555-555-5555",
   "support_email_address": "org-email@example.com",
   "skip_setup_items": [ "Registration", "AppleID", "TOS"],
   "devices": ["SERIAL1","SERIAL2"]
}
```

Gérer des postes macOS (pratiquement) **sans** macOS

… Pari réussi ?

Références

[BSDPy](#)
Implémentation d'un service serveur Apple NetBoot (BSDP) libre.

[Micro MDM](#)
Solution libre « expérimentale » de serveur MDM pour les terminaux Apple.

[AutoPkgr](#)
GUI pour automatiser la récupération des mises à jour d'applications.

[Homebrew](#)
Un gestionnaire de paquets (façon yum, apt-get, …)

[OSQuery](#)
Outil type requêteur SQL pour avoir des infos sur sa machine Linux, MS Windows ou macOS.

[Imagr](#)
Application capable de restaurer une image disque et d'installer des applications sur un volume macOS.

[Munki](#)
Ensemble d'outils qui s'appuient sur un serveur web pour proposer un catalogue d'applications en self-service.

[Packages](#)
Permet la création de paquets de distribution ou d'installation pour systèmes OSX.

[Google Santa](#)
Outil qui permet de gérer une blacklist/whitelist de binaires autorisés à être exécuté sur un Mac.

[Hello-IT](#)
Application qui ajoute un menu entièrement personnalisable sur le poste de travail de l'utilisateur (raccourcis applis, état de la connexion Internet, adresse IPv4, …).

[AutoNBI](#)
Outil pour automatiser la construction et la création d'images Apple NetInstall.

[munkireport-PHP](#)
Client de reporting pour Munki, complémentaire à une solution comme OCSng.

[Payload-Free Package Creator](#)
Utiliser AppleScript, des scripts shell et pkgbuild pour créer des paquets d'installation d'applis.

[NoMAD](#)
Permet de se connecter à un annuaire Active Directory et d'effectuer plusieurs opérations liées à l'AD (sans être « relié » à l'AD).

[suspicious package](#)
Application qui permet d'explorer le contenu d'un paquet macOS et de avoir ce qu'il renferme (bloatware, malware, … ?)

Questions ?