**PRODUCTION ASSOCIEE**

**Contexte :**

Le contexte de la Maison des Ligues de Lorraine (La M2L) a été retenu au sein de notre centre de formation dans le cadre des PPE. La M2L, établissement du Conseil Régionalde Lorraine, est responsable de la gestion du service des sports et en particulier des ligues sportives ainsi que d’autres structures hébergées. La M2L doit fournir les infrastructures matérielles, logistiques et des services à l’ensemble des ligues sportives installées. Elle assure l’offre de services et de support technique aux différentes ligues déjà implantées (ou à venir) dans la région.

L’une des préoccupations de l’administrateur est d’automatiser au maximum des tâches administratives pour répondre rapidement aux différentes sollicitations des départements de la M2L et des ligues sportives. C’est dans ce contexte que j’ai participé, avec d’autres élèves de mon groupe, au projet consistant à créer des VLANs, configurer les routeurs en OSPF et à mettre en place un serveur TSE pour permettre aux utilisateurs d’une ligue sportive de travailler à distance sur une application commune, la suite bureautique Open Office ou d’autres applications dans notre cas.

**RESEAU :**

Le réseau de la M2L est organisé VLANs et comporte des commutateurs de niveau 2 et des routeurs.

Le VLAN INFORMATIQUE est dédié aux serveurs : contrôleur de domaine, DHCP et serveur d’applications. Les ligues sont organisées aussi en VLANs. Au niveau du domaine la M2L et les ligues sont représentées en unités d’organisation. Les serveurs sont en Windows 2003 SP2 & les clients en Windows XP SP3 ou Seven.

**Liste du matériel :**

3 routeurs Cisco

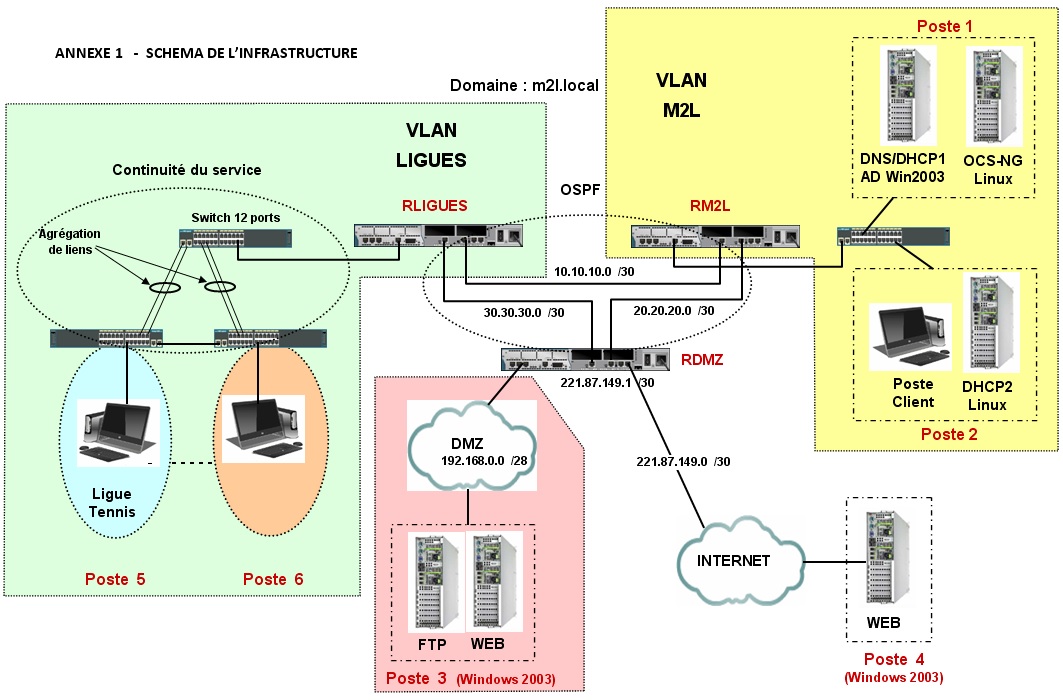
4 switch cisco

2 switch non manageable

Serveur 2003 vistualisé

Postes clients XP

**Schéma :**

****

Pour les liaisons entre routeurs/routeurs et les switchs/switchs, on utilise des câbles croisé. Pour les liaisons entre switch et routeurs on utilise des câbles droits.

Les routeurs utilisent le protocole OSPF (Open Shortest Path First), c’est un algorithme dynamique  à état de liens, qui permet de mettre à jour la table de routage automatiquement grâce aux messages hello échangés entre les routeurs.

Les switchs sont reliés aux routeurs par un lien Trunk, c’est un lien qui permet de faire transiter plusieurs VLANs sur un seul lien physique.

Afin d’éviter une situation de tempête de diffusion, on utilise le protocole spanning-tree qui permet de mettre fin à une tempête de broadcast en coupant temporairement un lien afin de cassé la boucle.

**CONFIGURATION :**

###################CONFIG RESEAU######################

Mot de passe console : cisco

Administration à distance (SSH) : login : admin MDP : admin

##### Adresses de gestion :

RouterM2L : 10.10.10.2

RouterLIGUES : 10.10.10.1

RouterDMZ : 20.20.20.2

SWLIGUE1 : 172.16.99.17

SWLIGUE2 : 172.16.99.18

SWLIGUE3 : 172.16.99.19

SWM2L : 172.16.99.1

SWDMZ : 172.16.99.33

####################RouterM2L#########################

en

conf t

hostname RouterM2L

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int fa 0/1

ip address 10.10.10.2 255.255.255.252

no shutdown

exit

int fa 0/0

ip address 20.20.20.1 255.255.255.252

no shutdown

exit

int eth 1/0

no shutdown

exit

int eth 1/0.2

encapsulation dot1Q 2

ip address 172.16.0.62 255.255.255.192

exit

int eth 1/0.3

encapsulation dot1Q 3

ip address 172.16.0.126 255.255.255.192

ip helper-address 172.16.0.61

ip helper-address 172.16.0.60

exit

int Eth 1/0.99

encapsulation dot1Q 99

ip address 172.16.99.14 255.255.255.240

exit

router ospf 1

network 172.16.0.0 0.0.0.63 area 0

network 172.16.0.64 0.0.0.63 area 0

network 172.16.99.0 0.0.0.15 area 0

network 10.10.10.0 0.0.0.3 area 0

network 20.20.20.0 0.0.0.3 area 0

passive-interface Ethernet 1/0

exit

####################RouterLIGUES#####################

en

conf t

hostname RLIGUES

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int Fa 0/1

ip address 10.10.10.1 255.255.255.252

no shutdown

exit

int Eth 1/0

ip address 30.30.30.2 255.255.255.252

no shutdown

exit

int Fa 0/0

no shutdown

exit

int Fa 0/0.10

encapsulation dot1Q 10

ip address 172.16.10.62 255.255.255.192

ip helper-address 172.16.0.61

ip helper-address 172.16.0.60

exit

int Fa 0/0.11

encapsulation dot1Q 11

ip address 172.16.11.62 255.255.255.192

ip helper-address 172.16.0.61

ip helper-address 172.16.0.60

exit

int Fa 0/0.12

encapsulation dot1Q 12

ip address 172.16.12.62 255.255.255.192

ip helper-address 172.16.0.61

ip helper-address 172.16.0.60

exit

int Fa 0/0.99

encapsulation dot1Q 99

ip address 172.16.99.30 255.255.255.240

exit

router ospf 1

network 172.16.10.0 0.0.0.63 area 0

network 172.16.11.0 0.0.0.63 area 0

network 172.16.12.0 0.0.0.63 area 0

network 172.16.99.16 0.0.0.15 area 0

network 10.10.10.0 0.0.0.3 area 0

network 30.30.30.0 0.0.0.3 area 0

passive-interface FastEthernet 0/0

end

##########################RouterDMZ#############################

en

conf t

hostname RDMZ

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int fa 0/0

ip address 20.20.20.2 255.255.255.252

ip nat inside

no shutdown

exit

int fa 0/1

ip address 221.87.149.6 255.255.255.248

ip nat outside

ip access-group 100 in

no shutdown

exit

int Eth 1/0

ip address 30.30.30.1 255.255.255.252

ip nat inside

no shutdown

exit

int Eth 1/1

ip address 192.168.0.14 255.255.255.240

ip nat inside

ip access-group 102 in

no shutdown

exit

router ospf 1

network 30.30.30.0 0.0.0.3 area 0

network 20.20.20.0 0.0.0.3 area 0

network 192.168.0.0 0.0.0.15 area 0

passive-interface Ethernet 1/1

default-information originate

exit

ip route 0.0.0.0 0.0.0.0 fa0/1

access-list 10 permit 172.16.0.0 0.0.255.255

ip nat inside source list 10 interface fa0/1 overload

ip nat inside source static tcp 192.168.0.5 80 221.87.149.6 80

ip nat inside source static tcp 192.168.0.5 443 221.87.149.6 443

! ----------- Filtrage Firewall -------------------

access-list 100 permit tcp any 172.16.0.0 0.0.255.255 established

access-list 100 permit tcp any host 192.168.0.13 eq 80

access-list 100 permit tcp any host 192.168.0.13 eq 443

access-list 100 permit tcp any host 192.168.0.12 eq 21

access-list 100 permit tcp any host 192.168.0.12 eq 20

access-list 100 permit icmp any host 172.16.0.54 echo-reply

access-list 100 permit icmp any host 172.16.0.55 echo-reply

access-list 100 permit icmp any host 172.16.0.54 unreachable

access-list 100 permit icmp any host 172.16.0.55 unreachable

access-list 102 permit icmp any host 172.16.0.54 echo-reply

access-list 102 permit icmp any host 172.16.0.55 echo-reply

access-list 102 permit icmp any host 172.16.0.54 unreachable

access-list 102 permit icmp any host 172.16.0.55 unreachable

############################SWLIGUE1##############################

en

conf t

hostname SW1LIGUE

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int range fa 0/2-3

channel-group 1 mode on

exit

int port-channel1

switchport mode trunk

switchport nonegotiate

exit

int range fa 0/4-5

channel-group 2 mode on

exit

int port-channel2

switchport mode trunk

switchport nonegotiate

exit

int fa 0/1

switchport mode trunk

exit

VLAN 99

name GESTION

exit

int VLAN 99

ip address 172.16.99.17 255.255.255.240

ip default-gateway 172.16.99.30

exit

###########################SWLIGUE2##############################

en

conf t

hostname SW2LIGUE

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int range fa 0/1-2

channel-group 1 mode on

int port-channel1

switchport mode trunk

switchport nonegotiate

VLAN 10

name ATHLE

VLAN 11

name TENNIS

VLAN 12

name BASKET

VLAN 99

name GESTION

int VLAN 99

ip address 172.16.99.18 255.255.255.240

ip default-gateway 172.16.99.30

int range fa 0/4-8

switchport mode access

switchport access VLAN 10

spanning-tree portfast

exit

int range fa 0/8-12

switchport mode access

switchport access VLAN 11

spanning-tree portfast

exit

int fa 0/3

switchport mode trunk

exit

##########################SWLIGUE3############################

en

conf t

hostname SW3LIGUE

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

int range fa 0/1-2

channel-group 1 mode on

exit

int port-channel1

switchport mode trunk

switchport nonegotiate

exit

VLAN 10

name ATHLE

exit

VLAN 11

name TENNIS

exit

VLAN 12

name BASKET

exit

VLAN 99

name GESTION

exit

int VLAN 99

ip address 172.16.99.19 255.255.255.240

ip default-gateway 172.16.99.30

exit

int range fa 0/4-8

switchport mode access

switchport access VLAN 12

spanning-tree portfast

exit

int fa 0/3

switchport mode trunk

exit

###########################SWM2L##########################

en

conf t

hostname SWM2L

no ip domain-lookup

no logging console

enable secret cisco

ip domain-name M2L.local

user admin secret admin

line vty 0 15

login local

transport input ssh

exit

crypto key generate rsa

1024

ip ssh version 2

ip ssh time-out 60

ip ssh authentication-retries 2

VLAN 2

name INFO

exit

VLAN 3

name ADMIN

exit

VLAN 99

name GESTION

exit

int fa 0/1

switchport mode trunk

switchport nonegotiate

exit

int range fa 0/2-11

switchport mode access

switchport access VLAN 2

spanning-tree portfast

exit

int range fa 0/12-16

switchport mode access

switchport access VLAN 3

spanning-tree portfast

exit

int VLAN 99

ip address 172.16.99.1 255.255.255.240

ip default-gateway 172.16.99.14

exit

**LE SYSTEME :**

Nous utiliserons le logiciel Virtual Box afin de simulée un environnement Windows Serveur 2003, qui joue le rôle de Contrôleur du domaine –Serveur DHCP- Serveur TSE :

-le contrôleur de domaine reflètera l’organisation de la Maison des Ligues, nous y trouverons ainsi les différentes représentées sous forme d’unité d’organisation. C’est dans l’active directory qu’on fera les stratégie de groupe afin de déployé des applications.

- Serveur DHCP (Dynamic Host Configuration Protocol) : Ce protocole dont le rôle est d’assurer la configuration automatique des paramètres IP d’une [station](http://fr.wikipedia.org/wiki/Station_de_travail), notamment en lui affectant automatiquement une [adresse IP](http://fr.wikipedia.org/wiki/Adresse_IP) et un [masque de sous-réseau](http://fr.wikipedia.org/wiki/Masque_de_sous-r%C3%A9seau). Nous allons créer différents plage d’adresse IP pour les différents Ligues de la M2L.

-WIN INSTALL LE: Cette application nous permet de convertir une application .exe en un paquet .msi (Microsoft System Installer )

Procédure de création d’un fichier MSI

# Principe de fonctionnement

Les fichiers MSI correspondent à des packages d’un ensemble de fichier permettant une installation automatisée des applications.

Leur principal intérêt est qu’avec ce type de fichier, un déploiement via GPO est possible ce qui facilite alors la mise en place des applications sur l’ensemble des postes puisqu’ainsi il n’est pas nécessaire d’intervenir sur les machines distantes.

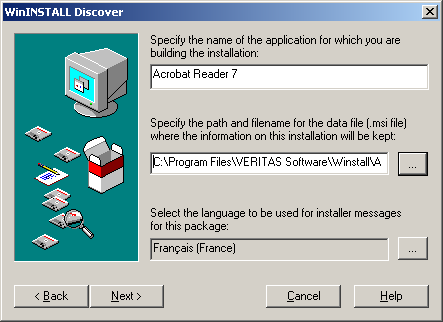
Le principe est simple, et se passe en 2 temps :

* on réalise une première analyse du registre avant l’installation du logiciel que l’on désire déployer
* on réalise dans un second temps, une nouvelle analyse du registre avec cette fois les modifications engendrées par l’installation du logiciel.

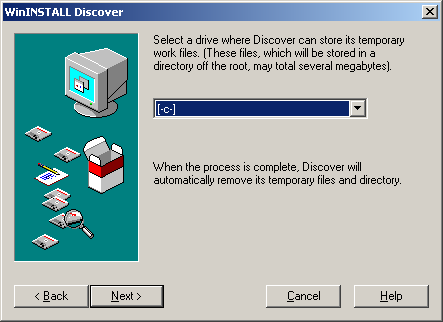
La différence entre ces 2 captures génère les valeurs de notre fichier MSI.

# Réalisation d’une capture instantanée Avant :

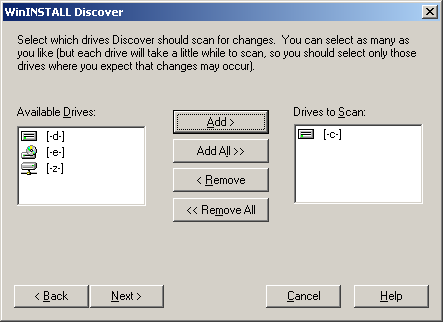
La première phase consiste à réaliser une capture instantanée AVANT toutes modifications ; En règle générale, il est conseillé de réaliser cette analyse sur un système « vierge », juste après une réinstallation « propre » de Windows.



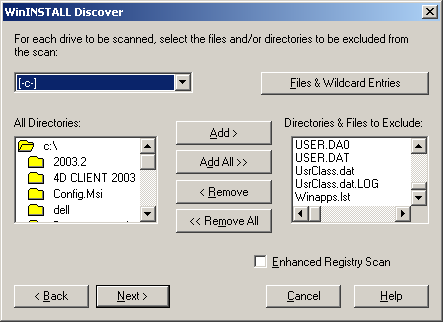
1. Sélectionner le disque que vous désirez utiliser pour stocker les fichiers de travail temporaires.



1. Sélectionnez ensuite les disques à surveiller pour identifier les changements qui pourraient intervenir suite à l'installation du logiciel.



1. Il est ensuite possible d'exclure de la surveillance un certain nombre de répertoire. Sauf cas particulier, gardez les paramètres par défaut.

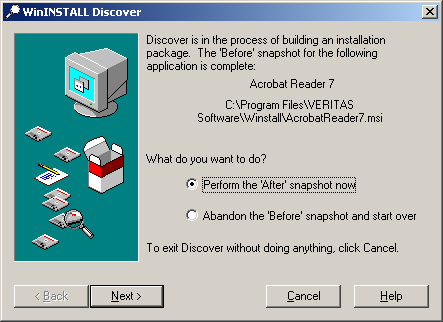


1. **WinINSTALL Discover** va alors réaliser un instantané de la configuration de l'ordinateur afin de pouvoir par la suite déterminer les changements effectués par l'application.

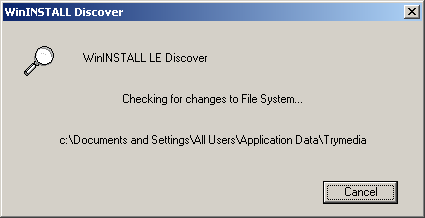
# Réalisation d’une capture instantanée Après :

La phase d'installation de l'applicatif a réalisé des modifications à tous les niveaux du système. Il est donc nécessaire d'identifier toutes les modifications réalisées pour les reproduire lors de l'installation à partir du système Windows 2000.

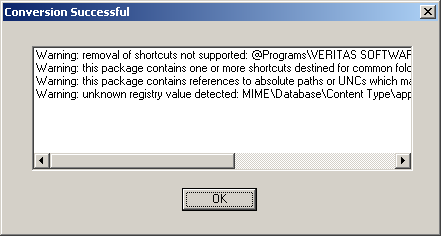
1. Allez dans **Démarrer\Programmes\VERITAS Software\VERITAS Discover\** puis cliquez sur **VERITAS Discover**.



1. Cliquez sur Next. **VERITAS Discover** va analyser les changements entre l'instantané Avant et l'état actuel du système pour en générer le lot Windows Installer de l'application.



1. Une fois le package généré une boite de dialogue **Conversion Successfull** va s'afficher avec une liste d'avertissements (ex: référence à des chemins absolu,... ). Vous pouvez cliquez sur OK.



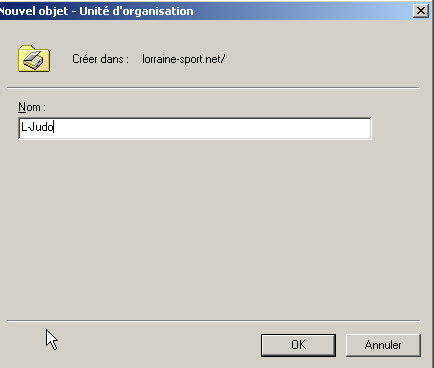
1. Puis une nouvelle fois, cliquez sur OK dans la boite de dialogue **After Snapshot Complete**.

Votre MSI est maintenant prêt à être déployé.

**MISE EN PLACE DE GPO AFIN DE DEPLOYER LE PAQUET MSI :**

Une ligue équivaut à une unité d’organisation => Nous allons donc crée une unité d’organisation Judo et intégrer des utilisateurs (ex : D.Douillet et T.Rinner)

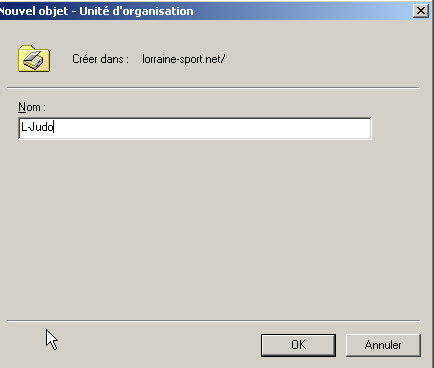
Pour cela je clic droit sur le domaine « lorraine-sport.net » je vais sur « nouveau » puis je selectionne « Unité d’organisation ».



Dans cette Unité d’oganisation de nouveau clic droit, puis « nouveau »,  « Utilisateur », et la je nomme mon client et je lui attribue un mot de passe. Je réitère l’opération pour mon autre Utilisateur (T.Rinner)

* Je crée un lecteur de partage dans lequel j’intègre les différents logiciels applicatifs que je dois déployer. Dans Ce Dossier de partage je définirai les droits des utilisateurs de l’unité d’organisation « L- Judo ».

Pour cela je rentre dans le disque dur C : , je crée un « Nouveau dossier » dans le lequel j’intègre les différents logiciels que je dois déployer puis une fois cette démarche faite je me dirige sur partage et sécurité.

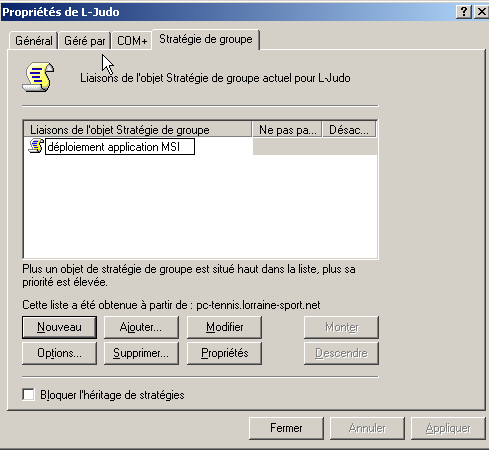


• Je crée un lecteur de partage dans lequel j’intègre les différents logiciels applicatifs que je dois déployer. Dans Ce Dossier de partage je définirai les droits des utilisateurs de l’unité d’organisation « L- Judo ».

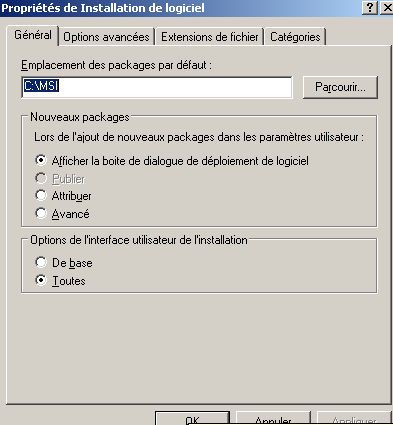
Pour cela je rentre dans le disque dur C : , je crée un « Nouveau dossier » dans le lequel j’intègre les différents logiciels que je dois déployer puis une fois cette démarche faite je me dirige sur partage et sécurité.



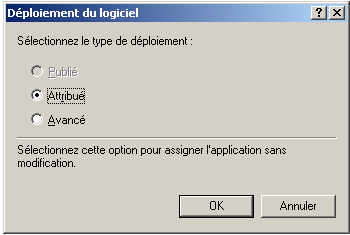
* Puis nous allons crées une stratégie de groupe dans laquelle nous intègrerons « VLC.msi » et « Mozilla Firefox .MSI». Dans cette stratégie, nous déploierons ces différentes applications et demanderons sa mise en place des le démarrage de la machine.

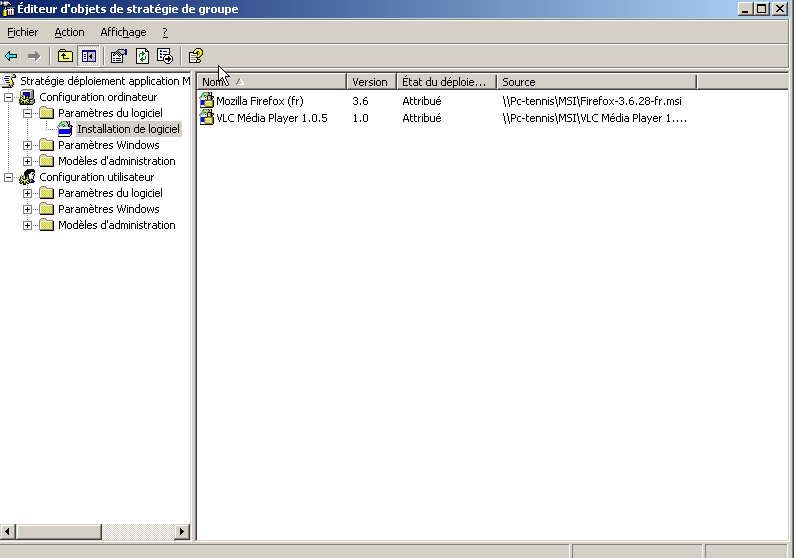


Je me dirige vers  «  modifier » /  « configuration ordinateur »/ « parametre du logiciel » /  « installation du logiciel »Clic droit « propriété » : je montre l’emplacement dans lequel se trouve le dossier de partage.

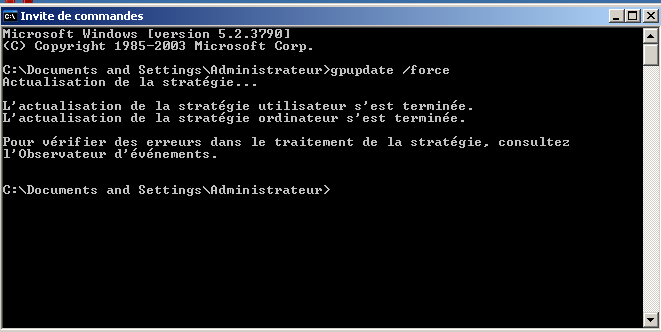


Clic droit « nouveau package » puis je selectionne le dossier de partage precedemment créer et enfin je selectionne les fichiers que je veux déployer.





* J’effectue un « gpupdate /force » dans le « cmd ». Cette commande permet de mettre à jour les différentes stratégies mise en œuvre sur Active Directory.



* Cette tache effectuée j’ouvre la session d’un poste client du Vlan judo et je verifie que les différentes stratégies mise en œuvre sur Active Directory.

