

---

# Méthodes et outils de Gestion de parc

---

Linux - windows

---

# Le concept

- 2 méthodes de maintenance de parc:
  - On réinstalle rapidement ...
  - On entretient le plus longtemps possible...

La réalité: 2 challenges à relever

---

---

On réinstalle très vite...

---

---

# Réinstaller vite... très vite

- On rejoue une installation automatiquement
    - Windows
      - Unattended (Source forge)
      - RIS de base (personnalisation via setupmgr.exe)
      - Nlite
    - Linux
      - Debian et dérivés (ubuntu)... : debootstrap (super!)
      - Redhat ?
-

---

# Réinstaller vite... très vite

- On remet une image pré fabriquée
    - Machines identiques:
      - Pas facile avec les marchés! Surtout en unité mixte...
      - Pas facile avec les chercheurs non plus...
    - Image générique
      - Dure à mettre au point (pb de driver chipset)...  
Merci les marchés! Pb récurrent chez DELL...
  - => Problèmes des mises à jour.
    - On ne les fait pas et on les scripte...
-

---

# Réinstaller vite... très vite

- ❑ **Ghost:** Toujours une bonne raison pour ne pas marcher...
  - ❑ **PXE ou RIS+RipPrep.**
    - RipPrep: Pas facile d'envoyer une image valide...
  - ❑ **Copieur de disque dur**
    - Super mais coûte cher et doit suivre les évolutions matériels des disques dur.
  - ❑ **Logiciel de copie**
    - dd=if/ ... lent, taille des disques!
    - Xcopy /O ... Ok mais lent. NTbackup beaucoup plus rapide
    - BartPE+Snapshot ... Change la taille des disques en copiant.
      - ❑ Très rapide! 39\$
-

- 
- Où sont les données ? => On les sauve comment?
    - 2 Procédures à prévoir:
      - installation d'une machine
      - Migration d'une machine
  
  - Quelles sont les softs ? => Peut-on les remettre facilement ?
    - Oui si on les a scriptés
-

---

On entretient...

---



---

# Maintenir, pas facile!

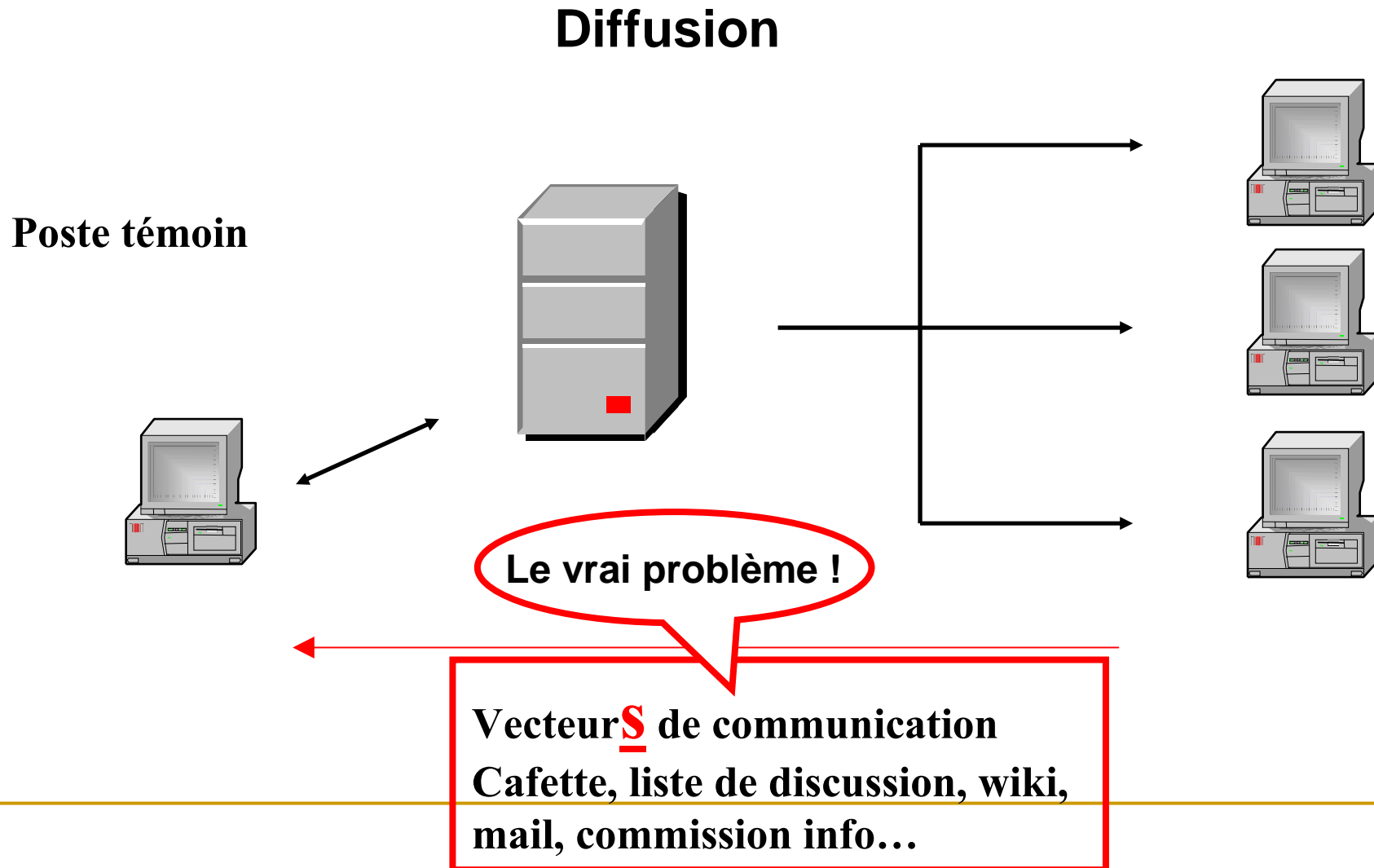
- ❑ On attend qu'on nous remonte un problème.
    - Faible pression jusqu'à 50 chercheurs...
    - Limite du système vite atteinte... les chercheurs deviennent administrateur.
      - ❑ Sécurité bof, divergence des techniques de travail, perte des standard, savoir et savoir faire répartis, évolution quasi impossible...
  - ❑ Quand on a vu un problème on le corrige et on attend qu'un autre nous le signale à nouveau?
-

---

# La maintenance centralisée: un problème de communication...

- On intervient sur tout le monde sans prévenir...
    - On est loin de tout savoir, restons modeste.
    - On propose: prend qui veut!
  
  - Dans certain cas : intervention forcée massive indispensable
    - Chargés de Sécurité...
    - Déploiement de politique laboratoire
      - Couvrez-vous... Casque anti-bruit en option.
      - Direction... Commission utilisateur
        - En cas de problème: la direction est toujours la 1ere à taper => privilège
          - Cf Asterix et les Goth
      - Atarax 1000mg
-

# Cheminement de l'information



---

# Pour diffuser : les scripts

- Pour être reproductible.
    - Correction d'erreurs
    - Evolutivité (changement de version)
  - Pour la qualité du service rendu.
  - Pour faire mieux que les utilisateurs
-

---

# Le langage de vos scripts

- Les scripts un vrai langage de communication et d'échange: **Une langue**
- NE PARLEZ PAS LE DIALECTE **Russe-kalmouke**

ON VOUS COMPRENDRA PAS !

- Stable dans le temps et durable...
  - Oublier le C, C+++... pas adapté!
-

---

# Comment coder

- Préférer les commandes fonctionnant sur toutes les versions.
- Utiliser aux maximum les commandes de votre système d'exploitation.

Exemple renommer un fichier en perl:

Ne pas écrire pour renommer le fichier toto.txt en tutu.txt:

```
use File::Copy;  
rename("toto.txt","tutu.txt");
```

Ecrire:

```
`mv "toto.txt" "tutu.txt" `;
```

- ❑ Pour la pérennité des scripts
  - ❑ Pour leurs portabilités
-

---

# Spécial Windows...

- `xcopy /E /C /R /K /I /Q` : force et ne renonce pas. `/O` pour les droits.
  - On ne peut pas remplacer un fichier en cours d'utilisation mais on peut renommer l'ancien et mettre le nouveau...
  - Version de l'OS : chercher un spécifique à l'OS
  - Mettre les droits: `cacls`
  - Créer un compte: `net user toto /add /` (sur un DC pour un compte de domaine) ou `curmgr.exe`
  - Mettre dans un groupe: `net localgroup`
  - Installer une imprimante réseau: `con2prt.exe`
  - Rebooter un ordinateur avec une alerte: `shutdown "nom_ordi" /T:60 /Y /R` (à éviter grandement...)
  - Lire/écrire une clef de registre : `reg`
  - Changer les droits sur les clefs `regdacl` (à installer localement!)
  - Tuer un processus: `taskkill`
  - Pour configurer le système: `ip, firewall, dns, wins ... netsh interface ip show adresse` (attention à bien respecter les espaces) Charger des clefs de registre : `regedit /s toto.reg`
  - Installer un msi: `msiexec /i \\serveur\MSI\WordView\WordView.MSI`
  - Utiliser le "Resource kit" en dernier recours...
-

# Un exemple de script perl

---

```
# Copy d'un répertoire c:\Fichiers vers tout les ordinateurs NT 2000 XP d'un domaine via leurs partage  
c$
```

```
Use strict;                                #syntaxe perl strict

@texte = `net view`;                        #liste les machines du réseau
foreach $i (@texte) {                       #Chaque ligne retournée est mise dans $i
    @ligne = split(/ /,$i);                 #On découpe par mot séparé par un espace
    $nom_ordi = $ligne[0];                  #Le 1er mot est le nom de la machine
    if ($nom_ordi =~ /^\\V ) {              #Un nom de machine commence par \\
        @reponse_xcopy =
            `xcopy "c:\\Fichiers\" \"$nom_ordi\\c$" /C /E /I /R`;
        #On écrit la dernière ligne retournée par la commande
        print ("$nom_ordi --- > $reponse_xcopy[$#reponse_xcopy]; ");
    }
}
}
```

---



---

La maintenance c'est quoi?

---

---

# La maintenance c'est quoi?

- Connaître/Auditer les machines
  - Installer/Désinstaller des logiciels
  - Détecter/Anticiper les pannes
  - Gérer les mises a jour
  - Imposer des standards labo
  
  - **Corriger les problèmes en temps réel**
-

---

# Techniques des outils de maintenance

- La méthode "Push" consiste à aller au devant des utilisateurs en leur fournissant automatiquement des informations.  
=> **On impose ⇔ temps réel**
  - La méthode "Pull" : inciter les utilisateurs à venir rechercher régulièrement des informations.  
=> **On propose**
  - Méthodes "Push/Pull" :  
=> **On annonce dans la machine, prend qui veut**
-

---

# Solutions très bas coût...

- On peut faire simple et pas cher en 1 ligne...

- Méthode pull

At 00:00 \\serveur\_de\_script.fr\ainstaller.bat  
/every:lundi,mardi

(toutes les heures... pas tous en même temps!)

- Méthode Push

Psexec \\client.fr -c ainstaller.bat

(pstools *www.sysinternals.com*)

---

---

# Gestion à distance

- Le vrai problème c'est les scripts...
    - Il faut les écrire ou les personnaliser....
    - Avant d'investir dans la gestion de masse commencer par faire des scripts pour gérer 1 machine. Vous pourrez les mettre ensuite sur un serveur puis les déployer à distance.
    - Il y a plein d'exemple sur le net, faire simple pour pouvoir réutiliser.
    - Beaucoup sont triviaux commencer par ceux la. Ne pas viser le 100% par script.
-

---

# Gestion centralisée la sécurité

---

Techniques, outils, recommandations

---

# Mise à jour automatique.

- Pas sur un serveur de production...
    - Très souvent des problèmes sur les pilotes de manip.
  - Windows: Vous pouvez utiliser le logiciel WSUS C'est un serveur de mise à jour.
    - Pour pré tester automatiquement les correctifs Microsoft avant de les diffuser sur votre site.
    - Pour diffuser à une date précise et, par conséquent, identifier facilement les problèmes liés aux mises à jour.
    - Pour retirer rapidement une mise à jour qui pose problème.
    - Après l'installation de WSUS, sur le serveur, tous vos services FTP, SMTP, NNTP seront désactivés. (Perturbe d'autres services)
  - Linux: apt-get update ...
-

---

# Analyse de log

- Consultation distante des événements windows
    - ❑ `dumpel -d 100 -l system -s \\nom_ordi`
  - Analyse des logs des clients
    - ❑ d'habitude j'en ai 3Kilo sur cette machine aujourd'hui c'est 30Kilo => suspect!
    - ❑ On peut aussi chercher l'événement redémarrage après crash
-



---

# Gestion centralisée

## Audit

---

Techniques, outils, recommandations

---

# Audit matériel d'un parc

- Ne pas mettre un réacteur nucléaire pour ne rien utiliser...
- L'outils de référence : OCS inventory
- Msinfo32.exe, un logiciel standard de Windows pour l'audit en ligne de commande:
  - Il donne le processeur, la mémoire les disques et leur place dispo, les drivers, les programmes lancé au démarrage...
  - Attendre 30 secondes, la commande se termine trop vite!
- sur une seul ligne taper par exemple :

```
"c:\program files\fichiers communs\microsoft shared\msinfo\Msinfo32.exe" /report  
nom__fichier.txt /categories SystemSummary+ComponentsStorage
```

---

---

# Audit logiciel d'un parc

- Les principes : 2 méthodes
  - Par les registres (windows)
    - On liste ce que Windows présente
    - Ce que l'on voit dans
      - "Ajout/suppression de programme"

reg query "\nom\_ordinateurs\HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\installer\folders"

- Par les fichiers (linux, windows)
  - On liste c:\program files ou les "Menu démarrer"
  - C'est loin d'être tout ce qui est installé dans les deux cas.
- On peut aussi chercher une signature (registre ou fichier) à soi...
  - Certains logiciels d'audit intègrent des fichiers de signature à eux. C'est un vrai besoin pour nous?

C'est

---

---

# Déploiement centralisé

---

---

# Outils de diffusion

(pour imposer un standard)

- **WPKG** (un élément de base)
  - **Ocs Inventory** (rustique, compte system!)
  - **Active Directory** (Microsoft, serveur dédié etc..)
  - **Software manager** (jeune)
  
  - **Plein d'outils commerciaux...**
    - Certains très complets et très chers...
-

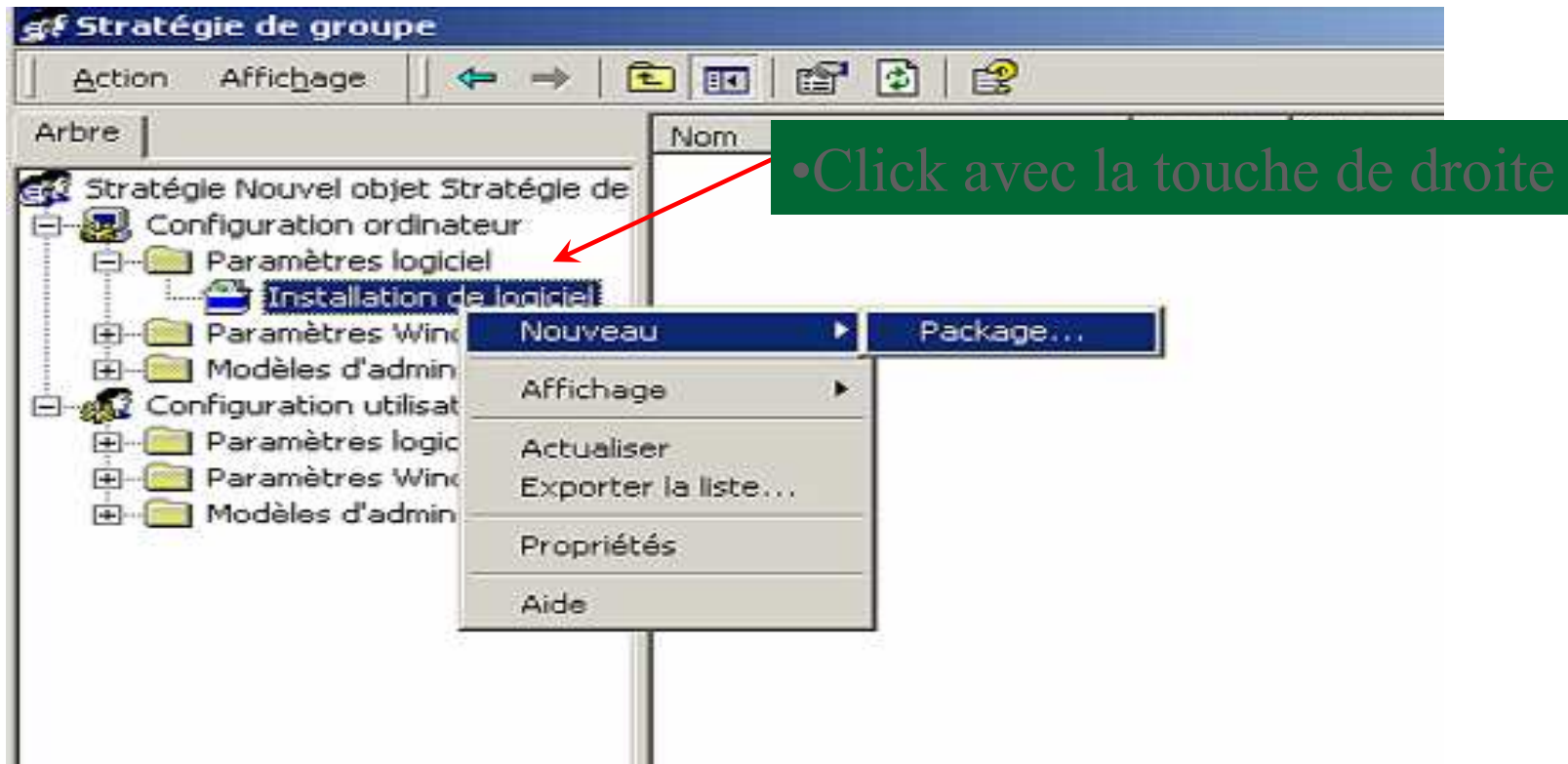
---

# Pour linux, la profusion...

On peut gérer un parc linux comme un cluster...

- **dsh** : l'ancetre, réplique une commande sur plusieurs ordi  
dsh -m machine1 -m machine2 -m ... "echo \$HOSTNAME"
  - **clusterssh** (<http://clusterssh.sourceforge.net/>) :  
Un terminal distinct pour chacune des machines que l'on contrôle.
  - **Clusterm** : idem clusterssh mais indique les différence entre machines
  - **Pssh** : Une suite d'outils bien pratique
    - parallel-ssh Distribue des commandes
    - parallel-scp Distribue des fichiers
    - parallel-rsync Synchronise des fichiers
    - parallel-nuke Tuer des processus sur plusieurs machines en parallèle
    - parallel-slurp Copier des fichiers de plusieurs vers un ordi
-

# Active Directory: Diffusion d'un logiciel .msi



---

# Construire les package

- sysdiff l'ancêtre, le principe
  - Image avant, installation, image après
- WinINSTALL LE : Freeware prenez une version à jour...
- On est pas obligé de construire un msi...
  - Conflit de msi, danger!
  - remplacer les @programfiles par c:\... dans le .reg pour le rendre valide
  - Copier les fichiers...  
Téléchargement <http://sup.scalable.com/>
- Un excellent site de référence pour les scripts de déploiement:

**<http://www.appdeploy.com>**

---



---

# WinInstall LE : Usage

- Utiliser une machine ayant un OS « Clean »
    - Installation de base avec service pack. Pas de soft installé!
  - Installer et configurer une seule application à la fois !
    - sinon vous ne pourrez plus mettre à jour les logiciels indépendamment
  - Le nom du fichier msi utilisé apparaîtra dans le menu de désinstallation.
  - Ne re-packager jamais un .msi, modifier le via un .mst
    - Un msi de msi = problèmes
-

---

# WinInstall LE : Les problèmes ...

- Vérifier toujours le package crée (indispensable)
    - Attention aux droits sur les fichiers...
      - Fichier de configuration des softs à autoriser en modification.
    - Les clefs HKeyCurrentUser sont sans doute à modifier...
  - Utiliser la « Console » puis touche de droite sur « Windows Package editor » « open » pour ouvrir puis régénérer le package.
  - La création des raccourcis ne marche pas bien!
  - N'hésitez pas à retirer les noms de fichiers suspects
-

---

# Créer des packages sur windows

- Wininstall lite, pour la lecture et la création des msi.
- Inno setup, pour packager une appli  
Simple mais il faut connaître ce que l'on installe  
Fichiers, registres...  
Package en français mais logiciel en anglais

Un tutoriel simple:

[http://www.siteduzero.com/tutoriel-3-14171-creer-une-installation.html#ss\\_part\\_2](http://www.siteduzero.com/tutoriel-3-14171-creer-une-installation.html#ss_part_2)

- Nsis idem inno setup
    - plus compliqué à prendre en main, mais bon aussi
-

---

Gestion centralisée

Prise de contrôle à distance

---

---

## Le vrai problème: Les firewalls...

Travail à faire: configurer tous les firewalls Mettre des exceptions pour vos serveurs, ne pas désactiver!

- ❑ "ssh -X ..."
  - ❑ Bureau à distance : pas de client à installer.  
Fermé par défaut
  - ❑ VNC fermer le port firewall après usage.
    - UltraVNC mieux en sécurité
-

---

# Software Manager

---

Un outil jeune mais fonctionnel et complet

---

# Software Manager

Software Manager, logiciel de gestion de parc « en 1 clic » automatise en toute simplicité:

- ❑ L'audit et l'inventaire
  - ❑ La surveillance et les remontées d'alertes
  - ❑ La gestion des mises à jour
  - ❑ La configuration des nouvelles machines
  - ❑ La maintenance des machines
  - ❑ Le déploiement des logiciels
-

---

# Contrôle distant

Connexion efficace et sécurisée en « 1 clic » aux postes du réseau adaptée aux différents OS

3 façons de prendre le contrôle à distance

- ❑ VNC
  - ❑ SSH
  - ❑ Bureau à distance
-



---

# Déploiement des logiciels

La bonne gestion d'un parc implique le déploiement, la mise à jour et la suppression des logiciels :

- sans intervenir physiquement sur chaque poste
  - sans interrompre le travail des utilisateurs en cours
- 
- ❑ Déploiement des logiciels et des imprimantes
  - ❑ 4 types de déploiement de logiciels:
    - par package simplifié (fichiers et registres)
    - par MSI
    - par exécution d'applicatifs personnalisés
    - par setup.exe ( Installshield, NSIS,etc.)
-

---

# Personnalisation

- ❑ Une action dans Software Manager est un script en langage Perl
- ❑ Une action peut être éditée et modifiée pour s'adapter à vos besoins



Les fonctionnalités de Software Manager sont extensibles à volonté par l'ajout de scripts

---

---

# Outils d'aide à la personnalisation

Software Manager met à votre disposition:

- ❑ Une librairie de fonctions évoluées (transfert d'un fichier, analyse d'une clé de registre, etc.)
  - ❑ Un assistant graphique pour la création d'actions
  - ❑ Les scénarios permettant d'enchaîner des actions
-

---

# Aspects de ComputeMode Software Manager

Version limitée à 2 actions simultanées, gratuite:

téléchargement:

<http://entreprise.01net.com/windows/Utilitaire/reseau/fiches/50408.html>

---

Version illimitée "Recherche" offerte

ComputeMode Software Manager - Local

Réseau Affichage Actions Assistants Outils ?

Tous imprimante inconnu linux Reseau windows Nouveau

NOM	ADRESSE IP	NOM DNS	DOMAINE	ETAT	COMPTE	NOM NETBIOS
194.254.67.251	194.254.67.251	lthe99.hmg.inpg.fr		Off	administrateur	194.254.67.251
194.254.67.254	194.254.67.254	gw-lthe.hmg.inpg.fr		On	administrateur	194.254.67.254
BELLEUDY-P1		lthe-cermo-11.ujf-g...	HYDRO2	Off	belleudy-p1\adminis...	BELLEUDY-P1
DGZKRH2J			HYDRO2	Off	administrateur	DGZKRH2J
ESTEVEES-PORT			HYDRO2	Off	administrateur	ESTEVEES-PORT
HMGPC2	194.254.67.171	hmgpc2.hmg.inpg.fr	HYDRO	Off	administrateur	194.254.67.171
LAURENT-P160	152.77.120.26	lthe-cermo-26.ujf-g...	HYDRO2	??	laurent-p160\admini...	LAURENT-P160
LTHE000	194.254.67.164	lthe000.hmg.inpg.fr	HYDRO2	??	administrateur	LTHE000
LTHE-BC89537...			HYDRO2	Off	administrateur	LTHE-BC89537...
LTHECREUTIN						LTHECREUTIN
LTHELN11	194.254.67.217	ltheln11.hmg.inpg.fr		Off	administrateur	LTHELN11
LTHELN9	194.254.67.210	ltheln9.hmg.inpg.fr		Off	administrateur	LTHELN9
LTHEPC101	194.254.67.130	lthe99.hmg.inpg.fr		Off	administrateur	LTHEPC101
LTHEPC11	194.254.67.135	lthe99.hmg.inpg.fr		Off	administrateur	LTHEPC11

Gestionnaire des tâches en cours

Tâches actives : 0  
Tâches en attente : 0 [Vider la file d'attente](#)

Rafraichissement du réseau fini 122 machines (122 dans cette vue)

----- sécurité -----

- Tester la protection AntiVirus temps réel
- Vérifier la configuration "Windows update"
- Tester l'absence d'un logiciel
- Tester la présence d'un logiciel
- Vérifier la présence d'un anti-virus
- Tester un port réseau

----- performances -----

- Tester la fragmentation du disque système
- Vérifier l'espace disque disponible

Prise de contrôle

LTHE

Alertes

Configuration

Maintenance

Informations

Ajout-Suppression de Programmes

Rafraichir l'état

Assigner label

Envoyer un email

Exclure de la liste

Retirer de la liste

Propriétés