Centre Universitaire d'Éducation et de Formation des Adultes Centre Régional de CNAM

WINDOWS NT 2000: Travaux Pratiques

- S 4 -

Michel Cabaré Juin 2003

ver 1.4

CUEFA - Département Formation Continue

BP 68

38402 ST MARTIN D'HÈRES



TABLE DES MATIÈRES

Réseau « SIMPLE » manuellement Objectifs et fonctionnalités : Création du domaine manuel.net : Installation du serveur DNS : Configuration du serveur DNS : Inscription du DC dans le serveur DNS : Ajouter les Hôtes et tester le serveur DNS :	7 7
Test de DNS Test DNS et Paramétrage TCP/IP des clients du domaine : nslookup : Test de résolution inverse :	10 10 10 11
Modifier le fichier hosts	13 13
Modifier le fichier Imhosts Inscrire une machine simple dans Imhosts : Inscrire un Contrôleur de Domaine dans Imhosts :	14 14 15
Test installation de AD Vérification configuration IP: Vérification des enregistrement de ressource SRV Vérification du dossier SYSVOL Vérification de la base de donnée d'annuaire et des fichiers journaux Vérification des journaux d'événement	17 17 17 19 19 19 19
Accès à internet Après installation d'un serveur DNS : Suppression de la zone DNS racine Utilisation des indications de racine Utilisation des redirecteurs Indication de la passerelle à utiliser.	20 20 21 21 21 21



Windows NT 2000 travaux pratiques

MISE en œuvre DHCP	22
Installation d'un serveur DHCP :	
Sécuriser un serveur DHCP :	23
Augmenter les sauvegardes automatique serveur DHCP :	23
	0.4
Paramétrage d'un client 2000 :	24 25
Paramétrage d'un client non 2000 :	
Publication restrainte dans AD	
	2/
Objectit : Publication sélective dans A.D. :	27 27
Recherche de dossiers partagés :	
Dálágation compátonco sur UO	
Delegation competence sur uC	30
Objectit : Mise en place délégation :	30 30
Utilisation de la délégation :	
Ajouter une délégation :	32
Modifier-Supprimer une délégation :	33
Commande Net send	24
La base de la commande Net send :	34
Commande Net user	35
La base de la commande Net user :	35
Les paramètres optionnels :	35
Script solon I'OS	
	37
Variable d'environnement :	3/ 37
Version d'OS :	
Corrigat our out of the statute	
script groupe utilisateurs	40
Tester l'appartenance à un groupe précis :	40
Solution native : Avec le resource kit	40 41
Script wsh	42
Mise en place des scripts :	42
1° script en vbs :	
un exemple en vos :	44
ID évènement	45
Signification d'un ID du gestionnaire évènement	

Windows NT 2000 travaux pratiques

Microsoft*

ndow

Å

cué

Cabaré Michel C.U.E.F.A. S4 T.P. v1.4 Page 3

Moniteur	system	e:	alerte	sur	une
imprimant Paramétrage Seuil	d'alerte :				47
Déclenchement Se	uil d'alerte :				
Moniteur	systeme	disc	que logio	que	50
Compteur sur disqu	e logique :			•	50
Alerte saturation de	• alsque :	••••••			51
Script de i	mise a l'	heu	re		52
Création du script : Droit de modification	on de l'heure syst	 ème :			52 52
Exemple d'écrasen	nent entre stratég	gie locale	e et stratégie de [DC :	54
Stratégie l	ocale 1	0			
Augmenter la sécu	rité :				55
Stratégie	locale 2	0			F7
Pister les tentatives		•••••			5/ 57
Audit sur le client :					57
Audit sur le serveur	·	•••••			58
Stratégie .	AUDIT a	cce	s dossier	.	59
Objectif :		•••••			59
Stratégie /	AUDIT in	nprir	nante		62
Savoir qui imprime :					62
Modele d	e straté	nie I	ocale		12
Objectif :	C Share				63 63
Création et sauveg	arde d'un modèl	le :			63
	lisation a un moc	iele :			64
Création (de GPO	sur	une UO.		66
Objectifs :	D ot cróor lour C				66
Changer d'UO = ch	anger de GPO :	,		•••••••••••••••••••••••••••••••••••••••	68
Forcer une applica	tion de GPO ave	c secedi	t :		69
GPO Ma	odèle	d'a	dministra	ation	de
domaine.					70
Objectifs :	ágia pour l'admir	oistratour			70
Mise en oeuvre de	la stratégie de do	omaine :			70 71
A Microsoft	Windows NT	2000	Cabaré Miche	l Pc	ige 4
	travaux prat	iques	C.U.E.F.A. S4 T.F	P. v1.4	~

GPO déploiement de Service Pa	ck75
Objectifs : Mise en oeuvre :	75 75
Creation a Uniot MSI	77
Objectifs :	
Installation du logiciel creation de msi :	
Installation du logiciel pour lequel on veut un msi :	
instantané après:	79
FFS - Cryptage de fichier	00
2 utilizateurs indés and entre	
sur une machine autonome	80
Dans un domaine	
Exportation Import de certificat :	
Exportation du certificat de pierre sur disquette	
Importation au certificat de pierre dans paul	83 84
EFS – Sécuriser un poste	
Vol d'un poste (portable ?) :	
Export du certificat de l'agent de récupération d'un poste autonome	:86
Import du certificat de l'agent de récupération d'un poste autonome	; :87
Sassian Tarminal Sarvar	
Analyser une session IS :	
Test de duplication d'AD	00
Créar un 2º CD sur patra Domaina :	
Visualisation du trafic de duplication :	
Réplication inter-site	
Créons 2 sites distants de 62 machines maximum relié par RNIS:	
Créer les sites nécessaires :	94
Définir un sous -réseau :	
Associer un sous -reseau a un sire:	
On oublie pas de poser un Contrôleur de domaine dans chaque site:	
Iransfert de maitre d'operation	
Objectif :	97
Cráation d'un Domaine Enfant	
Creation a un Domaine Enfant	
Création du C.D. "enfant.dom1.com" sur serveur S4 :	
verification des relations d'approbations :	101 102
Création d'une délégation sur le serveur DNS racine :	
<u> </u>	
Windows NT 2000 Cabaré Michel travaux pratiques C.U.E.F.A. S4 T.P. v1.4	Page 5

Å

cue

Installation du serveur DNS enfant :	104
test des zones DNS parent et enfant :	105
Création du C.D. "dans la forêt dom2.com" sur serveur S5: Vérifions les relations d'approbation : Localisation des maîtres d'opération :	fôrêt107
L'utilitaire dcdiag	111
Récupération de l'utilitaire dcdiag :	111
Quelques test possibles :	111
Installation Muette depuis CD	113
Objectifs et fonctionnalités :	113
Réponse :	113





RESEAU « SIMPLE » MANUELLEMENT

Objectifs et fonctionnalités :

Il s'agit de présenter ici un réseau local, constitué d'un seul Domaine, On va essayer de faire le plus d'étapes manuellement... Le Serveur NT 2000 nommé s1-man et de clients tantôt Windows 95-98 nommés win-man1, win-man2 tantôt NT 2000 professionnel nommés win2k-1, win2k-2

le protocole choisit est TCP/IP, Les adresse IP sont donnée manuellement avec **192.168.1.X** où X sera le n° de la machine sur laquelle on travaille, le masque de sous-réseau sera pour tous **255.255.255.0**

N.B: pour se « mettre » en situation d'un Contrôleur nouvellement installé, il suffit d'exécuter **DCPROMO** pour rétrograder le serveur, en précisant bien qu'il s'agit du dernier contrôleur de Domaine, et de demander de désinstaller DHCP et DNS dans Ajouter/supprimer des composants windows configuration, demandant du panneau de en 🔲 🚆 Services de mise en réseau puis Détail et décocher DNS et éventuellement DHCP ! on peut finir le "ménage" en supprimant dans Winnt\system32\ le contenu des dossiers DNS et DHCP éventuels

Création du domaine manuel.net :

Démarrer/Exécuter et tapez ensuite dcpromo. Dans l'« l'assistant installation Active directory » il faut alors répondre

- 1. Contrôleur de domaine pour un nouveau domaine
- 2. Créer une nouvelle arborescence de domaine
- 3. Créer une nouvelle forêt d'arborescence de domaines
- 4. Donner le nom DNS en manuel.net
- 5. Accepter le nom Netbios proposé , pour nous ici manuel
- 6. Choisir un emplacement pour les fichiers stockant Active Directory, comme ...\WINNT\NTDS (accepter l'emplacement proposé)
- 7. indiquer le lecteur NTFS comme destination du dossier Sysvol de publication d'Active Directory ...\WINNT\SYSVOL
- 8. lorsque l'assistant détecte que il n'y a pas de DNS disponible, <u>ne</u> <u>pas demander d'en créer un</u>
- 9. Autoriser la compatibilité avec les versions antérieures de NT
- 10. indiquer un mot de passe de restauration de service d'annuaire, par exemple **zk28a**

Puis re démarrer le poste



Installation du serveur DNS :

Pour installer un serveur DNS sur un serveur NT2000 Server il faut aller dans Ajouter/supprimer des composants windows du panneau de configuration, en demandant

🔲 🚔 Services de mise en réseau

puis Détail et cocher **DNS** ! (le CD est nécessaire)

Configuration du serveur DNS :

On a installé un serveur DNS; reste à l'installer soit via l'assistant en se positionnant dessus (après avoir lancé la console d'administration DNS par démarrer / programme / Outils d'administration / DNS) et en demandant le menu Action / Configurer le serveur



Dans les boites de « l'assistant configuration de serveur DNS » on réponds :

- 1. Ceci est le premier serveur DNS sur le réseau
- 2. Créer une zone de recherche directe
- 3. en Zone principale standard
- 4. donner le nom de la zone, ici pour nous manuel.net
- 5. accepter de créer le nouveau fichier manuel.net.dns
- 6. Créer une zone de recherche inversée
- 7. en Zone principale standard
- 8. avec un ID réseau de 210.200.200
- 9. accepter de créer le nouveau fichier 210.200.200.in-addr.arpa.dns

Inscription du DC dans le serveur DNS :

A l'heure actuelle on a un serveur 2000, C.D. et sur ce serveur 2000 on dispose d'un serveur DNS opérationnel

Il faut "inscrire tous les enregistrements SRV correpondant à mon domaine dans le DNS



Après s'être bien assuré que la zone accepte les mises à jours dynamiques,

	DNS	Propriétés de dom1.com		? ×
	$\begin{array}{c c c c c c c c c c c c c c c c c c c $	Serveurs de noms Général État : En cours d'exécutio Type : Principale	WINS Transfert Source de noms (Si on	s de zone DA) Pause Modifier
zone nommée dom1.com	È-(a) . dom1.com E-C Zones de recherche inversée E-C Recherches mises en cache	Nom de fichier zone : dom1.com.dns Autoriser les mises à jour dynamiques ?		

on lance sur le serveur une commande

net stop netlogon

C:	∖>net sto	op netlogo	٦					
Le	service	Ouverture	de	session	réseau	s	'arrê	ite.
Le	service	Ouverture	de	session	réseau	a	été	arrêté.

suivit de

net start netlogon

C:`	∖>net sta	art netlogo	n			
Le	service	Ouverture	de	session	réseau	démarre
Le	service	Ouverture	de	session	réseau	a démarré.

Ajouter les Hôtes et tester le serveur DNS : 🚊 DNS Se plaçant sur le zone de résolution crée, 🚊 <u>C</u>onsole on demande soit <u>F</u>enêtre 2 Action Affichage $\Leftrightarrow \Rightarrow$ £ Arbre Pour une Zone de recherche Directe Action/ nouvel hôte 🚊 DNS 🖻 📲 NTSERV-SIMP 🗄 💼 Zones de recherche directes Ė~@]. Pour une Zone de recherche inversée 🦾 🕞 manuel.net Action/ nouveau pointeur 🔄 🛄 Zones de recherche inversée Nouvel hôte ? X Emplacement : manuel.net Nom (utilise le domaine parent si ce champ est vide) Nouvel enregistrement de ressource ? X Pointeur (PTR) Adresse IP 0 0. 0. 0. Sous-réseau : 200.200.210.in-addr.arpa 🔲 Créer un pointeur d'enregistrement PTR associé Numéro IP de l'hôte 210 .200 .200 .0 Nom de l'hôte : Parcourir... Ajouter un hôte Annuler





Windows NT 2000 travaux pratiques

TEST DE DNS

Test DNS et Paramétrage TCP/IP des clients du domaine :

Le paramétrage de l'adresse du serveur DNS sur les clients peut se tester via IPCONFIG/ ALL ou Winipcfg

🚊 DNS Fenêtre - 2 La bonne marche du serveur DNS peut se tester via les Action Affichage propriété du Serveur DNS dans la console MMC de Arbre gestion du DNS 🚊 DNS E NTSERV-SIMP Propriétés de NTSER¥-SIMP ? X 🚊 🛄 Zones de recherche dire Redirecteurs Avancé Interfaces L Indications de racine Enregistrement Analyse Sécurité Pour vérifier la configuration du serveur, vous pouvez effectuer un test Onglet automatique ou manuel Analyse Sélectionnez un type de test : ✓ Une requête simple à un serveur DNS Une requête récursive aux autres serveurs DNS Pour effectuer le test immédiatement, cliquez sur Tester. Tester Effectuer un test automatique avec l'intervalle suivant : Intervalle de test : 1 Minutes Résultats des tests Requête sim. Date Heure Requête réc 23/02/2001 00:09:34 Correct 23/02/2001 00:07:08 Correct

On peut s'assurer que tous les clients du réseau ait bien leur adresse résolue sur notre serveur DNS, la bonne marche des enregistrement dans le DNS peut se tester via la commande **Nslookup**

nslookup:

Par exemple on teste que le client nommé ntpro-simp2 d'adresse 200.200.202.202.soit bien résolu sur notre serveur DNS **ntserv-simp**







Windows NT 2000 travaux pratiques

Normal, encore faut il :

1. dans le serveur DNS rentrer le poste dans la zone de recherche

Nouvel hôte	? X
Emplacement :	
simple.net	
Nom (utilise le domaine parent si ce champ est vide) :	
ntpro-simp2	
Adresse IP : 200 .200 .200 .201	
Créer un pointeur d'enregistrement PTR associé	

de manière à obtenir

Arbre	Nom	Туре	Données
	_msdcs		
	Lites		
Zones de recherche directes	🖾 _tcp		
	🖾 _udp		
	🗒 (identique au dossier parent)	Source de nom	[21], ntserv-simp.sim
🕂 🛄 _msdcs	🗒 (identique au dossier parent)	Serveur de noms	ntserv-simp.simple.ne
ites ⊡	🗒 (identique au dossier parent)	Hôte	200.200.200.201
🕂 🕀 🛄 _tcp	🗒 ntserv-simp	Hôte	200.200.200.201
	🗒 ntpro-simp2	Hôte	200.200.200.202
😟 🛄 Zones de recherche inversée			

2. préciser sur le client l'adresse du serveur DNS à contacter...

et lorsque l'on re-teste que le client nommé ntpro-simp2 d'adresse 200.200.200.202soit bien résolu sur notre serveur DNS ntserv-simp

Cela marche !!!...

🖼 Invite de commandes - nslookup	
> ntpro-simp2 ntserv-simp Serveur : ntserv-simp.simple.net Address: 200.200.200.201	
Nom : ntpro-simp2.simple.net Address: 200.200.200.202	

Test de résolution inverse :

La **résolution inverse** n'est pas nécessaire au fonctionnement des mécanismes 2000, et pourtant elle peut expliquer par exemple pour quoi on a un message d'erreur lorsque l'on lance nslookup...

Ainsi sur la machine ci dessous sur laquelle on a fait un ipconfig /all

Suffixe DNS spéc. à la	a c	:01	nne	ex	ioı	h.	:	
Description								3Com EtherLink III ISA (3C509b-TPO)
Adresse physique								00-20-AF-C5-21-51
DHCP activé								Non
Adresse IP	-			-		-		192.168.1.8
Masque de sous-réseau	-					-		255.255.255.0
Passerelle par défaut						_		
Serveurs DNS	_					_		192.168.1.22

puis un nslookup, on obtient







pourquoi?

parce que on essaye de faire un résolution inverse de l'adresse 192.168.1.22 qui est notée comme étant l'adresse du serveur DNS à interroger.

Pour que cela fonctionne, il faut sur le serveur DNS, se créer une zone de recherche inversée, et y rentrer ensuite

ouvel enregistrement de ressource	? ×
Pointeur (PTR)	
Sous-réseau :	
1.168.192.in-addr.arpa	
Numéro IP de l'hôte :	
192 .168 .1 .22	
Nom de l'hôte :	
[serveur2]	Parcourir

alors on pourra obtenir lors de l'appel à nslookup

E:∖>nslo	okuj	p			J
Serveur	par	défaut	: :	serveur2	
Address	· 19	92.168.	1.23	2	



MODIFIER LE FICHIER HOSTS

Inscrire une machine dans hosts :

Le fichier est fournit directement dans les postes 2000, ou avec une extension **.sam** sur les postes win98

Inscrivons le poste nommé **test** d'adresse **192.168.1.33** dans la table de résolution locale



du coup si avant o n'avait aucune possibilité , on peut désormais au moins envoyer la trame...

C:\>ping test Hôte inconnu test. C:\>ping test Envoi d'une requête 'ping' sur test [192.168.1.33] avec 32 octets de données : Délai d'attente de la demande dépassé. Statistiques Ping pour 192.168.1.33: Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%), Durée approximative des boucles en millisecondes : minimum = 0ms, maximum = 0ms, moyenne = 0ms



MODIFIER LE FICHIER LMHOSTS

Inscrire une machine simple dans Imhosts :

Inscrivons le poste nommé **pdistant** d'adresse **192.168.2.2** dans la table préchargée de résolution de nom netbios d'une machine:

Adresse 🗋 etc		
Adresse etc	etc Imhosts Fichier	Nom hosts Imhosts Imhosts.sam networks protocol cervices
Config Config	Modifié le: 09/05/2003 09:34 Taille : 4,18 Ko Attributs : (normal)	<u>₩</u> 36191C63

Il suffit d'éditer le fichier texte et d'y inscrire la ligne suivante

🖺 Imh	osts - W	ordPad						
Fichier	Edition	Affichage	e Inse	ertion	Format	?		
		6	#	×	è 🛍 •	റ	B	
192	.168.2	.2 PDI	STAN	T	#PRE			

On recharge par la commande nbtstat -R

C:\>nbtstat -R Purge et préchargement de la table nom de cache distant NBT terminés.

et on visualise par la commande **nbtstat -c**:

C:\>nbtstat -c Accton: Adresse IP du no	ud : [192 Table d	.168.1.3 le nom de	30] ID d'étendue : [] e cache distant NetBIOS	
Nom		Туре	Adresse d'hôte Vie	[sec]
PDISTANT PDISTANT PDISTANT PDISTANT	<pre><03> <00> <00> <20></pre>	UNIQUE UNIQUE UNIQUE	192.168.2.2 192.168.2.2 192.168.2.2 192.168.2.2	 -1 -1 -1



Inscrire un Contrôleur de Domaine dans Imhosts :

En général, on n'a pas besoin d'inscrire des postes génériques, mais plutôt un contrôleur de domaine...

Dans ce cas la ligne se complique un petit peu puisqu'il est nécessaire d'indiquer le nom de domaine en plus....

Il faut effectuer donc 2 entrées, une pour le PDC et l'autre pour le nom de domaine.

10.0.0.1 PDCName #PRE #DOM:Domain-name 10.0.0.1 "Domain-name \0x1b" #PRE

- **N.B** : Le nom de domaine dans cette entrée respecte la casse.
- **N.B:** L'espacement de ces entrées est obligatoire.
 - Remplacez 10.0.0.1 par l'adresse IP de votre contrôleur principal de domaine,

PDCName par le nom NetBIOS de votre contrôleur principal de domaine, **Domain** par le nom de domaine de Windows NT.

Inscrivons le contrôleur de domaine TEST nommé \$1 d'adresse 192.168.1.1 dans la table précharaée de résolution de nom netbios d'une machine:



la représentation hexadécimale NetBIOS du type de service).

NB: Attention, le fichier contient toujours une ligne blanche vide à la fin !



Ainsi une simple erreur de nombre de caractère (différent de 20 ici)

192.168.1.1	S1	#PRE	#DOM:TEST		
192.168.1.1	"TEST		\Ox1b"	#PRE	•

ne génère aucun message d'erreur, mais simplement une mauvaise inscription :

C:∖>nbtstat -c			
Accton: Adresse IP du no	oud : [192.168.1.2]	ID d'étendue : []	
	Table de nom de	cache distant NetBIC)S
Nom	Туре	Adresse d'hôte	Vie [sec]
S1 S1 S1 TEST TEST TEST TEST	<pre><03> UNIQUE <00> UNIQUE <20> UNIQUE <1C> GROUP <03> UNIQUE <00> UNIQUE <00> UNIQUE <20> UNIQUE</pre>	$\begin{array}{r} 192.168.1.1\\ 192.168.1.1\\ 192.168.1.1\\ 192.168.1.1\\ 192.168.1.1\\ 192.168.1.1\\ 192.168.1.1\\ 192.168.1.1\\ 192.168.1.1\\ 192.168.1.1\end{array}$	-1 -1 -1 -1 -1 -1 -1



TEST INSTALLATION DE AD

Vérification configuration IP:

Au niveau IP, II faut que le paramétrage serveur DNS soit configuré pour pointer vers lui-même... avec 127.0.0.1

Si ce n'est pas le cas, rafraîchir le cache avec la commande

C:\	∖>ip	conf	ig	∕f	1	ushd	lns		
Cor	ıfig	urat	ion	I	P	de	Windo	WS	2000
~			,	-			NUO		,

ipconfig /flushdns ^{Cache} de résolution DNS vidé.

suivie de la commande ipconfig /registerdns

C:\>ipconfig /registerdns
Configuration IP de Windows 2000
L'inscription des enregistrements de ressource pour toutes les cartes de cet ord inateur a été initiée. Toute erreur sera signalée dans l'Observateur d'événement s dans 15 minutes.

dans la console DNS on doit voire 3 enregistrement minimum...un Hôte pour le nom du serveur, un serveurs de nom et un source de nom.

🗒 (identique au dossier parent)	Source de nom
🗒 (identique au dossier parent)	Serveur de noms
📋 (identique au dossier parent)	Hôte
affichade détaillé cela do	nnerait

[25], s1.dom1.com., admini... s1.dom1.com. 192.168.3.1

en affichage détaillé cela donnerait

(identique au dossier parent)
 SOA
 (identique au dossier parent)
 NS
 (identique au dossier parent)
 A

[25], s1.dom1.com., admini... s1.dom1.com. 192.168.3.1

Vérification des enregistrement de ressource SRV

On regarde si les 4 dossiers suivants on été crées dans la zone DNS principale

÷	_msdcs
÷	_sites
	_tcp
·	_udp

et on liste les enregistrements de type SRV par un commande nslookup avec

Is -t SRV domaine

voire si on veut en garder une trace dans un fichier

Is -t SRV domaine >nomfich



et on peut décrypter un peu les enregistrement SRV à l'aide des informations suivantes

Enregistrement SRV	Critères de recherche
Idaptcp.Domaine_DNS.	Permet à un ordinateur de trouver un serveur LDAP dans le domaine
_ldaptcp.Sitesites.dc.	Permet à un ordinateur de trouver un contrôleur
_msdcs.Domaine_DNS.	de domaine sur le même site
_gctcp.Forét_DNS.	Permet à un ordinateur de trouver un serveur de catalogue global
_gctcp.Sitesites.Forêt_DNS	Permet à un ordinateur de trouver un serveur de catalogue global sur le même site
_kerberostcp.	Permet à un ordinateur de trouver un serveur
Domaine_DNS.	KDC dans le domaine
_kerberostcp.Site.	Permet à un ordinateur de trouver un serveur
_sites.Domaine_DNS.	KDC sur le même site
Les contrôleurs de d	omaine exécutant Windows 2000
inscrivent d'autres en	nregistrements SRV dans le sous-
domaine _msdcs au	format :
Service. Protocole	.DcType. msdcs.Domaine DNS

DcType pouvant valoir :

- dc pour Domain Controller
- gc pour Global Catalog

pour reconstruire la liste des enregistrement correspondant à AD dans le DNS on peut, après s'être bien assuré que la zone accepte les mises à jours dynamiques,

	🚊 DNS		a ()
	∫ 🚊 Console Eenêtre ?	Proprietes de dom1.com	<u>? ×</u>
	<u>Action</u> Affichage ↓ ⇐ → Arbre	Serveurs de noms WINS Général Source (Transferts de zone de noms (SOA)
	P, DNS	État : En cours d'exécution	Pause
Exemple ici pour une	ian III SI Ian IIII Zones de recherche directes	Type : Principale	Modifier
zone nommée	dom1.com	Nom de fichier zone :	
dom1.com		dom1.com.dns	
	├	Autoriser les mises à j <mark>Oui</mark> jour dynamiques ?	

on lance sur le serveur une commande

net stop netlogon

C:∖>net stop netlog	yon					
Le service Ouvertui	re de	session	réseau	s	' arré	Ète.
Le service Ouvertu	re de	session	réseau	a	été	arrêté.

suivit de

net start netlogon

C:N	Snet st;	awt netloou	n			
P	11100 300	Te neeroge	<u> </u>		,	- /
Le	service	Ouverture	de	session	réseau	démarre
	0011100			00001011	100000	
Le	service	Ouverture	de	session	réseau	a démarré.
	001 4 100			00001011	200044	

N.B: si le pb persiste on supprime la zone , puis on la recrée...



Vérification du dossier SYSVOL

Pour vérifier que le dossier SYSVOL à bien été crée il faut regarder si dans le dossier principal de NT on trouve le dossier **sysvol**....

Ce qui peut aussi se faire plus rapidement via

Ouvrir : %systemroot%\sysvol

dans lequel on doit trouver les 4 sous dossier suivants

Adresse 🗋 SYSVOL		
Nom 🛆	Taille	Туре
domain		Dossier de fichiers
📄 staging		Dossier de fichiers
🛅 staging areas		Dossier de fichiers
🔜 sysvol		Dossier de fichiers

La vérification du partage peut se faire rapidement via

📮 Gestion de l'ordinateur				<u>_ ×</u>
Action Affichage ← → 🔁 💽	■ 🗗 🗟 😫			
Arbre	Dossier par 🛆	Chemin d'accès partagé	Туре	Nb. de n
Gestion de l'ordinateur (local)	R ADMIN\$	C:\WINNT	Windows	0
🖻 📆 Outils système	∎€C\$	C:	Windows	0
💮 🗑 Observateur d'événements	R IPC\$		Windows	0
🗄 🖼 Informations système	RETLOGON	C:\WINNT\SYSVOL\sysvol\domaine1.edu\SCRIPTS	Windows	0
🗄 💮 🎆 Journaux et alertes de performar	Ressource	C:\ressource	Windows	0
🖻 😱 Dossiers partagés	SYSVOL	C:\WINNT\SYSVOL\sysvol	Windows	0
- 🕤 Partages				
Sessions				
Ouvrir les fichiers				
Gestionnaire de périphériques				

Vérification de la base de donnée d'annuaire et des fichiers journaux

Pour vérifier que la base de donnée à bien été crée il faut regarder si dans le dossier principal de NT on trouve le dossier **ntds**....

Ce qui peut aussi se faire plus rapidement via

Ouvrir : %systemroot%\ntds ▼

comprenant les fichiers suivants

Nom 🛆	Taille	Туре
Drop		Dossier de fichiers
🔊 edb.chk	8 Ko	Recovered File Frag
🗒 edb.log	10 240 Ko	Texte seulement
🔊 ntds.dit	10 256 Ko	Fichier DIT
🗒 res1.log	10 240 Ko	Texte seulement
🗒 res2.log	10 240 Ko	Texte seulement
🛋 temp.edb	2 064 Ko	Fichier EDB

Vérification des journaux d'événement

븘

🔢 Journal système **Directory Service** B DNS Server Service de réplication de fichiers



Windows NT 2000 travaux pratiques



ACCES A INTERNET

Après installation d'un serveur DNS :

Si vous installez DNS au cours du processus dcpromo, vous obtiendrez une zone racine. Celle-ci indique à votre serveur DNS qu'il est un serveur Internet racine. Par conséquent, votre serveur DNS n'utilisera pas de redirecteurs ou d'indications de racine lors du processus de résolution de noms.

Ce qui pour aller sur internet risque de poser probleme.

on ne peut pas spécifier les **Propriétés de SERVEUR2** redirecteurs (ils sont grisés)



Suppression de la zone DNS racine

Dans le Gestionnaire du DNS, développez l'objet Serveur DNS Développez le dossier Zones de recherche directe.



Cliquez avec le bouton droit sur la zone ".", puis demandez **Supprimer**.

Le serveur DNS va demander confirmation sur une action qui est irreversible



N.B: il faut bien penser à faire F5 pour que le DNS soit réactualisé !



Utilisation des indications de racine

A partir du moment ou la zone racine n'existe plus , les indications de racine sont utilisables par notre serveur DNS

Avantage : on est standard, et on de dépends pas des DNS du FAI

Inconvénient : cela génère un fort traffic

priétés de SER¥EUR2		? >
Interfaces	Redirecteurs	Avancé
Indications de racine	Enregistrement Ana	alyse Sécurité
Les indications de racine sur le réseau.	sont utilisées pour trouver d'a	utres serveurs DNS
Nom de serveur	Adresse IP	
m.root-servers.net.	[202.12.27.33]	
l.root-servers.net.	[198.32.64.12]	
k.root-servers.net.	[193.0.14.129]	
j.root-servers.net.	[198.41.0.10]	
i.root-servers.net.	[192.36.148.17]	
h.root-servers.net.	[128.63.2.53]	
g.root-servers.net.	[192.112.36.4]	
f.root-servers.net.	[192.5.5.241]	
e.root-servers.net.	[192.203.230.10]	
d.root-servers.net.	[128.8.10.90]	
c.root-servers.net.	[192.33.4.12]	
b.root-servers.net.	[128.9.0.107]	

Utilisation des redirecteurs

A partir du moment ou la zone racine n'existe plus , les redirecteurs sont utilisables	Propriétés de SERVEUR2 ? × Indications de racine Enregistrement Analyse Sécurité Interfaces Redirecteurs Avancé
	Les redirecteurs aident à résoudre les requêtes DNS auxquelles ce serveur n'a pas répondu.
	Activer les redirecteurs
II faut indiquer ceux du FAI	Pour ajouter un redirecteur, entrez son adresse IP, puis cliquez sur Ajouter. Adresse IP :
	Ajouter
	Supprimer
	Monter
	Descendre
	Délai d'expiration de redirection (secondes) : 5
	Ne pas utiliser la récursivité

N.B: Attention, pour éviter les prises de lignes intempestives par le DNS, il est préférable utiliser les redirecteurs pointant vers les DNS du FAI, supprimer les indications de racine et lire l'article F246804 de la Base de connaissance pour limiter les connexions du serveur DNS dynamique de windows !

Indication de la passerelle à utiliser

Bien sûr les clients indiques comme serveur DNS le serveur 2000 et pas celui du FAI...

Bien sûr, que ce soit sur le serveur DNS ou les clients, il ne faut pas oublier d'indiquer en paramètres TCP/IP l'adresse du routeur que l'on prendra pour sortir physiquement....



MISE EN ŒUVRE DHCP

Installation d'un serveur DHCP :

Installons sur le serveur 2000 un serveur DHCP distribuant des adresses comprises entre 192.168.1.60 et 192.168.1.70

Dans un premier temps, par de paramètres options de serveur...

LO DHCP			_ 8 ×
Action Affichage ← → È 🔃 🗗 🔀 😫 →	÷		
Arbre	Pool d'adresses		
DHCP	Adresse IP de début	Adresse IP de fin	Description
Serveur2.domaine2.edu [192.168.1.22] Étendue [192.168.1.0] test Fool d'adresses G Baux d'adresse G Réservations G Options d'étendue Options de serveur	J=192.168.1.60	192.168.1.70	Plage d'adresses pour la distribution

activons l'étendue, puis le serveur DHCP

Vérifions si sur le client on récupère bien une adresse IP dynamiquement...

F	Propriétés de Protocole Internet (TCP/IP) ? X
	Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.
	Obtenir une adresse IP automatiquement
	C Utiliser l'adresse IP suivante :
	Adresse IP :
	Masque de sous-réseau :

Et on obtient Adresse IP et Serveur DHCP...ainsi que le Bail

	Suffixe DNS spéc. à la connexion. : domaine2.edu
	Description
	Adresse physique
	DHCP activé Oui
	Autoconfiguration activée : Oui
▶	Adresse IP
	Masque de sous-réseau : 255.255.255.0
	Passerelle par défaut :
	Serveur DHCP
	Serveurs DNS : 192.168.1.22
	Bail obtenu : mardi 4 juin 2002 00:57:43
	P_{2} P_{2} = P_{2} P_{2} P_{2} = P_{2} P_{2} P_{2} = P_{2} P_{2} P_{2} = P_{2} P_{2} = P_{2} P_{2} P_{2} = P_{2} P_{2} =

Pour libérer une adresse on peut faire IPCONFIG / RELEASE... voire /RENEW



Sécuriser un serveur DHCP :

Je souhaite que n'importe qu'elle machine ne puisse plus récupérer une adresse ip au hasard. Par conséquent on va mettre en place une réservation d'adresse basée sur les adresses mac des clients que je pense avoir a terme.

Pour connaître l'adresse mac d'une machine, si je peux l'atteindre par un ping, la commande en ligne

arp –a

me donnera son adresse mac

Il ne me reste plus qu'a créer des reservation avec ces adresses.

Augmenter les sauvegardes automatique serveur DHCP :

Modifier la clé de la base de registre afin que les sauvegardes s'effectuent de manière automatique toutes les 20 minutes (14 en hexa) au lieu de toutes les heures comme cela est prévu par défaut.





MISE EN ŒUVRE DDNS

Paramétrage d'un serveur DHCP :

Il faut rajouter dans les options de serveur, l'adresse du serveur DHCP que l'on souhaite fournir aux clients DHCP...

Options Serveur	? ×
Général Avancé	
Options disponibles OD5 Serveurs de noms OD6 Serveurs DNS OD7 Serveurs de connexion O08 Serveurs de cookies	Descriptio ▲ Tableau c Tableau c Tableau c Tableau c
	•
Entrée de données Nom du serveur :	
serveur2	Résoudre
Adresse IP : 192 . 168 . 1 . 22 Ajouter	

De manière à avoir

$ \underline{A}_{ction} Affichage $					
Arbre Options de serveur					
DHCP	Nom d'option	Fabricant	Valeur		
🚊 🗟 serveur2.domaine2.edu [192.168.1.22]	😡 006 Serveurs DNS	Standard	192.168.1.22		
Étendue [192.168.1.0] test	🕼 015 Nom de domaine DNS Standard		domaine2.edu		
Pool d'adresses					
🚾 Baux d'adresse					
- 💼 Réservations					
Options d'étendue					
Options de serveur					

Puis il faut vérifier que les propriétés de ce serveur DHCP soient

	Фрнср	
	<u>A</u> ction Affichage ⇐ → ि 🖬	
	Arbre	Options de serveur
Pour des — clients 2000 —	DHCP Serveur2.domaine2.edu [192.168.1.22] Etendue [192.168.1.0] test Pool d'adresses Baux d'adresse Réservations Options d'étendue Options de serveur	Propriétés de serveur2.domaine2.edu [192.168.1.22] ? × Général DNS Avancé Vous pouvez paramétrer le serveur DHCP pour mettre à jour automatiquement les informations de nom et d'adresse sur les serveurs DNS qui prennent en charge les mises à jour dynamiques. ✓ Mettre à jour automatiquement les informations de client DHCP dans DNS ✓ Mettre à jour DNS uniquement si un client DHCP le demande ✓ Toujours mettre à jour DNS ✓ Ignorer les résultats de recherche directe (noms/adresses) lorsque le bail expire Activer les mises à jour pour les clients DNS qui ne prennent pas en charge la mise à jour dynamique Les mises à jour sont envoyées aux serveurs DNS qui sont configurés dans les propriétés TCP/IP pour les connexions actives sur ce serveur.



Paramétrage d'un client 2000 :

Dans les propriétés avancées de TCP/IP, vérifier que l'on a
Paramètres TCP/IP avancés
Paramètres IP DNS WINS Options
Adresses des serveurs DNS, dans l'ordre d'utilisation :
Î
Ð
Ajouter Modifier Supprimer
Les trois paramètres suivants sont appliqués à toutes les connexions pour lesquelles TCP/IP est activé. Pour la résolution des noms non qualifiés :
Ajouter des suffixes DNS principaux et spécifiques aux connexions
Ajouter des suffixes parents du suffixe DNS principal Ajouter des suffixes DNS (dans l'ordre) :
Ţ.
Ajouter Modifier Supprimer
Suffixe DNS pour cette connexion :
 Enregistrer les adresses de cette connexion dans le système DNS Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS

Ce qui fait que lorsque sur ce client on fait IPCONFIG /RELEASE on a

hernet carte Connexion au réseau local :	
Suffixe DNS spéc. à la connexion. Description	3Com EtherLink III ISA (3C509b-TPO) 00-20-AF-C5-21-51 Oui Oui 0.0.0 0.0.0 0.0.0 255.255.255.255

avec un IPCONFIG /RENEW on obtient

hernet carte Connexion au réseau local :	
Suffixe DNS spéc. à la connexion. Description Adresse physique DHCP activé Autoconfiguration activée Adresse IP. Masque de sous-réseau Passerelle par défaut Serveur DHCP. Serveurs DNS Bail obtenu Bail expire	<pre>: domaine2.edu : 3Com EtherLink III ISA (3C509b-TPO) : 00-20-AF-C5-21-51 : Oui : Oui : 192.168.1.60 : 255.255.255.0 : : 192.168.1.22 : 192.168.1.22 : mardi 4 juin 2002 01:31:47 : mercredi 12 juin 2002 01:31:47</pre>

et surtout l'enregistrement correspondant et crée dans le DNS...





Paramétrage d'un client non 2000 :

Peu de modification, a dire vrai, vérifier que les propriétés de ce serveur DHCP soient

	Фрнср			
	Action Affichage ↓ ← → 1 €	× 6 0 6 6 1 里 9		
	Arbre	serveur2.domaine2.edu [192.168.1.22]		
	DHCP	Contenu du serveur DHCP État		
	🖻 🖓 serveur2.domaine2.edu [192.168.1.22]	Étendue [192.168.1.0] test ** Actif **		
	Etendue [192.168.1.0] test	priétés de serveur2.domaine2.edu [192.168.1.22]		
	Baux d'adresse	iénéral DNS Avancé		
	Options de serveur	Vous pouvez paramétrer le serveur DHCP pour mettre à jour automatiquement les informations de nom et d'adresse sur les serveurs DNS qui prennent en charge les mises à jour dynamiques.		
		Mettre à jour automatiquement les informations de client DHCP dans DNS		
		C Mettre à jour DNS uniquement si un client DHCP le demande		
		Toujours mettre à jour DNS		
Pour des clients autres que 2000 —		Ignorer les résultats de recherche directe (noms/adresses) lorsque le bail expire		
		Activer les mises à jour pour les clients DNS qui ne prennent pas en charge la mise à jour dynamique		
		Les mises à jour sont envoyées aux serveurs DNS qui sont configurés dans les propriétés TCP/IP pour les connexions actives sur ce serveur.		

et sur un client windows 98 on obtient par exemple

P Configuration IP	_ 🗆 >
🗖 Informations sur l'hôte	
Nom de l'hôte	poste8.domaine2.edu
Serveurs DNS	192.168.1.22
Type de noeud	Diffuser
Identificateur d'étendue NetBIOS	
Routage IP activé	WINS Proxy activé
La résolution NetBIOS utilise DNS	
Carte Ethernet Informations	
E	LNK3 Ethernet Adapter 📃
Adresse de la carte	00-20-AF-C5-21-51
Adresse IP	192.168.1.60
Masque de sous-réseau	255.255.255.0
Passerelle par défaut	
Serveur DHCP	192.168.1.22
Serveur WINS principal	
Serveur WINS secondaire	
Bail obtenu	04 06 02 01:44:45
Expiration du bail	12 06 02 01:44:45
OK Libérer Renouvele	r Tout li <u>b</u> érer Tout <u>r</u> enouveler

et surtout l'enregistrement correspondant et crée dans le DNS...



PUBLICATION RESTREINTE DANS AD

Objectif:

Dans un domaine, on souhaite faire que seuls les membre du groupe d'utilisateur "**maintenance**" puisse accéder à des ressources partagées avec le mot clé "**pilote**"...

On crée un groupe de sécurité global d'utilisateurs nommé **maintenance** à l'intérieur duquel on placera par exemple un utilisateur **bob**.



Groupe de sécurité - Global

On partage 2 dossiers, un sous l'appellation **dos-drivers**, l'autre sous l'appellation **dos-data**, en imaginant que le premier contienne des sources de drivers, et le deuxième des données....

N.B: ces dossiers peuvent se trouver physiquement n'importe où dans mon domaine...

词 dos-data 词 dos-drivers

Publication sélective dans A.D. :

Pour publier ces dossiers dans AD on se place dons dans la mmc Utilisateurs et ordinateurs Active Directory et on crée une UO nommée par exemple ressources contenant mes 2 dossiers partagés

Nouvel objet - Dossier partagé	Nouvel objet - Dossier partagé
Créer dans : dom1.com/ressources	Créer dans : dom1.com/ressources
Nom :	Nom :
drivers	datas
Chemin réseau (\\serveur\partage): \\s1\dos-drivers	Chemin réseau (\\serveur\partage) : \\s1\dos2-datas
donc on obtient	
Arbre	ressources 2 objets
A Utilisateurs et ordinateurs ústive Directory [s1.dom1.s	
in a dominante and a second and the second s	Orivers Dossier partagé
	datas Dossier partagé
🗄 🥘 Domain Controllers	



et on ajoute au dossier partagé drivers le mot clé "pilote"...





庄 🕋 🛄 Users

🐼 ressources

🗄 🧰 ForeignSecurityPrincipals

Windows NT 2000 travaux pratiques

Pour modifier les permissions de sécurité des objets publiés, il est nécessaire de demander Affichage / fonctionnalités avancées

Arbre		re	ssources	2 objets
a Utilisateurs et ordina	ateurs Active Directory [s1.dom1.com]	N	om	Туре
🔄 🗊 dom1.com		Ş	drivers	Dossier partagé
🗄 🛄 Builtin		⊊	datas	Dossier partagé
🗄 🛅 Computers		1		
🗄 🙆 Domain Con	trollers	L .		
🗄 💼 ForeignSecu	urityPrincipals	L .		
🛨 🛄 Users		L .		
ressources		Ε.,		
	Délégation de contrôle			
	Ajouter des membres à un groupe			
	Déplacer			
	Rechercher			
	Nouveau	•		
	Toutes les tâches			
		_		
	Affichage		Choisir	des colonnes
	Nouvelle fenêtre à partir d'ici	-	Grande	s icônes
	Supprimer		Petites	icônes
	Benommer		Licto	leonos
	Actualiser		 Détaile 	
	Exporter la liste		- Dotails	
	Exporter la listeria	_	🗸 Utilisate	eurs, groupes et ordi
	Propriétés		Fonctio	nnalités avancé <u>es</u>

A partir de là on accède à l'onglet Sécurité



On y ajoute le groupe **maintenance**...

Et on supprime le groupe **Utilisateurs authentifiés**...

Recherche de dossiers partagés :

• Si un utilisateur simple (non membre du groupe maintenance) fait une recherche dans AD de tous les dossiers partagés avec le mot clé pilote...

Rechercher Dossier: Fichier Edition Affichag	s partagés je ?			
Rechercher : Dossiers p Dossiers partagés Ava Nommé : Mots-clés : pilote	artagés 💽 Dans : 🗊 d ancé	om1 💌	Parcourir Rechercher Arrêter Effacer tout	
Nom	Nom de partage mots-clés Aucun élément ne correspond à la rech	erche actuelle	Image: A = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 =	La recherche n'aboutit pas
Microsoft WindowsNT	Windows NT 2000 travaux pratiques	Cabaré M C.U.E.F.A.	1ichel S4 T.P. v1.4	Page 28

Si ce même utilisateur simple (non membre du groupe maintenance) fait ٠ une recherche dans AD de tous les dossiers partagés ...

Rechercher Dossi Fichier Edition Affici	iers partagés hage ?			_ 🗆 ×	
Rechercher : Dossier	s partagés	Dans: 🗊 dom1	•	Parcourir	
Dossiers partagés 🗼	Avancé				
Nommé :				Auctor	
Mots-clés :				Arreter	
				Erracer tout	
				- X	Caul la alassian
				, i i i i i i i i i i i i i i i i i i i	Seul le dossier
					recherche
Nom	Nom de partage	mots-clés			n'aboutit pas
₽datas	\\s1\dos2-datas	•			naccom pas
		•			
1 élément(s) trouvé(s)				li	

• Si bob, (membre du groupe maintenance) fait une recherche dans AD de tous les dossiers partagés avec le mot clé pilote...

🍕 Rechercher Doss	iers partagés		
Fichier Edition Affic	hage ?		
Rechercher : Dossie	rs partagés	💌 Dans : 🗊 dom1	▼ Parcourir
Dossiers partagés	Avancé		
Nommé :			Hechercher
Moto clác y 🖉	lata		Arrêter
Mots-cles ; [p	loce		Effacer tout
Nom	Nom de partage	mots-clés	
I⊊drivers	\\s1\dos-drivers	pilote	

Si bob, (membre du groupe maintenance) fait une recherche dans AD de • tous les dossiers partagés ...

🐗 Rechercher Dossi	ers partagés			
Fichier Edition Affich	iage ?			
Rechercher : Dossiers	: partagés	Dans: 🗊 dom1	• P	arcourir
Dossiers partagés 🛛	Wancé		- 10	Rechercher
Mots-clés :				Arrêter Effacer tout
				Ś
Nom	Nom de partage	mots-clés		
🕎 datas	\\s1\dos2-datas			
₽ drivers	\\s1\dos-drivers	pilote		
2 élément(s) trouvé(s)				//.



DELEGATION COMPETENCE SUR UO

Objectif:

Dans un domaine, on souhaite faire que le service « formation », soit autonome quant à la gestion de ses utilisateurs, postes etc

L'idée est de créer une OU sur laquelle on effectuera une délégation de compétence pour un compte particulier, nommé **adform**...

Mise en place délégation :

On va créer une UO formation, contenant un utilisateur adform,

puis on va pour cette UO faire une délégation de compétence complète à





Windows NT 2000 travaux pratiques

En controle total	Assistant Délégation de contrôle	×
	Autorisations Sélectionnez les autorisations que vous voulez déléguer.	(F)
	Afficher ces autorisations :	
	🔽 Générales	
	✓ Spécifique aux propriétés	
	Création/suppression d'objets enfants spécifiques	
	Autorisations :	
	Contrôle total	_
	Créer tous les objets enfants	
	Supprimer tous les objets enfants	
	🗹 Lire toutes les propriétés	-
Ce que nou confirme l'assistant	S	

Assistant Délégation de conti	rôle
J.	Fin de l'Assistant Délégation de contrôle L'Assistant Délégation de contrôle est terminé.
dans le dossier Active Directory suivant : domaine1.edu/formation Les groupes, utilisateurs ou ordinateurs auxquels vous avez délégué le contrôle sont : adform (adform@domaine1.edu) Ils ont les autorisations suivantes : Contrôle total	

Utilisation de la délégation :

Pour voir si cela fonctionne, il faut essayer d'administrer cette OU en tant qu'utilisateur adform.

Mais cet utilisateur n'est qu'un utilisateur classique au niveau des groupes de domaine, donc il ne peut pas ouvrir de session sur le CD. On peut soit modifier les stratégies de Contrôleur de Domaine pour lui permettre d'ouvrir une session locale sur le serveur (déconseillé) soit lui installer les outils d'administrations à distance sur son poste (mieux).

N.B: le fichier permettant l'installation des outils d'Administration, est stocké dans le CD de distribution 2000 serveur, dans i386... (fichier Adminpak.msi)

Depuis un client, et connecté en tant que adform, on lance la console Utilisateurs et ordinateurs Active Directory, on n'a d'action possible que sur I'UO formation ...



Ajoutons deux stagiaires stg1 et stg2 , formation, cela est possible sans problème	(sans mot de passe) dans l'UO es
Et un compte ordinateur clientform placé	dans notre UO formation
Rattachons un nouveau poste nomme membre d'un workgroup) au domaine	é clientform (donc actuellement Modifications de l'identification
Il suffit après une ouverture de session locale en tant qu'administrateur du poste, de demander un rattachement domaine	Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Les modifications peuvent affecter l'accès aux ressources réseau. Nom de l'ordinateur : clientform Nom complet de l'ordinateur : clientform.domaine1.edu
en donnant comme identificateur le compte que l'on à crée comme administrateur de notre UO, c'est à dire adform	Autres Membre de O Domaine : domaine1.edu Groupe de travail : WORKGROUP
domaine.	
Nom : adtorm	
Mot de passe :	
OK Annuler	

N.B: Si l'utilisateur **adform**, ne crée pas un compte ordinateur au préalable dans son UO formation, il pourra rattacher la station au domaine (a condition bine sur que l'enregistrement hôte ait été crée dans le dns...), et le compte ordinateur (crée au préalable dans le dns) ira se ranger dans le conteneur d'AD prévu par défaut à cet effet, c'est à dire **computers**...

Mais là, toute tentative de gestion de ce compte machine par notre **adform** se soldera par un échec, car ses droits sont limités a son UO **formation** !



Ajouter une délégation :

On réutilise l'assistant de délégation



Modifier-Supprimer une délégation :

Il faut accéder aux propriétés de l'objet AD sur lequel la délégation à été faite. Seul le propriétaire de l'objet peut le faire.





voire Afficher/Modifier

Entrée d'autorisation pour formation		? ×
Objet Propriétés		
Nom : adform (adform@domaine1.edu)		Modifier
Appliquer à : cet objet et tous les objets en	fant	•
Autorisations :	Autorise	r Refuser
Contrôle total Lister le contenu Lire toutes les propriétés Écrire toutes les propriétés Supprimer Supprimer la sous-arborescence Autorisations de lecture Modifier les autorisations Modifier le propriétaire Toutes les écritures validées Tous les droits étendus Créer tous les objets enfants Créer tous les objets enfants Appliquer ces autorisations uniquement de ce conteneur		
	ОК	Annuler



Windows NT 2000 travaux pratiques

COMMANDE NET SEND...

La base de la commande Net send :

Cette commande utilise des **noms netbios**... (le 16° caractère spécifie la nature du nom 03h affichage des messages...)

Que se passe-t-il si l'administrateur à ouvert une session sur le serveur est sur un client ? à qui sera envoyé le net send ?

°⊡ WINS				_
Action Affichage ⇐ → ि 💽 😧				
Arbre	Inscriptions actives Élé	ments trouvés pour le propriétaire	: 169.254.64.189: 2	2
WINS	Nom d'enregistrement	Туре	Adresse IP	État
État du serveur	BMSBROWSE	[01h] Autre	192.168.1.100	Actif
🗄 🖷 🚮 serveur1.domaine1.edu [169.254.64.189]	B ADMINISTRATEUR	[03h] Affichage des messages	169.254.64.189	Actif
Inscriptions actives	📕 CABARÉ	[03h] Affichage des messages	192.168.1.3	Libéré
Partenaires de réplication	CLIENT1	[00h] Station de travail	192.168.1.3	Libéré
	CLIENT1	[03h] Affichage des messages	192.168.1.3	Libéré
	CLIENT1	[20h] Serveur de fichiers	192.168.1.3	Libéré
	CLIENT1R1	[00h] Station de travail	192.168.1.2	Actif
	CLIENT1R1	[03h] Affichage des messages	192.168.1.2	Actif
	CLIENT1R1	[20h] Serveur de fichiers	192.168.1.2	Actif
	DOMAINE1	[00h] Groupe de travail	192.168.1.2	Actif
	DOMAINE1	[1Bh] Explorateur principal de	192.168.1.100	Actif
	DOMAINE1	[1Ch] Contrôleur de domaine	192.168.1.100	Actif
	DOMAINE1	[1Eh] Nom de groupe ordinaire	192.168.1.2	Actif
	🖲 INet~Services	[1Ch] Contrôleur de domaine	169.254.64.189	Actif
	圖IS~SERVEUR1	[00h] Station de travail	169.254.64.189	Actif
	MARIE	[03h] Affichage des messages	192.168.1.2	Actif
	SERVEUR1	[00h] Station de travail	192.168.1.100	Actif
	SERVEUR1	[01h] Autre	169.254.64.189	Actif
	SERVEUR1	[03h] Affichage des messages	192.168.1.100	Actif
	SERVEUR1	[20h] Serveur de fichiers	192.168.1.100	Actif
	🖲 TEST	[00h] Groupe de travail	192.168.1.3	Libéré
	🕮 TEST	[1Eh] Nom de groupe ordinaire	192.168.1.3	Libéré

Pour envoyer le message "Réunion reportée à 15:00 au même endroit " à l'utilisateur marie, tapez :

net send marie " Réunion reportée à 15:00 au même endroit. "

Pour envoyer un message à tous les utilisateurs connectés actuellement au serveur, tapez :

net send /users Ce serveur va s'arrêter dans 5 minutes.





COMMANDE NET USER...

La base de la commande Net user :

Ce qui est intéressant, c'est de pouvoir en ligne de commande, ajouter un utilisateur. Avec les paramètres de base :

ajouter un compte d'utilisateur pour Michel et l'autorisez le à se avec le mot de passe obligatoire (mc):

C:\>net user michel mc /add La commande s'est terminée correctement

Les paramètres optionnels :

/fullname:"nom"

Spécifie le nom complet de l'utilisateur plutôt qu'un nom d'utilisateur. Placez le nom entre guillemets.

/passwordchg:{yes | no}

Indique si les utilisateurs peuvent modifier leur propre mot de passe. La valeur par défaut est yes.

/passwordreq:{yes | no}

Indique si un compte d'utilisateur doit posséder un mot de passe. La valeur par défaut est yes.

/times:{heures | all}

Précise quand l'utilisateur est autorisé à employer l'ordinateur. Le paramètre heures est exprimé en jour[-jour][,jour[-jour]] ,heure[heure][,heure[-heure]] et limité à des incréments d'une heure. Les jours peuvent être écrits en toutes lettres ou abrégés sous la forme lun, mar, mer, jeu, ven, sam et dim. Les heures peuvent être exprimées à l'aide de la plage 12 ou 24 heures. Pour la plage 12 heures, utilisez AM, PM ou A.M., P.M. La valeur all signifie qu'un utilisateur peut toujours se connecter. La valeur nulle (blanc) signifie qu'un utilisateur ne peut jamais se connecter. Séparez le jour et l'heure par des virgules et les unités du jour et de l'heure par des points-virgules (par exemple, L,4AM-5PM;Ma,1PM-3PM). N'utilisez pas d'espaces pour désigner les heures

/workstations:{nom_ordinateur[,...] | *}

Répertorie jusqu'à huit stations de travail à partir desquelles un utilisateur peut se connecter au réseau. Séparez les entrées multiples de la liste par des virgules. Si /workstations ne possède pas de liste ou si elle correspond à *, cela signifie que l'utilisateur peut se connecter à partir de n'importe quel ordinateur.



supprimez ce compte, puis ajouter un compte d'utilisateur pour Michel
 Cabare et l'autorisez le à se avec le mot de passe obligatoire (mc):

net user michel mc /add /fullname:"michel cabare"

 supprimez ce compte et ajouter un compte d'utilisateur pour Michel Cabare autorisé à se connecter lundi de 04:00 à 17:00 (pas d'espace dans la désignation des heures) avec le mot de passe obligatoire (mc):

Les 2 syntaxes équivalentes —	C:\>net user michel mc /add /times:L,4AM-5PM La commande s'est terminée correctement. C:\>net user michel mc /add /times:L,4-17 La commande s'est terminée correctement.					
	donnent					
	Horaire d'accès pour michel	x				
	Image: Connexion autorisée mardi mercredi	9				

 supprimez ce compte et ajouter un compte d'utilisateur pour Michel Cabare autorisé à se connecter du lundi au vendredi de 08:00 à 17:00 (pas d'espace dans la désignation des heures) avec le mot de passe obligatoire (mc):

C:\>net user michel mc /add /times:L,8-17;MA,8-17;ME,8-17;J,8-17;V,8-17 La commande s'est terminée correctement.

NB : notez dans cette syntaxe la différence MA mardi et ME mercredi !

 supprimez ce compte et ajouter un compte d'utilisateur pour Michel Cabare autorisé à se connecter du lundi au vendredi de 08:00 à 17:00 (pas d'espace dans la désignation des heures) avec le mot de passe obligatoire (mc) depuis le poste client1:

C:\>net user tions:poste1 La commande :	michel mc /add /times:L,8 s'est terminée correctemen	-17;MA,8-17; t.	ME,8-17;J,8-17;V,8-17	/worksta
Stati	ions de travail accessibles	<u>? </u> ×	(
Cet	te fonctionnalité nécessite le protocole NetBIOS. Da rez le nom de l'ordinateur avant l'installation de Wind	ns Nom de l'ordinateur, ows 2000.		
Cet	utilisateur peut ouvrir une session sur :			
0	Tous les ordinateurs			
	Les ordinateurs suivants			
۹]]	Nom de l'ordinateur : poste1	Ajouter Modifier		




SCRIPT SELON L'OS

Détecter l'OS du client :

Il est fréquent que certaine commandes ne soient pas traitées comprises de la même manière selon l'OS du client....ainsi, pour la création du lecteur logique, on sait que une lettre peut être attachée automatiquement au répertoire de base, mais on sait aussi que on peut via un script donner l'instruction suivante **net use g : /home**

Le problème dans ce cas c'est que ce script fait « double emplois » lors d'une exécution sur un client 2000.

On voudrait faire exécuter différent selon la nature du client :

- Si le client est windows95-98, il faut créer un lecteur sur le dossier de base
- Si le client est 2000, il n'est pas nécessaire de créer ce lecteur logique, car il est crée automatiquement

Variable d'environnement :

Il existe une variable d'environnement nommée %OS%

Dans le panneau de configuration / système on trouve

	¥aria	bles d'environne	ement	? ×
s d'environnement Les variables d'environnement indiquent à votre ordinateur où trouver certains types d'informations. Variables d'environnement		ariables utilisateur p Variable TEMP TMP	our Administrateur Valeur E:\Documents and Settings\Administrat E:\Documents and Settings\Administrat	
dans lequel on voit que		ariables système —	Nouveau Modifier Supprime	er
	E	Variable	Valeur	
		NUMBER_OF_PR	1 Windows NT	
		Os2LibPath Path	E:\WINNT\system32\os2\dll; E:\WINNT\system32:E:\WINNT:E:\WIN	-
			Nouveau Modifier Supprime	er

Donc on peut dire que si on a "%OS%"=="Windows_NT" on est sur un client 2000 (ou NT4.0)

Soit donc un script avec les étiquettes SUITE-FIN suivantes :



Windows NT 2000 travaux pratiques

If not "%OS%"=="Windows_NT" goto SUITE REM partie qui va etre executée sur un client 2000

goto FIN:

REM partie qui va etre executée sur un client non 2000 :SUITE

:FIN

exercice : faire un script qui ne crée de lecteur réseau sur le répertoire de base que si le client n'est pas un client nt ou un client 2000....

Version d'OS :

cette variable d'environnement nommée **%OS%** est la même pour 2000 et pour NT4, ce qui fait que si l'on voulait descendre au niveau de la détection de la version de Windows il faudrait employer une commande **VER** qu'il faudrait rediriger ensuite avec une commande **FIND** de recherche de caractère...

en effet ver renvois les valeurs suivantes selon les versions de système

pour Windows NT 4.0 (wks ou srv)



pour Windows 2000 (pro ou server)



On peut donc rechercher la chaîne "4.0" pour savoir si on est sur un poste NT4.0 ou un poste 2000. Pour rediriger la sortie de la commande **ver** sur la commande **FIND** on utilise un **| (pipe)**, ce qui donnerait à peu près la ligne suivante

Ver | find "4.0" | goto nt4

exercice : faire un script qui détecte si le client sur lequel il s'exécute est un client windows95-98, nt4.0 ou 2000





🔊 detecteos.bat - Bloc-notes

Fichier Edition Format ? if not "%OS%"=="Windows_NT" goto suite @echo le client est nt ver | find "4.0" | goto nt4 @echo le client est nt2000 goto fin :nt4 @echo le client est nt4.0| goto fin :suite @echo le client est autre que nt ver :fin pause





SCRIPT GROUPE UTILISATEURS

Tester l'appartenance à un groupe précis :

Il est aussi fréquent que certaine commandes ne soient pas applicable à tous les utilisateurs, mais qu'elles aient un sens uniquement si l'utilisateur est membre de tel ou tel groupe...

Imaginons un fichiers **.bat** spécifique à des commerciaux, nommé **commercial.bat**, et un fichier **.bat** spécifique à des secrétaires, nommé **secretaire.bat**

Ces deux fichiers sont appelables dans mon script via la commande **call** mais comment détecter l'appartenance d'un utilisateur à tel groupe ?

Cela n'est possible que si le client est un client NT...

Solution native :

On sait que **net user toto /domain** renvois alors les paramètres de cet utilisateur.

Un script permettant d'avoir les informations concernant l'utilisateur en train d'ouvrir la session ressemblerait donc à ceci :



soit l'utilisateur toto membre d'un groupe secretaire,

et titi membre d'un groupe commercial



alors ce script sur l'ouverture de titi amène l'info suivante :



La demande sera traitée sur contrôleur de domaine du domaine domaine2.edu. Nom d'utilisateur Nom complet titi titi Commentaire Commentaires utilisateur Code du pays 000 (Valeur par défaut du système Compte : actif 0ui Le compte expire Jamais Mot de passe : dernier changmt. Le mot de passe expire Le mot de passe modifiable Mot de passe exigé L'utilisateur peut changer de mot de passe 5/14/2002 12:49 6/26/2002 11:37 5/14/2002 12:49 AM PM Oui Oui Stations autorisées Script d'ouverture de session Profil d'utilisateur Répertoire de base Tout selongroupe \\serveur2\ressource\titi
5/14/2002 1:18 PM Dernier accès Tout Heures d'accès autorisé Appartient aux groupes locaux Appartient aux groupes globaux ¥Utilisateurs ¥Utilisa. du domaine ×commercial La commande s'est terminée correctement.

Pour détecter l'appartenance à un groupe, il suffit maintenant d'utiliser **FIND** en récupération de la sortie du script précédant...

Et bien sur prévoir les 2 fichiers bat à exécuter...

@if not "%OS%"=="Windows_NT" goto suite @echo le client est nt ©net user %username% /domain | find /i "*commercial" && call commercial.bat ©net user %username% /domain | find /i "*secretaire" && call secretaire.bat goto fin :suite @echo le client est autre que nt :fin

Avec le resource kit

Avec l'utilitaire nommé **ifmember.exe** qu'il faut installer sur tous les clients en \WINNT\SYSTEM32 (ou un chemin disponible dans les variables d'environnement système)

🛃 selonifmember.bat - Bloc-notes				
Fichier Edition Format ?				
@if not "%OS%"=="Windows_NT" goto suite				
©echo le client est nt ifmember "commercial" if errorlevel 1 call commercial.bat ifmember "secretaire" if errorlevel 1 call secretaire.bat				
goto fin				
suite ©echo le client est autre que nt				



crosoft

SCRIPT WSH

🗄 🛅 domain

🗄 💭 sysvol

🖻 🛄 domaine2.edu - DO_NOT_REM

🖻 😱 scripts 🔄 vbs

Mise en place des scripts :

On veut utiliser des scripts que l'on placera dans un 🚊 💼 sysvol dossier spécifique du serveur nommé par exemple vbs...de manière à ne pas les mélanger avec ceux existant.

il faudra du coup indiquer dans le profil utilisateur cette redirection

CHOM	
Profil utilisateur	
Chemin du profil :	
Script d'ouverture de session :	vbs\premier

1° script en vbs :

La commande la plus simple que l'on puisse faire, comme d'habitude, c'est faire afficher un message.

En vbs la commande est la suivante :

Wscript.Echo "test script en vbs avec WSH"

On peut donc mettre cette ligne dans un fichier xxxx.vbs, par exemple premier.vbs

💐 prer	mier.vbs	- Ble	oc-n	ote	5				_ [IJ×
Fichier	Edition	For	mat	?						
Wscri	pt.Ecł	10 '	'tes	st	script	en	vbs	avec	WSH"	

Bon, notre premier fichier en vbs à destination de WSH est prêt, mais comment l'exécuter sur le client ?

Le problème c'est que cette commande doit être exécutée via l'environnement 'en ligne de commande» de WSH, et non pas l'environnement graphique.

Comme on ne peut pas savoir si sur le client par défaut WSH est positionné en ligne de commande, ou en interface GUI, on faut lancer la commande avec des paramètres d'appel, du genre

cscript //i //nologo %0\\..\\premier.vbs



l'utilisation des paramètres **//i** et de **//nologo** est simple, ces paramètres expriment en wsh le mode interactif, sans logo de démarrage, et sont possibles par l'appel de **cscript**....

Plus délicat la signification de %0\\..\\premier.vbs

En effet le script que l'on écrit doit aller chercher le fichier **premier.vbs** à son emplacement d'origine, hors le client ne le connaît pas ! **%0** contient toujours le chemin complet vers le script en cours, de la on peut utiliser et écrire le chemin permettant de trouver **premier.vbs**

Par conséquent un script **premier**.bat et contenant

🖾 premier.bat - Bloc-notes				
Fichier Edition Format ?				
echo off echo %%0=%0 cscript //i //nologo pause	%0\\premier.vbs			

devrait donner à l'exécution sur un client « comprenant wsh » le résultat suivant :

\\SERVEUR2\NETLOGON\vbs\premier.bat	
C:\>echo off x0=\\SERVEUR2\NETLOGON\vbs\premier.bat test script en vbs avec WSH Appuyez sur une touche pour continuer	

Si on voulait vraiment, on pourrait affiner le test de la présence de WSH en testant la présence des fichiers système, par un script **second.bat** du genre :

🖉 second.bat - Bloc-notes
Fichier Edition Format ?
 echo off rem ceci pour WSH if exist %windir%\command\cscript.exe goto :WSHPRESENT if exist %windir%\system\cscript.exe goto :WSHPRESENT if exist %windir%\system32\cscript.exe goto :WSHPRESENT goto :WSHABSENT
Echo WSH present tout va bien cscript //i //nologo %0\\premier.vbs goto :EXIT :WSHABSENT Echo WSH manquant ERREUR :EXIT

appelant mon script **premier.vbs**...

En effet la présence de l'installation de WSH sur un OS est donnée ci-dessous

Composant	Fichier clé	Emplacements
Windows Script Host	CSCRIPT.EXE	%windir%\command %windir%\system %windir%\system32
VBScript	VBSCRIPT.DLL	%windir%\system %windir%\system32
ADSI	ADSNT.DLL	%windir%\system %windir%\system32



Un exemple en vbs :

Soit le fichier **exemple.bat** permettant de lancer le script **exemple.vbs** suivant :

Dim variable					
Wscript.Echo "exemple script en vbs avec WSH"					
Set variable = WScript.CreateObject("WScript.Network")					
Wscript.Echo "machine " & variable.ComputerName Wscript.Echo "utilisateur " & variable.UserName Wscript.Echo "domaine " & variable.UserDomain					
variable.MapNetworkDrive "S:", <u>\\serveur2\ressource</u>	Bien sur il vaut mieux que ce partage ait été crée				
Wscript.Echo "fin test script en vbs avec WSH"	préalablement à l'exécution du script !				





ID ÉVÈNEMENT

Signification d'un ID du gestionnaire évènement :

Un site répertorie et traite une bonne partie des évènements qui surviennent au quotidien. Il s'agit du site **www.eventid.net**

Sur la page d'accueil, on ait une recherche par ID

Ever	ntID.Net		
Home	Search Resources Documents Forums About Us		
com	nputer giving you a headache ?		
Enter the eve Enter event source (optio	nt ID: nal): Search		
Event ID: 54			
Source	w32time		
Туре	Warning		
Description	The Windows Time Service was not able to find a Domain Controller. A time and date update was not possible.		
Comments	 A.G.: "As per Microsoft: This issue can occur because of repeated network issues or if the Time service has been unable to find a domain controller to synchronize with for a long time. To reduce network traffic, the Time service will wait 960 minutes before it tries again, and no synchronization takes place during this interval, even if network connectivity is restored after being in a disconnected state for an amount of time that is less than the synchronization interval." A.G.: "Windows 2000 computers are attempting to synchronize their time with a domain controller. If none is found this message is generated. The domain controller must run the w32time service. This service can be syncronized with an external source (ie.atomic clocks like the one maintained by Navy Observatory). A syncronized time is very import for Active Directory implemenations due to its distributed nature." 		
Links	Q312534; Windows 2000 Time		

CUETa CUETa



ligne...

Event ID: 62	Event ID: 62				
Source	w32time				
Туре	Error				
Description	This Machine is a PDC of the domain at the root of the forest. Configure to sync from External time source using the net command, 'net time /setsntp:'.				
Comments	Adrian Grigorof: The Time service is not configured to use a reliable source for synchronization. Try "net time /setsntp:ntp2.usno.navy.mil" followed by "w32tm /s" (Internet connectivity should be available between the server and the ntp2.usno.navy.mil NTP - Network Time Protocol server)				
Contributors	Adrian Grigorof				

La commande pour qu'il y ait synchronisation serait

Net TIME /SetSNTP:nomserveur





MONITEUR SYSTEME : ALERTE SUR UNE IMPRIMANTE

Paramétrage Seuil d'alerte :

Soit une imprimante HP laserjet 6P définie sur une machine client2kp7. On tient à ce que l'on sache immédiatement lorsque une attente de plus de 2 document existe sur ce périphérique. On souhaite que cela soit consigné dans le journal des évènements application et qu'un message soit envoyé sur le poste de l'administrateur, situé en Serveur2...

Sur le client il faut d'abords définir l'imprimante...(pour les test on la mettra hors connexion **Utiliser l'imprimante hors connexion**)



On crée sur le poste ou se trouve l'imprimante une nouvelle alerte, nommé par exemple "attente imprimante"

🙀 Analyseur de performances					
∫∰ <u>C</u> onsole Fe <u>n</u> être <u>?</u>					
Action Affichage Eavoris	- → โตโต [8] [8] [1] → =				
Arbre Favoris	Nouveaux paramètres d'alerte				
🔲 Racine de la console	Nom :				
	attente imprimante				
🖃 🎆 Journaux et alertes de perform					
Journaux de compteur	OK Annuler				
Journaux de traçage					
Alertes					

et on la configure de la manière suivante :



pour obtenir

attente imprimante	×
Général Action Planification	
Cette alerte commence dès que vous appliquez les modifications.	
Commentaire :	
permet de détecter une file d'attente trop importante	
Compteurs :	
\\CLIENT2KP7\File d'impression(HP LaserJet 6P)\Travaux	
Alerte lorsque la valeur est : supérieure à 💌 Limite : 3	
Ajouter Supprimer	
Période d'échantillonnage des données :	
Intervalle : 30 🔹 Unités : secondes 🔽	
OK Annuler Appliquer	

Au niveau de l'action on demandera :



et une planification manuelle

attente imprimante
Général Action Planification
Démarrer l'analyse
 Manuellement (à l'aide du menu contextuel)
C Heure: 01:56:06
Arrêter l'analyse
 Manuellement (à l'aide du menu contextuel)
C Après : 1 👘 Unités : jours 💌
C Heure: 01:56:06 → date: 23/05/2002 ▼

Il ne reste plus qu'à la démarrer, via le menu contextuel.

🚡 Analyseur de performances			_ 🗆 ×
∫ 🗑 ⊆onsole Fe <u>n</u> être <u>?</u>			D 🖨 🔛 💷 💶 🗆
Action Affichage Eavoris	> → £ 🖬 Ø É	יום[8	
Arbre Favoris	Nom	Commentaire	
Racine de la console Moniteur système Journaux et alertes de perform Journaux de compteur Journaux de traçage Alertes	attente imprimante	permet de détecter (une file d'attente trop importante



Windows NT 2000 Cabaré Michel travaux pratiques

C.U.E.F.A. S4 T.P. v1.4

Déclenchement Seuil d'alerte :

Après avoir mis l'imprimante hors connexion, il suffit de demander une impression de quelques documents pour obtenir :

鑬 HP LaserJet 6P - Utiliser l'imprimante hors connexion					
Imprimante Document Affichage ?					
Nom du document	État	Propriétaire	Pages	Taille	Sour
Document		Administrat	1	6,01 Ko	02:09
Document		Administrat	1	6,01 Ko	02:09
Document		Administrat	1	6,01 Ko	02:10
Document		Administrat	1	6,01 Ko	02:1:
•					Þ
4 document(s) dans la file					

avec dans le	journal d'événe	ement basé	sur le poste

🚦 Observateur d'événements							_ & ×	
Action Affichage ↓ ← → 🗈 📧 😰 🔂 🛱								
Arbre	Arbre Journal applications 2 événement(s)							
🗊 Observateur d'événements (local)	Туре	Date	Heure	Source	Catégorie	Évén	Utilisateur	
Journal applications	Informations	22/05/2002	02:12:09	SysmonLog	Aucun	2031	N/A	
Journal sécurité	Informations	22/05/2002	02:11:39	SysmonLog	Aucun	2031	N/A	

avec le détail

Propriétés de Événement			? ×
Événement			
Date : 22/05/2002 Heure : 02:12 Type : Informations Utilisateur : N/A Ordinateur : CLIENT2KP7	Source : Catégorie : ID événement :	SysmonLog Aucun 2031	 ↑ ↓ ●
Description : Compteur : <u>\\CLIENT2KP7</u> dépassé son seuil d'alerte. I valeur limite de 3.	<u>\File</u> d'impressior La valeur du com	n(HP LaserJet 6P)\Travau npteur de 4 est Au-dessus	x a de la

et avec une notification sur le serveur

Service Affichage des messages
Message de CLIENT2KP7 à SERVEUR2 le 22/05/2002 02:10:59
2002-05-22 02:10:39 \\CLIENT2KP7\File d'impression(HP LaserJet 6P)\Travaux a dépassé son seuil d'alerte. 4 est Au-dessus de la valeur limite de 3.
ОК

N.B : bien penser a placer les alertes sur les machines sur lesquelles on veut visualiser les évènements.



MONITEUR SYSTEME DISQUE LOGIQUE

Compteur sur disque logique :

Par défaut, lorsque le système démarre, il active les compteurs d'analyse du disque par un pilote **Diskperf.sys**

Ce pilote par défaut active les compteurs uniquement sur les disques physiques, mais on peut par une ligne de commande, demander de l'activer aussi sur un lecteur logique...

Ainsi la commande

Diskperf.sys -YV permet de disposer d'un compteur de plus, permettant d'afficher la place disponible sur un lecteur logique

E:\>DISKPERF -YV

Les compteurs de performance des disques logique et physique de ce système sont maintenant initialisés pour être lancés lors du démarrage.





Windows NT 2000 travaux pratiques

Après redémarrage, on aura dans l'analyseur de performance, la possibilité de demander un disque logique...

Objet de performance :	
Disque logique	•
Disque logique	▲
Disque physique	
Distributed Transaction Coordinator	

Et sur les disques logiques, on demande la taille disponible...

Alerte saturation de disque :

Un fois que l'on sait comment demander d'activer un compteur pour les disques logiques sur un poste à distance,

Diskperf.sys -YV \\nomposte

installer une alerte ne devrait pas poser de problème

🔯 Analyseur de performances	
∫ 🗑 ⊆onsole Fe <u>n</u> être <u>?</u>	
$\int \underline{A}$ ction Affic <u>h</u> age Eavoris $\int \Leftrightarrow \Rightarrow \int \underline{f}$	
Arbre Favoris Nom	Commentaire
Racine de la console Moniteur système Journaux et alertes de perform Journaux de compteur Journaux de traçage Alertes	eaux paramètres d'alerte ? X on de disque OK Annuler
	saturation de disque
Avec les paramètres suivants	Général Action Planification
	Cette alerte commence dès que vous appliquez les modifications.
	Commentaire : permet de voir une saturation prochaine du disque
Sur la machine <u>\\client2kp7</u>	Compteurs : \\CLIENT2KP7\Disque logique(C:)\% Espace libre
Lorsque l'on a 60% de plein	Alerte lorsque la valeur est : supérieure à 🔽 Limite : 60 Ajouter Supprimer
Tester 1 fois pas jour	Période d'échantillonnage des données : Intervalle : 1 💌 Unités : jours 💌

📓 Analyseur de performances			
∫ 🛃 Console Fe <u>n</u> être <u>?</u>			🗋 🖨 🖬
	- → £ 🖬 Ø 🗟) \$\$] D ▶ ■	
Arbre Favoris	Nom	Commentaire	
Racine de la console	saturation de disque	permet de voir une saturation prochaine du disque	
Moniteur système	attente imprimante	permet de détecter une file d'attente trop importante	
🗄 🗑 Journaux et alertes de perform			
🛛 🌌 Journaux de compteur			
Journaux de traçage			
Alertes			





SCRIPT DE MISE A L'HEURE

Création du script :

Un petit script de mise à l'heure fonctionnera très simplement à partir du moment ou il est stocké dans le dossier adéquat du serveur 2000,

Dossiers	x	Nom 🛆	T	Туре
		💿 essai.bat	1 Ko	Fichier de commande MS-DOS
庄 🧰 domain				
🛄 staging				
🗄 💼 staging areas				
🖹 🗐 sysvol				
🖻 💼 domaine2.edu				
DO_NOT_REMOVE_NtFrs_PreInstall_Director	У			
🔁 💼 Policies				
a scripts				
DO_NOT_REMOVE_NtFrs_PreInstall_Director	y			

et qu'il contiendra des instructions du type :

🛃 essai.bat - Bloc-notes	
Fichier Edition Format ?	
het use g: /home net time \\serveur2	/set /y

Droit de modification de l'heure système :

Bien sûr sur une machine windows, le script s' exécutera sans problème, car tout le monde a le droit de modifier cette heure système.

Mais il n'en va pas de même pour un client 2000, sur lequel nativement un tel script n'a aucun effet...

En effet il faut aller voir dans

panneau configuration / outils d'administration/ Stratégies locales, et vérifier qui peut modifier l'heure système...

Stratégie de sécurité locale

🖥 Paramètres de sécurité locaux			_ 8 ×
$ $ <u>A</u> ction Affichage $ $ $\Leftrightarrow \Rightarrow$ $ $ E $ $ \times $ $) E		
Arbre	Stratégie 🔺	Paramètre local	Paramètr 🔺
Paramètres de sécurité	Contraction de la cet ordinateur depuis le réseau	Tout le monde,Utilisateurs,Utilisateurs a	Tout le m
	Agir en tant que partie du système d'ex		
⊨⊡ Stratégies locales	Ajouter des stations de travail au domaine		
🕀 🛄 Stratégie d'audit	Arrêter le système	Utilisateurs,Utilisateurs avec pouvoir,Op	Utilisateu
	B Augmenter la priorité de planification	Administrateurs	Administr
🗄 🛄 Options de sécurité	Augmenter les quotas	Administrateurs	Administr
🗄 🖳 Stratégies de clé publique	Autoriser que l'on fasse confiance aux c		
	Charger et décharger des pilotes de pér	Administrateurs	Administr
	_		
0			

on peut alors voir que



Windows NT 2000 travaux pratiques

Stratégie 🛆	Paramètre local	Paramètre en cours
聞Accéder à cet ordinateur depuis le réseau 聞Agir en tant que partie du système d'ex	J Tout le monde,Utilisateurs,Utilisateurs a	. Tout le monde, Utilisateurs, Utilisateurs avec po
ie Ajouter des stations de travail au domain:		Lindenstanding the state of the
iojArreter le systeme	Utilisateurs, Utilisateurs avec pouvoir, Op.,	Utilisateurs, Utilisateurs avec pouvoir, Operateu
Augmenter la priorite de planification	Administrateurs	Administrateurs
Augmenter les quotas	Administrateurs	Administrateurs
Matoriser que fon fasse conhance aux c	A desinistentes yes	Administration
	Auministrateurs	Administrateurs
Biglicheen des objets partages permanents Biglicheen un fichier d'échange	Administrateurs	Administrateurs
BCréer un objet-jeton	Mahimistratears	Mammilistratears
Déboquer des programmes	Administrateurs	Administrateurs
Bercer l'arrêt à partir d'un système distan	t Administrateurs	Administrateurs
Générer des audits de sécurité		
Gérer le journal d'audit et de sécurité	Administrateurs	Administrateurs
Modifier les valeurs d'env. de microprog	. Administrateurs	Administrateurs
Modifier l'heure système	Utilisateurs avec pouvoir,Administrateurs	Utilisateurs avec pouvoir,Administrateurs
Optimiser les performances système	Administrateurs	Administrateurs
exemple, alors on fe nanipulation suivante : in double-cliquant dessu On obtient	Attribué à Attribué à Administrateurs Utilisateurs avec pouvo	re système Local Effectif Paramètre de stratégie Paramètre de stratégie ir I
Dans lequel on Ajoute		
es utilisateur authentifiés	;	
	Ajouter	
	Si des paramètres de strate remplacent les paramètres	égie sont définis au niveau du domaine, ils de stratégie locale.
	V	OK Annuler

Dans le dossier

pour obtenir finalement

ANONYMOUS LOGON TACHE CREATEUR PROPRIETAIRE GROUPE CREATEUR LIGNE

Vérifier les noms

Nom

🕵 Tout le monde 🕵 Utilisateurs authentifiés

Ajouter

Microsoft



٠

•

	Paramètre de stra	atégie de sécurité local	e 📔	? ×
	Modifi	er l'heure système		
	Attribué à	Local Paramètre de straté	Effectif gie Paramètre de stratég	jie
	Administrateurs Utilisateurs avec Utilisateurs auth	pouvoir 🛛 🗹 entifiés 🔹 🔽		
ou enco	ore			
88 Modifi	er les valeurs d'er	nv. de microprog A	dministrateurs	
Modifi	er l'heure systèm	e U	tilisateurs authentifiés,U	tilisateurs avec pouvoir,Administrateurs
[<mark>88</mark>]Optimi	iser les performar	ices système A	dministrateurs	

Exemple d'écrasement entre stratégie locale et stratégie de DC :

Regardons la même chose, à titre de curiosité sur le contrôleur de Domaine.

On a dit que les paramètres locaux sont modifiées dans cet ordre (si cela à un sens)

stratégies locale – stratégie de Contrôleur de Domaine

Par conséquent si on regarde les **stratégies locales** sur un contrôleur de domaine (notre serveur), en ce qui concerne **Modifier l'heure système** on va trouver alors

	Paramètre de st	ratégie de sécurité locale	<u>? ×</u>
	Modi	fier l'heure système	
On retrouve « classiquement » les administrateur et les	Attribué à	Local Paramètre de stratégie	Effectif Paramètre de stratégie
utilisateurs avec pouvoir, mais on s'aperçoit que les paramètres effectifs diffèrent !	Opérateurs de Administrateurs Utilisateurs ave	serveur 🔲 - c pouvoir 🗹	
\backslash			

En effet au niveau stratégie de contrôleur de Domaine on va trouver

		Paramètre de stratégie de sécurité	? ×
		Modifier l'heure système	
Et les stratégies cumulatives !	sont	 Définir ces paramètres de stratégie : Administrateurs Opérateurs de serveur 	1



STRATEGIE LOCALE 1°

Augmenter la sécurité :

Pour augmenter la sécurité à propos de la connexion sur un réseau, on souhaite effectuer plusieurs modification de la sécurité d'une machine

1. Ne pas faire afficher le dernier identificateur de session utilisé sur cette machine

Ne pas afficher le dernier nom d'utilisateur dans l'écran d'ouverture de session

2. Ne pas permettre une ouverture de session si le contrôleur de domaine est indisponible

📖 Nombre d'ouvertures de session précédentes dans le cache (au cas ou le contrôleur de domaine

Mettez en œuvre localement cette stratégie, testez là, puis redonnez les valeurs par défaut...

Il faut aller dans les options de sécurité



et demander pour

🔃 Ne pas affich	er le dernier nom d'utilisateur dans l'écran d'ouverture de session		Désactivé	Désactivé
	Paramètre de stratégie de sécurité locale Ne pas afficher le dernier nom d'utilisateur dans l'écran d'ouverture de session	<u>?</u> ×		
On double clic puis on demande Activée	Paramètres de la stratégie en cours : Désactivé Paramètre de stratégie locale :			
	Activée Désactivé			
	Si des paramètres de stratégie sont définis au niveau du domaine, ils remplacent les paramètres de stratégie locale.			
on obtien	it alors		↓ ·	
🛄 Ne pas affich	ner le dernier nom d'utilisateur dans l'écran d'ouverture de session	Ļ	• Activé	Désactivé





Windows NT 2000 travaux pratiques

	Nombre d'ou	ivertures d	le session précédentes dans le	e cache (au cas ou	u le contrôleu	l0 Ouvertures	de session 1	0 Ouvertures de se	ssion
		Paramèt	re de stratégie de sécurité	locale	? X				
		F	Nombre d'ouvertures de sessie cas ou le contrôleur de domair	on précédentes da ne ne serait pas di	ans le cache (au sponible)				
		Paramèti	res de la stratégie actuelle						
On double clic	nuis	10 0	Duvertures de session						
on demande 0	pois	Param	ètre de stratégie locale						
		► Nep	oas mettre en cache les ouvertu Uuvertures de sessio	res de session : m					
		Si des pa remplace	aramètres de stratégie sont défir ent les paramètres de stratégie lo	nis au niveau du do ocale.	omaine, ils				
				OK	Annuler	•			
	on obtier	nt alors	5						
	Nombre d'ou	vertures de	e session précédentes dans le	cache (au cas ou	u le contrôleu () Ouvertures d	le session 1	0 Ouvertures de se	ession
	Après rec	lémarr	rage du poste on	aura bier	า				
	🛞 Nombre d'ou	ivertures d	le session précédentes dans le	e cache (au cas c	ou le contrôleu	0 Ouvertures	de session C) Ouvertures de sei	ssion
	🗓 Ne pas affic	her le dern	iier nom d'utilisateur dans l'écr	ran d'ouverture c	le session	Activé	ł	Activé	
	pour retro manière	ouver à obte	la situation initia	ile, il faut	faire les r	nanipulc	ations inv	erses, de	

Ne pas afficher le dernier nom d'utilisateur dans l'écran d'ouverture de session Désactivé Activé
 Nombre d'ouvertures de session précédentes dans le cache (au cas ou le contrôleu... 10 Ouvertures de session 0 Ouvertures de session

puis effectuer un re démarrage !



STRATEGIE LOCALE 2°

Pister les tentatives d'accès :

Dans une entreprise, on souhaite pister les tentatives d'accès infructueuses effectuées sur le réseau. On souhaite avoir des renseignements lorsque on a des tentatives de connexion qui échouent....

Le principe va consister à armer une stratégie d'audit basée sur les **évènements de connexion aux comptes**.

Par définition on n'auditera que les tentatives qui échouent, en sachant que l'événement est enregistré sur la machine sur laquelle l'identification se fera...

Audit sur le client :

On suppose que les tentatives de connexions se font depuis une machine isolée dans un bâtiment, la nuit. On va placer dessus donc un audit sur les echec.

Paramètres de sécurité locaux								
Action Affichage $4 \leftrightarrow \rightarrow 1$ $1 \otimes 1 $								
Arbre	Stratégie 🗸	Paramètre local	Paramètre en cours					
Paramètres de sécurité	Auditer l'utilisation des privilèges	Pas d'audit	Pas d'audit					
🗄 📴 Stratégies de comptes	B Auditer les modifications de stratégie	Pas d'audit	Pas d'audit					
🖻 🤷 Stratégies locales	B Auditer les événements système	Pas d'audit	Pas d'audit					
Stratégie d'audit	BAUditer les événements de connexion aux comptes	Échec	Échec					
🗄 🧰 Attribution des droits utilisateur	B Auditer les événements de connexion	Pas d'audit	Pas d'audit					
🕀 📴 Options de sécurité	Auditer le suivi des processus	Pas d'audit	Pas d'audit					
🕀 🖳 Stratégies de clé publique	Auditer l'accès aux objets	Pas d'audit	Pas d'audit					
🗄 🛃 Stratégies de sécurité IP sur Ordinat	Auditer l'accès au service d'annuaire	Pas d'audit	Pas d'audit					
	B Auditer la gestion des comptes	Pas d'audit	Pas d'audit					

Essayez d'ouvrir une session en tant qu'administrateur du domaine, en vous trompant . Que lisez vous dans le journal d'événement ?

•••

Les évènements sont consignés sur le système qui effectue l'authentification, par conséquent ce n'est que **si on se trompe en essayant d'ouvrir une session locale**, que l'on pourra observer alors dans le journal sécurité

Observateur d'événements								_ 8 ×
Action Affichage $4 \Rightarrow 12$ 12 12 12 12 12 12								
rbre Journal sécurité 2 événement(s)								
Observateur d'événements (loc	Туре	Date	Heure	Source	Catégorie	Évén	Utilisateur	Ordinat
Journal applications	Audit des échecs	29/05/2002	01:06:56	Security	Connexio	681	SYSTEM	CLIENT
	of Audit des succès	29/05/2002	01:04:06	Security	Événeme	517	SYSTEM	CLIENT:







	Propriétés de Événement					
	Événement					
	Date : Heure : Type : Utilisateur : Ordinateur :	29/05/2002 01:06 Audit des AUTORITE N CLIENT2KP8	Source : Catégorie : ID événement : IT\SYSTEM	Security Connexion de compte 681	 ↑ ↓ ■ 	
avec comme explication	Description Échec de I par : MICF depuis la s Le code d	: 'ouverture de s lOSOFT_AUTI station de trava 'erreur est : 322	ession sur le com HENTICATION_P il : CLIENT2KP8 21225578	pte : administrateur ACKAGE_V1_0		

Audit sur le serveur :

Si on veut une trace des tentatives infructueuses sur le domaine, il faut auditer le contrôleur de domaine, on se place sur le contrôleur, on active les stratégies de sécurités locale.....

🖥 Observateur d'événements							_ 8 ×		
Action Affichage $4 \Rightarrow 12$ III 2^{2} 2^{2}									
Arbre Journal sécurité 2 événement(s)									
Observateur d'événements (local)	Туре	Date	Heure	Source	Catégorie	Évén	Utilisateur		
Journal applications Journal sécurité Journal système Directory Service DIS Server Service de réplication de fichiers	Audit des échecs	29/05/2002 29/05/2002	01:08:47 00:39:03	Security Security	Connexion de compte Événements système	675 517	SYSTEM SYSTEM		
	Propriétés Événemen	de Événemen t	t			<u>? x</u>			
	Date : Heure : Type : Utilisateu Ordinateu Descriptio	29/05/2002 01:08 Audit des r: <u>AUTORITE</u> ar: SERVEUR2	Source : Catégorie : ID événem NT\SYSTEM	Security Connex ent : 675	, ion de compte	► ► ■			
Échec de la pré-authentification : Nom de l'utilisateur : Administrateur ID de l'utilisateur : DOMAINE2\administrateur Nom du service : krbtgt/DDMAINE2 Type de pré-authentification : 0x2 Code d'échec : 24 Adresse du client : 192.168.1.8									

N.B: on s'apperçoit que les sratégies définies sur les contrôleurs de Domaines viennent "écraser" les stratégies définies localement.



STRATEGIE AUDIT ACCES DOSSIER

Objectif:

On veut savoir qui essaye d'utiliser (alors qu'il n'en a pas le droit) le dossier de pierre, qui contient des documents confidentiels mis à disposition pour certains de ses collègues.

Il faut d'abords sur la machine sur laquelle le dossier existe, activer l'audit au niveau des ressources de manière générale.

Paramètres de sécurité locaux			_ 🗆 🗵
Action Affichage $4 \Leftrightarrow \Rightarrow 1 \textcircled{1} \textcircled{1} \times$	E 2		
Arbre	Stratégie 🔺	Paramètre local	Paramètre en cou
Paramètres de sécurité	BB Auditer la gestion des comptes	Pas d'audit	Pas d'audit
Final Stratégies de comptes	🕮 Auditer l'accès au service d'annuaire	Pas d'audit	Pas d'audit
🗄 🚾 Stratégies locales	Auditer l'accès aux objets	Pas d'audit	Pas d'audit
🕂 💼 Stratégie d'audit	Auditer le suivi des processus	Pas d'audit	Pas d'audit
🕂 🛄 Attribution des droits utilisateur	Auditer les événements de connexion	Pas d'audit	Pas d'audit
⊕ @ Options de sécurité	Auditer les événements de connexion aux comptes	Échec	Échec
Paramètre de stratégie d Auditer l'accès au Paramètres de la stratégie en Pas d'audit Paramètre de stratégie loc Auditer ces essais : Essais ayant réussi Image: Essais ayant échoué Si des paramètres de stratégie remplacent les paramètres de	e sécurité locale ? 🗶 k objets ale ie sont définis au niveau du domaine, ils e stratégie locale.	emarrer	

Mais là on obtient une surprise de taille, c'est que la boite de dialogue sécurité locale affiche une information un peu déroutante :

On a bien demandé Audit sur Echec, mais en cours il y a pas d'audit !

Paramètres de sécurité locaux			
Action Affichage ⇐ ⇒ 🔁 🗊			
Arbre	Stratégie 🔺	Paramètre local	Paramètre en cours
Paramètres de sécurité	🕮 Auditer la gestion des comptes	Pas d'audit	Pas d'audit
🗄 👜 Stratégies de comptes	🕮 Auditer l'accès au service d'annuaire	Pas d'audit	🔻 Pas d'audit
🗄 📑 Stratégies locales	聞Auditer l'accès aux objets	Échec	Pas d'audit
🚾 Stratégie d'audit	Auditer le suivi des processus	Pas d'audit	Pas d'audit
🕀 📴 Attribution des droits utilisateur	Auditer les événements de connex	Pas d'audit	Pas d'audit
in minimise de sécurité	Auditer les événements de connex	Échec	Échec





Windows NT 2000 travaux pratiques Cabaré Michel C.U.E.F.A. S4 T.P. v1.4 Page 59

Cela provient du fait que pour les contrôleur de domaine, il existe des paramètres que l'on gère dans la mmc **Outils Administration / Stratégie de Sécurité du contrôleur de domaine** passant après les paramètres de sécurité locaux d'une machine...

🖸 Stratégie de sécurité du contrôleur de domaine						
Action Affichage	□ × B₀ £					
Arbre	Stratégie 🛆	Paramètre de l'ordinateur				
Paramètres Windows	Auditer la gestion des comptes	Pas d'audit				
🗄 🖬 Paramètres de sécurité	B Auditer l'accès au service d'annuaire	Pas d'audit				
🗄 🛃 Stratégies de comptes	避Auditer l'accès aux objets	Pas d'audit				
🗄 🖓 Stratégies locales	B Auditer le suivi des processus	Pas d'audit				
🖬 🖅 🚮 Stratégie d'audit	Auditer les événements de connexion	Pas d'audit				
🕀 🛒 Attribution des droits utilisate	B Auditer les événements de connexion aux co	Non défini				
🖭 🛃 Options de sécurité	BB Auditer les événements système	Pas d'audit				
🕀 🚽 Journal des événements	Auditer les modifications de stratégie	Pas d'audit				
Groupes restreints Groupes restr	Auditer l'utilisation des privilèges	Pas d'audit				
Envices systeme	l					
Or ceux-ci sont positionné	par défaut à					
Paramètre de stratégie de sécurité						

			Paramet	cre	'e de strategie de securi	e			
			F	A	Auditer l'accès aux objets				
Pas d'A	Ludit !	>	Défi Aud	finir dite Es Es	ir ces paramètres de stratégie er ces essais : ssais ayant réussi ssais ayant échoué				
						[OK	Annule	r

Soit on demande de désactiver à ce niveau, et on garde la commande dans les permissions de sécurités locales, soit on "force" ici en demandant d'activer l'audit sur les ressources en cas d'Echec...

Paramètres du contrôle d'accès pour pierre ? × Autorisations Audit Propriétaire puis il faut pour le dossier de Entrées d'audit : pierre accéder aux permissions Type Nom Accès Appliquer à NTFS et demander Avancée on a alors Supprimer Afficher/Modifier... Aiouter.. 🥅 Permettre la propagation d'entrées d'audit provenant de l'objet parent à cet objet Réinitialiser les entrées d'audit sur tous les objets enfants et permettre la propagation des entrées d'audit pouvant être héritées.

Dans laquelle il faut Ajouter



	Sélectionnez Utilisateur, Ordinateur ou Grou	ре	<u>? x</u>
La graupa prádáfini	Regarder of domaine2.edu		•
Le groupe predenni	Nom	Dans le dossier	
Tout le monde			
\			
\backslash			
\setminus	WENTERPRISE DUMAIN CONTROLLERS		_
·	Tout le monde		
	Nom :		
		OK Annu	ler

et en indiquant l'audit voulu :

Audit de l'entrée pour pierre Objet Nom : Tout le monde Appliquer à : Ce dossier, les sous-dossi	Modifie	? × m			
Accès : Parcourir le dossier/Exécuter le fichier Liste du dossier / Lecture de données Attributs de lecture Lire les attributs étendus Création de fichiers / Écriture de donné Attributs d'écriture Écriture d'attributs étendus Suppression de sous-dossiers et de fir Supprimer Autorisations de lecture Modifier les autorisations Appliquer ces entrées d'audit aux ob et/ou aux conteneurs à l'intérieur de conteneur uniquement	Réussite Échec	tout	Audit pour (tentat	sur la ive)	Echec lecture

Lorsqu'un utilisateur non autorisé tente la lecture du dossier de pierre,

🖁 Observateur d'événements							_ 8 ×
$ $ <u>A</u> ction Affichage $ $ $\Leftrightarrow \Rightarrow $ E		Ê					
Arbre	Journal sécurité 3 é	vénement(s)					
Observateur d'événements (local)	Туре	Date	Heure	Source	Catégorie	Évén	Utilisateur
Journal applications	Audit des échecs	29/05/2002	02:31:00	Security	Accès aux objets	560	titi
Journal sécurité	Audit des échecs	29/05/2002	02:31:00	Security	Accès aux objets	560	titi

L'événement est consigné

	Propriétés de Événement	<u>? x</u>
	Événement	
└ ▶	Date: 29/05/2002 Source: Security Heure: 02:31 Catégorie: Accès aux objets Type: Audit des ID événement: 560 Utilisateur: DOMAINE2XIII Ordinateur: SERVEUR2 Description:	 ↑ ↓ □
	Objet Ouverture : Objet Serveur : Security Objet Type : File Objet Nom : C:\ressource\pierre N [®] du nouveau handle : - N [®] d'opération : {0,164229} N [®] de processus : 8	•





Cabaré Michel C.U.E.F.A. S4 T.P. v1.4 Page 61

STRATEGIE AUDIT IMPRIMANTE

Savoir qui imprime :

Il faut activer l'Audit "Accès aux objets" dans les stratégies locales de l'ordinateur sur lequel l'imprimante est connectée.

On doit demander Audit sur Réussite

Ensuite il faut se placer sur l'imprimante que l'on souhaite auditer, et demander dans les propriétés de l'imprimante:

Paramètres d	u contrôle d'a	accès pour HP Lase	erJet 6P	?>	×1
Autorisations	Audit Prop	riétaire			
Entrées d'au	udit :				
Туре	Nom	Accès	Appliquer à		
Réussit	e Tout le mon	de Imprimer	Cette imprimante et le	s documents	
Ajouter	r S	upprimer Affiche	er/Modifier		
Cette entrée	e d'audit est défi	nie directement sur ce	et objet. Cette entrée d'aud	it est héritée par	
les objets er	irants.				

onglet Sécurité / Avancées et onglet Audit...

Audit de l'entrée pour HP LaserJe	≥t 6P	? ×
Objet		
Nom : Tout le monde	es documents	Modifier
Accès :	Réussite	Échec
Imprimer Gestion d'imprimantes Gestion des documents Autorisations de lecture Modifier les autorisations Appropriation		



MODELE DE STRATEGIE LOCALE

Objectif:

Obtenir sur disquette 3 modèles de stratégie locale, permettant de définir via un message qui s'afficherait avant l'invite d'ouverture de session, l'appartenance de la machine a un groupe particulier...

On pourrait ainsi disposer de 3 modèles :

- 1. Un modèle affichant l'appartenance à un « groupe A »
- 2. Un modèle affichant l'appartenance à un « groupe B »
- 3. Un modèle n'affichant plus aucune appartenance (efface les effets des modèles précédents...)

Rappelez vous que les stratégies sont définies dans des fichiers xxxx.inf stockés en général dans Winnt\Security\Templates

Création et sauvegarde d'un modèle :

Après avoir lancé (crée ?) la console , on se crée un nouveau modèle correspondant au groupe A...



dans lequel on défini uniquement le titre et le contenu du message pour les utilisateurs essayant de se connecter





Windows NT 2000 travaux pratiques pour enregistrer le modèle on peut bien sur enregistrer classiquement, puis copier manuellement le fichier sur disquette, mais on peut aussi demander directement **enregistrer sous**...

È C groupe A È-C P Strat E-C P Strat È-C P Strat E-C P 4	Ouvrir Définir la description Enregistrer Enregistrer sous	Et ch	noisir classiquement !	
	Enregistrer sous			<u>? ×</u>
	Enregistrer dans :	🔄 templates	. ← 🗈 💣 💷 -	
	policies basicdc.inf basicsv.inf basicwk.inf 窗 compatws.inf 窗 DC security.inf	groupe A.inf hisecdc.inf hisecws.inf notssid.inf ocfiless.inf ocfilesw.inf	securedc.inf securews.inf setup security.inf test.inf	
	Nom de fichier :	groupe A.inf		Enregistrer
	Type :	Modèle de sécurité	(.inf)	Annuler

Si on a appliqué le modèle, il est possible de demander exporter le modèle...

Récupération et utilisation d'un modèle :

Après avoir lancé (crée ?) la console,

🗎 Racine de la console
Configuration et analyse de la sécurité

un fois une base de donnée crée (ouverte) il faut récupérer notre modèle. via le menu contextuel **importer un modèle**...

Modèle d'importati	on		? ×
Rechercher dans :	Disquette 3½ (A:)		-
S groupe A			
modele B			
iii neutre			
Nom de fichier :	groupe A		Ouvrir
Туре:	Modèle de sécurité (.inf)		Annuler
Fifacer cette bas	se de données avant d'importer		1.
	Modèle d'importati Rechercher dans : groupe A modele A modele B neutre Nom de fichier : Type : Effacer cette bas	Modèle d'importation Rechercher dans : Image: Disquette 3½ (A:) Image: groupe A Image: modele B Image: modele B <td>Modèle d'importation Rechercher dans : Disquette 3½ (Å:) groupe A modele A modele B neutre neutre Modèle de sécurité (.inf) Effacer cette base de données avant d'importer</td>	Modèle d'importation Rechercher dans : Disquette 3½ (Å:) groupe A modele A modele B neutre neutre Modèle de sécurité (.inf) Effacer cette base de données avant d'importer





Windows NT 2000 travaux pratiques il ne reste plus que l'analyse,

via le menu contextuel analyser l'ordinateur maintenant...

Arbre Favoris	Stratégie 🛆	Paramètre de base de d	Paramètre de l'ordin
Racine de la console	🐯 Contenu du message pour les utilis	vous êtes du groupe A !	
🗄 🗃 Configuration et analyse de la sécurité	Créer un fichier d'échange de mém	Non défini	Désactivé
🗄 🛃 Stratégies de comptes	BDésactiver la combinaison de touc	Non défini	Non défini
🖻 🖓 Stratégies locales	BDurée d'inactivité avant la déconn	Non défini	15 minutes
🔃 🛃 Stratégie d'audit	BBEmpêche la maintenance par le sy	Non défini	Désactivé
🗄 📆 Attribution des droits utilisateur	Empêcher les utilisateurs d'installer	Non défini	Désactivé
Options de sécurité	BD Envoyer un mot de passe non cry	Non défini	Désactivé
🗄 🖓 Journal des événements	Fermer automatiquement la sessio	Non défini	Activé
	🕮 Ne pas afficher le dernier nom d'ut	Non défini	Désactivé
Gervices système	🕮 Ne permettre l'accès au CD-ROM q	Non défini	Désactivé
	🕮 Ne permettre l'accès aux disquett	Non défini	Désactivé
±	🕮 Niveau d'authentification Lan Man	Non défini	Envoyer les répons
	Nombre d'ouvertures de session p	Non défini	0 Ouvertures de se
	BBPermet au système d'être arrêté s	Non défini	Activé
	BBPermet aux opérateurs de serveur	Non défini	Non défini
	Bermet l'éjection des supports NTF	Non défini	Administrateurs
	B)Prévenir l'utilisateur qu'il doit chan	Non défini	14 derniers jours
	Renforcer les autorisations par dé	Non défini	Activé
	BBRenommer le compte administrateur	Non défini	Administrateur
	Renommer le compte Invité	Non défini	Invité
	Restrictions supplémentaires pour	Non défini	Aucun. Utiliser les a
	Signer numériquement les commun	Non défini	Activé
	Signer numériquement les commun	Non défini	Désactivé
	Signer numériquement les commun	Non défini	Désactivé
	Bigner numériquement les commun	Non défini	Désactivé
	🐯 Titre du message pour les utilisate	bonjours	

et l'application

via le menu contextuel **configurer l'ordinateur maintenant**...

- **N.B** : pensez a vérifier l'application de votre modèle....



CREATION DE GPO SUR UNE UO

Objectifs:

Dans le domaine, on dispose de deux services, un service pour les commerciaux, et un autre pour les secrétaires.

A terme, le gestion des postes des commerciaux est radicalement différente de celle des postes des secrétaires, par conséquent on va se créer des UO et des GPO pour chacune de ces entitées.

- Vérifier que lorsqu'un ordinateur fait partie d'une UO (commerciaux par exemple), il récupère automatiquement sa stratégie...
- Vérifier que pour récupérer la stratégie de l'autre UO (secretaire donc), il suffit de déplacer le compte ordinateur dans l'OU adéquate...

Le but ici étant pédagogique, les GPO n'auront pas d'autres effet que d'annoncer lors d'un message apparaissant à la mise sous tension l'appartenance à telle ou à telle entité (du genre, "bonjours, votre poste est régit par le modèle de sécurité affecté aux commerciaux/ (ou)secrétaires....")

Définir 2 UO dans AD , et créer leur GPO :

Il faut commencer par se créer deux UO commerciaux et secretaires

🔏 Utilisateurs et ordinateurs Active Directory [serveur2.do	Nom	Туре
🗄 🗊 domaine2.edu	📕 client2kp7	Computer
🗄 🛅 Builtin	elient2kp8	Computer
Computers		
🛛 🧭 Domain Controllers		
🗄 💼 ForeignSecurityPrincipals		
🗄 📲 Users		

On se place ensuite sur l'UO des commerciaux, et on demande propriété, puis onglet **Stratégie de groupe/ Nouveau**

	Liaisons de l'objet Stratégie de groupe actuel pour commerciaux			
Liaisons Øpour	a de l'objet Stratégie de groupe commerciaux	Ne pas pas		

puis modifier





On va créer notre GPO pour les commerciaux affichant notre appartenance au groupe des commerciaux



Si on se place sur l'UO prédéfinie **Computers**, on voir normalement tous les postes du domaine...



Il est nécessaire de déplacer les postes faisant partie de la section des commerciaux dans leur UO pour qu'ils héritent de leur stratégie. Prenons par exemple client2kp8

Arbre	Computers 2	2 objet:	s	
Utilisateurs et ordinateurs Active Directory [serveur2.do	Nom		Туре	Description
🗄 🗊 domaine2.edu	elient2kp7		Computer	
	client2kp8		Computor	
		Non	nmer les mappa	ages
		Dés	activer le comp	ote
		Réir	nitialiser le com	pte
		Dép	olacer	



on	obtient	a	lors

Déplacer Conteneur vers lequel l'objet doit être dé	placé :	1
Image: Comparison of the comparison		On indique sa nouvelle UO d'appartenance
Arbre	commerciaux 1 objets	5
Utilisateurs et ordinateurs Active Directory [serveur2.dor - - - - - - - - - - - - -	Nom T Sclient2kp8 C	ype Description computer

• vérifier que lorsque l'on démarre le poste, un message indique bien l'appartenance aux commerciaux...

Changer d'UO = changer de GPO :

On va créer une GPO pour les secretaire affichant notre appartenance au groupe des secretaire.

Donc on procède de manière identique a ce que l'on a fait précédemment



Puis on déplace le poste faisant partie de la section des commerciaux dans leur UO pour qu'ils héritent de leur stratégie. Prenons par exemple client2kp8, qui "passe" dons de commercial à secretaire...

Arbre		commerciaux	1 objets	
Utilisateurs et ordinateurs Active domaine2.edu Utilisateurs et ordinateurs Active Builtin Commerciaux Computers Computers Computers	Directory [serveur2	t.doi Mom	Type Nommer les map Désactiver le cor Réinitialiser le co Déplacer	Description pages npte mpte
On indique sa nouvelle UO d'appartenance, de commerciaux on la passe dans secretaire	Déplacer Conteneu	rr vers lequel l'objet doi domaine2 Builtin Computers Domain Controllers ForeignSecurityPrin LostAndFound Secretaires	t être déplacé : ncipals	? ×
Microsoft WindowsNT. travaux p	NT 2000 Dratiques	Cabaré N C.U.E.F.A.	∕ichel S4 T.P. v1.4	Page 6

 vérifier que lorsque l'on ouvre une session, un message indique toujours l'appartenance aux commerciaux...et non pas aux secretaires !

Forcer une application de GPO avec secedit :

La GPO que l'on construit avec l'UO secretaire et commerciaux, est une GPO d'ordinateur, donc pour être prise en compte, elle nécessite un redémarrage du poste.

Il est possible avec Secedit de forcer la propagation de cette stratégie, avec la commande :

Secedit /refreshpolicy machine_policy

🖾 Invite de commandes	
Microsoft Windows 2000 [Version 5.00.2195] (C) Copyright 1985-1999 Microsoft Corp.	_
E:\>secedit /refreshpolicy machine_policy La propagation des stratégies de groupe à partir du domaine a été initiée po et ordinateur. La terminaison de la propagation et la prise d'effet de la no le stratégie peuvent prendre quelques minutes. Vérifiez qu'il n'y a pas d'en s dans le journ E:\>^P	our c ouvel rreur

On vérifie dans le journal d'événement que cela s'est bien passé

🖁 Observateur d'événements							
] <u>A</u> ction Affic <u>h</u> age] ⇐ → 🗄	I 🖬 🖬 🚺	B 2					
Arbre	Journal application	ons 123 événem	ent(s)				
🗑 Observateur d'événements (local)	Туре	Date	Heure	Source	Catégorie	Évén	Utilisateur 🔺
Journal applications	Informations	02/06/2002	11:02:37	SceCli	Aucun	1704	N/A
Propriétés de Événement Événement				<u>? ×</u>			
Date: 02/06/2002 So Heure: 11:02 Co Type: Informations ID Utilisateur: N/A Ordinateur: CLIENT2KP8	ource : atégorie : , événement :	SceCli Aucun 1704		 ↑ ↓ ↓ ↓ 			
Description :							
La stratégie de sécurité dans correctement.	les objets Straté	ègie de groupe :	est appliquée				

• vérifier que lorsque l'on ouvre une session, un message indique maintenant l'appartenance aux secretaires !



GPO MODELE D'ADMINISTRATION DE DOMAINE

Objectifs :

Dans un domaine, on souhaite pour tous les utilisateurs du domaine sauf l'administrateur (si on ne veut pas quelle s'applique à l'administrateur, il faut le placer dans une UO spécifique et bloquer l'héritage sur cette UO...) la GPO suivante :

- 1. Supprimer le menu exécuter du menu Démarrer
- 2. Désactiver Active desktop
- 3. Désactiver l'accès au Panneau configuration affichage
- 4. Exécuter uniquement les applications prévues
- 5. Désactiver Windows Update

Blocage de la stratégie pour l'administrateur:

Puisque l'on va définir une GPO sur des utilisateurs, on bloque l'héritage sur une l'UO que l'on définie manuellement, dans laquelle tous les utilisateurs sur lesquels on ne veut pas que notre GPO de domaine s'applique ...(a savoir pour nous l'administrateur)

A thick as a set of the star of A stine Directory	Propriétés de a part
dominateurs et ordinateurs Active Directory	Général Géré par Objet Sécurité Stratégie de groupe
⊡ Builtin ⊡ Computers ⊡…@ Domain Controllers ⊕ ForeignSecurityPrincipals	Liaisons de l'objet Stratégie de groupe actuel pour a part
	L'interne de Pakies Chastánia de antiga
· ···· · · · · · · · · · · · · · · · ·	Liaisons de robjet strategie de groupe ne pas pas
	Plus un objet Stratégie de groupe est haut dans la liste, plus sa priorité Cette liste a été obtenue à partir de : s1.dom1.com
	Nouveau Ajouter Modifier
on bloque l'héritage	Options Supprimer Propriétés D
de L' UO contenant	✓ Bloquer l'héritage de stratégies
l'administrateur	





Windows NT 2000 travaux pratiques

Mise en oeuvre de la stratégie de domaine :

En se plaçant sur le domaine, on grée une nouvelle GPO nommée « **politique** globale »

N.B : Il vaut mieux créer une nouvelle GPO que modifier la GPO **Default Domain policy** existante par défaut...

Propriétés de domaine1.edu	? ×
Général Géré par Objet Sécurité Stratégie de	groupe
Liaisons de l'objet Stratégie de groupe ac	stuel pour domaine1
Liaisons de l'objet Stratégie de groupe	Ne pas pas Désacti
🛃 Default Domain Policy	
∰politique globale	

Puis on demande modifier...



Bien sûr il faut appliquer cette GPO sur le client, soit on attends le temps de propagation standard, soit on force depuis le client via la commande

Secedit /refreshpolicy machine_policy (si c'est une config ordinateur)

Secedit /refreshpolicy user_policy

(si c'est une config utilisateur)

1. Supprimer le menu exécuter du menu Démarrer...



2. Désactiver Active Dekstop



3. Désactiver l'accès au Panneau configuration affichage



4. Exécuter uniquement les applications prévues !







Windows NT 2000 travaux pratiques Cabaré Michel C.U.E.F.A. \$4 T.P. v1.4 Page 72
5. Désactiver Windows Update

Arbre	Stratégie	Paramètre
Stratégie politique globale [serveur1.domaine1.edu]	🛱 Supprimer le dossier des utilisateurs du menu Démarrer	Non configuré
🖃 폟 Configuration ordinateur	🛱 Désactiver et supprimer les liens vers Windows Update	Non configuré
🗄 🔲 Paramètres logiciel	🛱 Supprimer le groupe de programmes communs du menu Démarrer	Non configuré
🗄 💼 Paramètres Windows	😰 Supprimer le menu Documents du menu Démarrer	Non configuré
	🛱 Désactiver les programmes du menu Paramètres	Non configuré
🗄 🚜 Configuration utilisateur	🛱 Supprimer les Connexions réseau et accès distant du menu Démar	Non configuré
🗄 🛄 Paramètres logiciel	🛱 Supprimer le menu Favoris du menu Démarrer	Non configuré
🚊 🛄 Paramètres Windows	🛱 Supprime le menu Rechercher du menu Démarrer	Non configuré
🖻 🖳 Modèles d'administration	🚰 Supprimer le menu Aide du menu Démarrer	Non configuré
⊡ Composants Windows □	🕞 Supprimer le menu Exécuter du menu Démarrer	Désactivé
Menu Démarrer et Barre des tâches	Ajouter Déconnecter au menu Démarrer	Non configuré
	🛱 Désactiver la fermeture de session dans le menu Démarrer	Non configuré
H. D fanneau de configuration	🛱 Désactiver et supprimer la commande Arrêter	Non configuré
	🛱 Désactiver le glisser-déplacer des menus contextuels dans le men	Non configuré
H. Systeme	Empêcher la modification des paramètres de la barre des tâches e	Non configuré









Windows NT 2000 travaux pratiques Cabaré Michel C.U.E.F.A. S4 T.P. v1.4

GPO DEPLOIEMENT DE SERVICE PACK

Objectifs :

Déployer automatiquement un SP sur un ensemble de machine ...

Mise en oeuvre :

Dans un dossier que l'on partage en lecture seule, on copie le source du SP3,

C:\SP>dir Le volume da Le numéro de	ans le lecte e série du v	eur C n'a pa volume est B	s de nom. C11-DBEF
Répertoire d	le C:∖SP		
04/06/2003 1 04/06/2003 1 29/08/2002 0	L5:56 L5:56 28:41	<dir> <dir> 131 303</dir></dir>	536 W2Ksp3.exe

que l'on explose via la commande w2ksp3.exe -x dans le même dossier...

on peut observer qu'un dossier /i386/update est crée contenant un fichier update.msi...



On se crée ensuite une GPO



dans laquelle on va choisir une configuration d'ordinateur...





on va chercher un chemin réseau amenant à notre \\serveur\Sp\i386\update\update.msi

on devrait arriver à cela

<i>⊈t</i> Strat	égie de groupe				
<u> </u>	Affic <u>h</u> age	• •			
Arbre		Nom A	Vers	ion	
G Strate	égie appli_sp [s1.dom1.com] ▲ onfiguration ordinateur ☐ Paramètres logiciel ☐ Installation de logiciel	Hindows 2000 Service Pa	ck 3 (1036) 5.0		
État du déploie	Installation automatique	Type de mise à niveau	Mise à niveau	Paramètr	Source
Attribué	Oui	Nécessaire	Aucun	Français	\\S1\sp\i386\update\update.msi

Il n'y a plus qu'à disposer les UC voulues dans notre UO... et redémarrer les postes...





CREATION D'UN LOT MSI

Objectifs:

Dans le but d'effectuer un déploiement par GPO, il nous faut un fichier MSI adéquat...

Il est possible de s'en créer un, soit avec des outils professionnels, soit avec un outils livré en "démo" avec windows 2000...

Installation du logiciel création de msi :

Il est stocké sur tous les CD 2000, on prends le fichier SWIADMLE.MSI...



on obtient de nouveaux raccourcis:

👼 VERITAS Software 💿 🕨	🔎 VERITAS Discover
	🛃 VERITAS Software Console

Le principe de création d'un fichier msi est le suivant:

- 1. il va falloir faire un instantané du système "avant" l'installation du programme pour lequel on veut faire un fichier msi,
- 2. puis un instantané "après" l'installation du programme
- 3. et le soft crée un différentiel entre les deux...
- **N.B:** Bien sûr ceci doit se faire sur une machine dont la configuration logicielle est la plus proche possible de celle des machines cibles...



instantané avant:

on démarre Veritas Discover, puis NEXT, puis

WinINSTALL Discover	X
	Specify the name of the application for which you are building the installation: snagit
	Specify the path and filename for the data file (.msi file) where the information on this installation will be kept: C:\configsnagit
	Select the language to be used for installer messages for this package: Français (France)
< Back Next	Cancel Help

On indique le nom de l'application

Et l'endroit ou le MSI doit être crée à terme...

on choisit un disque ou il y a de la place (pour stocker les fichiers d'enregistrement de config) et ensuite on précise puis les disques a surveiller...

WinINSTALL Discover Select which drives Discover sho you like (but each drive will take drives where you expect that cha	ould scan for change a little while to scan, anges may occur).	es. You can select as many as so you should select only those	×
Available Drives:	Add > Add All >> < Remove << Remove All	Drives to Scan:	
< Back Next >		Cancel Help	

et s'il faut exclure certains dossiers de ... "la surveillance"

the scan:	.	Files & Wildcard Entries
All Directories:	Add > Add All >> < Remove << Remove All	Directories & Files to Exclude *SPART.PAR OFIDX*.FF? c:\rsecure.nt\ c:\catalog.wci\
< Back Next >		Cancel Help



Windows NT 2000 travaux pratiques puis le travail se fait et un message comme quoi la configuration actuelle est mémorisée apparaît.

L	aunch A.	pplication Setup Program
		The 'Before' snapshot is complete.
	\checkmark	If you click OK, Discover will prompt you for the setup program to run and will exit after launching it.
		OK Annuler

Installation du logiciel pour lequel on veut un msi :

Dans la foulée,

Run Application Set	up Program		? ×
Rechercher dans :	🖃 Disque local (C:)	• 🖬 📩 🖬 •	
 bidet configsnagit Discover.wrk doc Documents and Si Program Files 	WINNT Transformed and the second se		
Nom de fichier :	× ×		Ouvrir
Type :	All Files (*.*)	•	Annuler

et on peut paramétrer le logiciel, et ses points de lancement (raccourcis, modif de menu...)

instantané après:

l'instantané après se lance comme pour l'instantané de début ...

on obtient dans le dossier indiqué au début (pour nous le dossier C:\configsnagit\) la totalité de ce que l'on doit publier y compris le fichier msi de départ...!

le reste est désormais routinier....



EFS - CRYPTAGE DE FICHIER

3 utilisateurs indépendants :

Soit sur une machine 3 utilisateurs farouchement indépendants, pierre, paul jacques, pour lesquels il faut s'assurer que ils ne puissent absolument aller lires leurs documents respectifs...

On décide que le dossier dans lequel ils doivent poser leurs document est le dossier DATA, sur lequel on activera le cryptage. En tant qu'administrateur du poste, on active le cryptage du dossier DATA...

Vérifier que lorsqu'un document y à été crée par pierre il y est automatiquement crypté avec la clé personnelle privée de pierre, et par conséquent ni paul ni jacques ne peuvent y accéder.... (mais que l'administrateur, agent de récupération par défaut, peut)

sur une machine autonome

sur une machine autonome, c'est l'administrateur qui est agent de récupération : ici on a ouvert une mmc avec ses certificats. par défaut

🚡 Console1 - [Racine de la console\Certificats - Uti	lisateur actuel\Pers	sonnel\Certifical	ts]			_ 8 ×
j ∰ <u>C</u> onsole Fenêtre <u>?</u>] 🗋 🖨		: <u>- 8 ×</u>
] Action Affichage Eavoris] ⇐ → € 💽	E B B 2			★		
Arbre Favoris	Délivré à 🔺	Délivré par	Date d'expiration	Rôles prévus		Nom complet
Racine de la console Gertificats - Utilisateur actuel Gertificats - Utilisateur actuel Gertificats	Administrateur	Administrateur	26/04/2102	Récupération de	fichier	<aucun></aucun>
et dans les propriétés on voit bien que le système EFS a	Certificat Général Détails Afficher :	Chemin d'accès	de certification		ļ	? ×
demandé le certificat lors de	Champ		Valeur			
l'installation du poste	Version Numéro de s Algorithme o Émetteur Valide à par Valide jusqu Objet Clé publique	série de signature tir du 'au	V3 CD12 C564 8974 sha1RSA EFS File Encrypt lundi 20 mai 200 mercredi 26 avri EFS File Encrypt RSA (1024 Bits)	4 BB89 4326 5 ion Certificate 2 15:17:17 I 2102 15:17:17 ion Certificate	T	

Si l'administrateur crypte lui

même un dossier, il se voir attribuer un certificat d'identification pour la diffusion de sas clé publique...





Windows NT 2000 travaux pratiques Cabaré Michel Pc C.U.E.F.A. S4 T.P. v1.4

$]$ <u>Action</u> Affichage Eavoris $] \leftarrow \Rightarrow]$	n 🗗 🖬 🖻			
Arbre Favoris	Délivré à 🔺	Délivré par	Date d'expiration	Rôles prévus
Racine de la console	Administrateur	Administrateur	26/04/2102	Récupération de fichier
💼 🗐 Certificats - Utilisateur actuel	🖭 Administrateur	Administrateur	26/04/2102	Système de fichiers de cryptage
Certificats				

Dans un domaine

E:\>cd data
E:\data>efsinfo
E:\data\
pierre.doc: Encrypted Users who can decrypt: CLIENT2KP8\pierre (CN=pierre,L=EFS,OU=EFS File Encryption Certificate)
E:\data>efsinfo /r
E:\data\
pierre.doc: Encrypted Recovery Agents: DOMAINE2\Administrateur (OU=EFS File Encryption Certificate, L=EFS, CN=Admin istrateur)
E:\data>

N.B : dans cet exemple, le fichier crypté par l'utilisateur local pierre du poste client2kp8 est crée sur une machine appartenant à un domaine DOMAINE2. Par conséquent seul l'administrateur de domaine est l'agent de récupération. une fois que le fichier sera placé sur la machine contrôleur de domaine (le serveur initial de config de domaine, car seulement sur cette machine il y a le certificat de l'administrateur du domaine). Si cela ne convient pas, et que l'on veut ouvrir le fichier sur le poste ou il a été crée, il faut y ouvrir une session en tant qu'administrateur du domaine, et y ajouter les certificats préalablement exportés depuis le contrôleur de domaine : A NE PAS FAIRE POUR DES RAISONS DE DISPERTION DES CERTIFICATS !)

N.B: Si le poste se **déconnecte** du domaine, on n'aurait alors plus d'agent de récupération pour ce fichier... (si on s'y reconnecte, on retrouve notre agent de récupération)

```
E:\data>efsinfo /r
E:\data\
pierre.doc: Encrypted
Recovery Agents:
Unknown (OU=EFS File Encryption Certificate, L=EFS, CN=Administrateur)
```

Exportation Import de certificat :

Pour pouvoir faire en sorte que paul puisse modifier le fichiers cryptés par pierre, il faut exporter le certificat de pierre, et l'importer pour paul

Exportation du certificat de pierre sur disquette

Ayant une session pour pierre, on crée une mmc certificats







On se place sur certificats à gauche, puis menu contextuel sur le certificat de pierre

Dans laquelle on va enclencher l'exportation de certificat avec la clé privée de Pierre

Les étapes sont claires

4	ssistant Exportation de certificat	×
	Exportation de la clé privée Vous pouvez choisir d'exporter la clé privée avec le certificat.	
	Les clés privées sont protégées par mot de passe. Pour pouvoir exporter la clé privée avec le certificat, vous devez entrer son mot de passe dans une des pages suivantes.	
	Voulez-vous exporter la clé privée avec le certificat ?	
	Oui, exporter la dé privée	
	C Non, ne pas exporter la clé privée	





Assista	ant Exportation de certificat		x
Mo	t de passe Pour maintenir la sécurité, vous devez protéger la clé privée en utilisa passe.	int un mot de	
	Entrez et confirmez le mot de passe.		
	Mot de passe :		
	Confirmer le mot de passe :		
Assista	nt Exportation de certificat		×
Fic	n ier à exporter Spécifiez le nom du fichier à exporter		
	Nom du fichier :		_
	a:\pierre	Parcourir	

A partir de là, on dispose du certificat de pierre (et de sa clé privée) sur une disquette. Il reste à le donner à paul...

Importation du certificat de pierre dans paul

Ayant une disquette contenant le certificat de pierre,

Disquette 31/2 (A:)	
pierre.pfx Échange d'informations personnelles	pierre.pfx
Modifié le: 19/05/2002 10:59	
Taille : 1,71 Ko	

et ayant ouvert une session pour paul, on crée une mmc certificats

🛗 Console Fenêtre ?) D 🖨 日	•
Action Affichage Eavoris	⇔ → € 💽 💼 🔮	5			
Arbre Favoris	Délivré à 🔺	Délivré par	Date d'expiration	Rôles prévus	Nom co
Racine de la console Gertificats - Utilisateur actuel Gertificats - Utilisateur actuel Gertificats	[≌] paul	paul	25/04/2102	Système de fichiers de cryptage	<aucur< td=""></aucur<>
 ⊕ ··· → Autorités de c ⊕ ··· → Approbation d ⊕ ··· → Autorités inter Autorités inter Nouvelle 	es tâches 🔹 🕨 e 🔹 kan bartir d'ici	Demander un no Importer	ouveau certificat		

on va enclencher l'importation de certificat avec la clé privée de Pierre...



Assistant Importation de certificat	×
Fichier à importer	
Spécifiez le fichier à importer.	
Nom du fichier :	
A:\pierre.pfx Parcourir	
Remarque : plusieurs certificats peuvent être stockés dans un seul fichier aux formats suivants :	
Échange d'informations personnelles - PKCS #12 (.PFX,.P12)	
Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.p7b)	
Magasin de certificats sérialisés Microsoft (.sst)	

Assistant Importation de certificat	x
Mot de passe	
Pour maintenir la sécurité, la clé privée a été protégée avec un mot de passe.	
Entrez le mot de passe de la clé privée.	
Mot de passe :	
Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.	
Marquer la clé privée comme étant exportable	

Lorsque l'assistant se termine on devrait avoir

Arbre Favoris	Délivré à 🔺	Délivré par	Date d'expiration	Rôles prévus
Racine de la console Gertificats - Utilisateur actuel Personnel Gertificats	🖼 paul	paul	25/04/2102	Système de fichiers de cryptage
	🔛 pierre	pierre	25/04/2102	Système de fichiers de cryptage

et paul peut désormais modifier les documents de pierre

Annulation non rétro-active de l'import de certificat

Le temps passe, et paul se fâche avec pierre, comment peut on empêcher paul d'accéder aux fichiers de pierre ?

Il faut ouvrir une session en tant que Paul, aller dans les certificats...

Arbre Favoris	Délivré à 🔺	Délivré par	Date d'expiration	Rôles prévus
Certificats - Utilisateur actuel	🔤 paul 🔛 pierre	paul pierre	25/04/2102 25/04/2102	Système de fichiers de cryptage Système de fichiers de cryptage
Personnel	1			

et supprimer le certificat de pierre dans sa liste de certificats...



Pourquoi Pierre peut il toujours modifier les documents déjà existant de pierre ? car s'il les a déjà ouvert, leur champs liste DRF (liste des agents récupérateurs) inclus l'utilisateur Pierre comme personne habilité à les gérer.

Par contre, si maintenant Paul crée d'autres documents, ceux-ci sont inutilisables à Pierre





EFS – SECURISER UN POSTE

Vol d'un poste (portable ?) :

Si on a compris le principe de la sécurisation, on a compris que sur une machine, par défaut le Compte de l'Agent de récupération par défaut est celui de l'Administrateur de Domaine (dans le cas d'une machine faisant partie d'un domaine) ou le compte de l'Administrateur Local...

Si on sécurise le dossier mes documents par exemple, le seul compte permettant de visualiser tous les fichiers est donc celui de l'agent de récupération...

Pour sécuriser au maximum une machine, il suffit d'exporter le certificat du compte de l'agent de récupération, en exportant sa clé privée en un endroit sûr, par exemple une disquette que l'on stockera en un lieur sur !

A partir de la , l'agent de récupération n'existe plus !!!!! il faut pour le « reconstruire » que l'on importe le certificat et sa clé privée, ce qui suppose d'avoir accès à la disquette

Export du certificat de l'agent de récupération d'un poste autonome :

Le poste étant autonome (hors Domaine), il faut ouvrir une session en tant qu'administrateur local...

🎢 certificats - [Racine de la console\Certificats - Ul	tilisateur actuel\Pei	rsonnel\Certificat:	5]	_ 12
∫ 🊰 ⊆onsole Fe <u>n</u> être <u>?</u>] 🗋 🖨 🔚 🔲 💶
Action Affichage Eavoris \rightarrow \leftarrow \rightarrow \bigcirc \blacksquare \checkmark \textcircled{B} \times \textcircled{B} \textcircled{B}				
Arbre Favoris	Délivré à 🔺	Délivré par	Date d'expiration	Rôles prévus
Racine de la console Gertificats - Utilisateur actuel Gertificats - Utilisateur actuel Gertificats	Administrateur Administrateur	Administrateur Administrateur	26/04/2102 26/04/2102	Récupération de fichier Système de fichiers de cryptage

et demander d'exporter

dans l'assistant il faut indiquer alors



	Assistant Exportation de certificat	x
	Exportation de la clé privée Vous pouvez choisir d'exporter la clé privée avec le certificat.	
	Les clés privées sont protégées par mot de passe. Pour pouvoir exporter la clé privée avec le certificat, vous devez entrer son mot de passe dans une des pages suivantes.	
	Voulez-vous exporter la clé privée avec le certificat ?	
	 Oui, exporter la cle privée Non, ne pas exporter la clé privée 	
et surtout		
	Assistant Exportation de certificat	×
Sinon la clé est	Format de fichier d'exportation Les certificats peuvent être exportés sous plusieurs formats de fichier.	
laissée localement	Sélectionnez le format à utiliser :	
	C Binaire codé DER X.509 (.cer)	
	🖸 Codé à base 64 X.509 (.cer)	
I	 Standard de syntaxe de message cryptographique - Certificats PKCS #7 (,p7b) Inclure tous les certificats dans le chemin d'accès de certification si possible 	
	Échange d'informations personnelles - PKCS #12 (.pfx)	
	🦳 Inclure tous les certificats dans le chemin d'accès de certification si possible	
	🔽 Activer la protection renforcée (nécessite IE 5.0, NT 4.0 SP4 ou supérieur)	
	Effacer la clé privée si l'exportation s'est terminée correctement	

Vérifier que désormais l'administrateur n'est plus agent de récupération (ou plutôt il est toujours agent de récupération, mais ne dispose plus de la clé privée...)

Import du certificat de l'agent de récupération d'un poste autonome :

En cas de problème, on ouvre une session en tant qu'administrateur et on demande d'importer la clé

🐂 certificats - [Racine de la console\Certificats - U	tilisateur actuel\Pe	rsonnel\Certifical	:s]	_ 6	X
∫∰ <u>C</u> onsole Fe <u>n</u> être <u>?</u>] D 🗳 🖬 💷 💷	١×
_ <u>A</u> ction Affic <u>h</u> age Eavoris ↓ ← → 🗈 🖬	Image: A marked and a marked				
Arbre Favoris	Délivré à 🔺	Délivré par	Date d'expiration	Rôles prévus	Nom
Racine de la console	🔤 Administrateur	Administrateur	26/04/2102	Récupération de fichier	<al< td=""></al<>
🗄 🝘 Certificats - Utilisateur actuel	🕮 Administrateur	Administrateur	26/04/2102	Système de fichiers de cryptage	<au< td=""></au<>
🛱 📲 Personnel					
Certificats					
🕀 💼 Autorités de c 👘 Toutes les tâches	Demand	ler un nouveau certif	icat		
Approbation c Affichage	Importe	r			

depuis la disquette...



Assistant Importation de certificat	x
Fichier à importer	
Spécifiez le fichier à importer.	
Nom du fichier :	
A:\adminserveur1.pfx Parcourir	
Remarque : plusieurs certificats peuvent être stockés dans un seul fichier aux formats suivants :	
Échange d'informations personnelles - PKC5 #12 (.PFX,.P12)	
Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.p7b)	
Magasin de certificats sérialisés Microsoft (.sst)	

N.B : pour que cela marche, la clé ne suffit pas, il faut la réimporter dans le compte qui est agent de récupération par défaut... (ici administrateur local). Ainsi une tentative d'import de la clé dans un autre compte quelconque du poste, se solderait par un échec de la lecture des fichiers cryptés !

donc deux choses importantes :

le compte administrateur (agent de récupération) la clé privée exportée dans la disquette



SESSION TERMINAL SERVER

Analyser une session TS :

on veut savoir actuellement quelles sont les sessions en cours via Terminal Server, on peut sur le serveur ou TS est installé lancer la mmc **Gestionnaire de services Terminal Server**



Soit un utilisateur boby, pour lequel on a donné les autorisations nécessaires... Regardons à travers le gestionnaire des services Terminal server, une session depuis le poste **client2kp8**, d'un utilisateur **boby** lançant **wordpad** sur le serveur2...

Lorsque boby sur le client demande une session Terminal Server, avant même qu'il ait pu s'identifier, le simple fait de demander

Démarrer / Programmes puis Client Terminal Server donne dans le gestionnaire de service







rosott



Cabaré Michel Page 89 C.U.E.F.A. S4 T.P. v1.4 lorsque boby s'identifie correctement sur le client, on peut alors voir

sa session								
ESERVEUR2 - Gestionnaire des services Terminal Server								
Actions Affichage Outils Aide								
Tous les serveurs énumérés	Utilisateurs Sessi	ions Processu	s					
	Session	Utilisateur	ID	État	Туре	Nom du client		
RDP-Tcp (écouteur)	(en attente)		2	Inactif				
RDP-Tcp#10 (boby)	(en attente)		3	Inactif				
Console (administrateur)	🖳 Console	administrateur	0	actif	Console			
···· (Inactif)	- RDP-Tcp		65536	écouter	Microsoft RDP 5.0			
(Inactif)	⊶ RDP-Tcp#10	boby	1	actif	Microsoft RDP 5.0	CLIENT2KP8		
	' 🗡							

Une vue des session en cours pour le domaine ou le serveur est disponible :



On peut suivre précisément ce que fait boby par les processus qu'il lance



Puis boby commet l'erreur classique de fermer sa fenêtre , donc il se **déconnecte**, mais **ses processus tournent toujours**..



Si ici boby se reconnecte, il retrouve son environnement , et toutes ses applications...



rosott



IT 2000 Cabaré Michel atiques C.U.E.F.A. S4 T.P. v1.4

\sim			• •				•		
()n	noutcur	la carva ir	VOIL	20	nrocassi is c		2001020	decor	nnactaac
\sim \sim				63		10	303310113	accor	111001003

SERVEUR2 - Gestionnaire des services T	erminal Server					_ 8 ×
Actions Affichage Outils Aide						
🖃 👰 Tous les serveurs énumérés	Litilisateurs Se	ssions Processus				
🗄 🗊 DOMAINE2			<u> </u>			
	Utilisateur	Session	ID	PID	Image	<u> </u>
BDP-Tcp (écouteur)	System	Console	0	792	dfssvc.exe	
Console (administrateur)	System	Console	0	812	topsvos.exe	
	System	Console	0	840	svchost.exe	
deconnecte (boby)	System	Console	0	852	ismserv.exe	
(Inactif)	System	Console	0	868	llssrv.exe	
i (Inactif)	System	Console	0	904	ntfrs.exe	
	System	Console	0	948	regsvc.exe	
	System	Console	0	960	locator.exe	
	System	Console	0	976	mstask.exe	
	System	Console	0	1028	termsrv.exe	
	System	Console	0	1092	lserver.exe	
	System	Console	0	1172	winmgmt.exe	
	System	Console	0	1192	dns.exe	
	System	Console	0	1220	inetinfo.exe	
	System	Console	0	1820	svchost.exe	
	System	(en attente)	3	1996	winlogon.exe	
	System	(en attente)	3	1296	csrss.exe	
	System	(en attente)	2	1888	winlogon.exe	
	System	(en attente)	2	1600	CSISS.exe	
	System	Déconnecté	1	2140	winlogon.exe	
	System	Déconnecté	1	2128	CSISS.exe	
	administrateur	Console	0	1080	wordpad.exe	
	administrateur	Console	0	2088	snagit32.exe	
	administrateur	Console	0	1328	tsadmin.exe	
	administrateur	Console	0	368	internat.exe	
	administrateur	Console	0	2052	explorer.exe	
	boby	Déconnecté	1	1728	rdpclip.exe	
	boby	Déconnecté	1	1972	explorer.exe	
F	boby	Déconnecté	1	1344	internat.exe	
	boby	Déconnecté	1	2024	wordpad.exe	_
						•

Si boby se reconnecte, et demande **démarrer /arreter / fermer la session** tout rentre dans l'ordre

Mais on peut aussi depuis le serveur « faire le ménage »





TEST DE DUPLICATION D'AD

Créer un 2° CD sur notre Domaine :

Dans un domaine **dom1.com** on doit se créer un 2° CD à partir d'un serveur 2000 nommé **S2**.... pour venir épauler notre premier CD nommé **S1**.



Un fois le 2° Contrôleur de Domaine opérationnel, par exemple **\$2**, on crée sur ce serveur un compte **Nouveau**, mot de passe **n**.

Essayez d'ouvrir un session avec ce compte **Nouveau** depuis une machine du domaine: bien sûr cela marche !

Revenons sur le premier serveur **\$1**, le compte utilisateur Nouveau n'apparaît pas. Il n'apparaîtra que dans un délais d'environ **5 mn** !

Visualisation du trafic de duplication :

Visualiser le trafic entre 2 nos CPD et forcer la mise a jour sans attendre les 5 mn, pour vérifier à des fins de test que la réplication est bien opérationnelle.

Le fichier sur le CD se trouve dans les **SUPPORT\TOOLS\SETUPEXE** et se nomme **repimon.exe.**

Une fois l'installation effectuée on lance Active Directory Replication Monitor









on voit que la dernière synchronisation s'est faite le 23/05 à 5h15:32

on se place sur l'ensemble des 3 composants Schéma-Configuration-Domaine et on clique avec le bouton contextuel, **Synchronize...** ou via le menu **Action / Replication partner / Synchronise with...**

🍜 Active Directory Replication Monitor	
File Edit Action View Help	
Monitored Servers:	Cancel Auto Update
Monitored Servers	Log: C:\Documents and Settings
🖻 🏢 Premier-Site-par-defaut	Status as of: 23/05/2003 17:1
⊡…] s2	>> Direct Replication Partn
CN=Schema,CN=Configuration,DC=dor	Server is current throug
CN=Configuration DC=dom1 Synchro	onize with this Replication Partner
message de confirmation apparaît	

UN MESSAGE DE CONTIFMATION APPARAII Active Directory Replication Monitor

•	Synchronization queued successfully. Note that Active Directory Replication Monitor only requested that the synchronization be initiated. Refresh the statistics to verify if replication completed successfully.

et si on demande de rafraîchir via le menu view refresh

🍜 Active Directory Replication Monitor	_ 🗆 🗵
File Edit Action View Help	
Monitored Servers:	Cancel Auto Update
Monitored Servers Monitored Servers S2 CN=Schema,CN=Configuration,DC=dor Premier-Site-par-defaut\S1 CN=Configuration,DC=dom1,DC=com Premier-Site-par-defaut\S1 C=- Premier-Site-par-defaut\S1	Log: C:\Documents and Settings\administrateur.SERVEUR1\Mes documents\s2-CN=Schem Status as of: 23/05/2003 17:14:15 >> Direct Replication Partner Data << Server is current through Property Update USN: 2901 The last replication attempt was successful. This took place at: 5/23/2003 4:57:00 Status as of: 23/05/2003 17:16:02 >> Direct Replication Partner Data << Server is current through Property Update USN: 2939 The last replication attempt was successful. This took place at: 5/23/2003 5:15:32 Status as of: 23/05/2003 17:21:07 >> Direct Replication Partner Data << Server is current through Property Update USN: 2963 The last replication Attempt was successful. This took place at: 5/23/2003 5:20:26
	٩ 🔪 ۲
	23/05/2003 17:21

on voit que la dernière synchronisation s'est faite le 23/05 à 5h20:26



Υl

REPLICATION INTER-SITE

Créons 2 sites distants de 62 machines maximum relié par RNIS:

Soit pour nous par exemple une **adresse privée réseau de classe** C **192.168.1.xx**, si on veut créer des sous réseau dans cette adresse, il va falloir poser un masque de sous réseau autre que 255.255.255.0

Si on veut **2 sous réseaux** comportant chacun **62 machines maximum**, on pourra prendre alors comme masque de sous réseau **255.255.255.192**

• Id réseau

pour trouver les ld réseau je dois trouver toutes les combinaisons de **2 bits** de 11 à 00 en laissant tomber les valeurs n'ayant que des 0 ou que des 1 (non autorisée).J'obtient 10-01-soit en décimal 128-64.

que je rajoute à mon ld réseau d'origine 192.168.1.xx soit donc les ld réseau suivantes :

192.168.1.**128** 192.168.1.**64**

• Id hôte valide un petit calcul nous donne :

sous-réseau	1° adresse IP	dernière adresse IP
192.168.1. 64	192.168.1.65	192.168.1.127
192.168.1. 128	192.168.1.129	192.168.1.191

Créer les sites nécessaires :

Dans la mmc Sites et services Active Directory on crée le site distant (puisque le premier site par défaut existe déjà)

uvel objet	- Site			
	Créer dans :	domaine2.edu/Configuratio	on/Sites	
Nom :	distant			
Sélectionne dans le cor	ez un objet lie Iteneur Trans	n de site pour ce site. Les o ports sites/inter-sites.	bjets lien de site	sont situés
Nom du li	en		Transport	
BBBBBB	и тирентски	NIZ.	ID	



Définir un sous -réseau :

Dans la mmc Sites et cervies Active Directory

Pour créer les deux sous-réseaux nécessaires, il faut se mettre sur le dossier **Subnets**

et demander clic droit Nouveau / subnet

Nouvel objet - Subnet	X Nouvel objet - Subnet
Créer dans : domaine2.edu/Configuration/Sites/Subnets	Créer dans : domaine2.edu/Configuration/Sites/Subnets
Adresse : 192.168.1.64	Adresse : 192.168.1.128
Masque : 255 . 255 . 192	Masque : 255 . 255 . 192
Nom : 192.168.1.64/26	Nom : 192.168.1.128/26
Entrez l'adresse et le masque de sous-réseau, qui seront traduits automatiquement en un nom de sous-réseau de la forme réseau/bits masqués. Exemple : l'adresse 10.14.209.14 avec le masque 255.255.240.0 deviendra le sous-réseau 10.14.208.0/20.	Entrez l'adresse et le masque de sous-réseau, qui seront traduits automatiquement en un nom de sous-réseau de la forme réseau/bits masqués. Exemple : l'adresse 10.14.209.14 avec le masque 255.255.240.0 deviendra le sous-réseau 10.14.208.0/20.
Sélectionnez un objet du site pour ce sous-réseau.	Sélectionnez un objet du site pour ce sous-réseau.
Nom de site	Nom de site
distant	🗒 distant
# Premier-Site-par-defaut	🗒 Premier-Site-par-defaut

De manière à obtenir

🔣 Sites et services Active Directory								
Sing ⊆onsole Eenêtre ?								
Action Affichage $4 \Rightarrow 1$ 1 1 1 1 1 1 1 1 1								
Arbre	Nom	Site	Туре					
Sites et services Active Directory [serveur2.domaine2.edu] Sites Inter-Site Transports SMTP SMTP Premier-Site-par-defaut Subnets 192.168.1.128/26]⊞ 192.168.1.64/26]⊞ 192.168.1.128/26	Premier-Site-par-defaut distant	Subnet Subnet					

Associer un sous -réseau à un site:

On vérifie que l'on a bien

Propriétés de 192.168.1.64/26	Propriétés de 192.168.1.128/26
Sous-réseau Emplacement Objet Sécurité	Sous-réseau Emplacement Objet Sécurité
192.168.1.64/26	192.168.1.128/26
Description :	Description :
Site : Premier-Site-par-defaut	Site : distant 💌
Réseau: 192.168.1.64	Réseau: 192.168.1.128
Masque : 255.255.192	Masque : 255.255.192

Cabaré Michel

C.U.E.F.A. S4 T.P. v1.4

Page 95

Windows NT 2000

travaux pratiques

Création des liens de site:

Il faut créer un lien de site entre notre **premier-site-par-defaut** et notre site **distant.** On se place sur le protocole IP

🚮 Si	tes et services Active Directory [serveur2.domaine2.edu]		
ė@	Sites		
Ē	🛄 Inter-Site Transports		
		N.	
	Nouvel objet - Site Link	X	
	Créer dans : domaine2.edu/Configuration/Sites/Inter-Si		
			On nomme notre
			liaison
	Nom : liaison numeris		
	Sitos obsents do os lien Sitos présente dons co		liaison numeris
	de sites : Sites presents dans de		
	distant		
	Premier-Site-par-defaut		
	Ajouter >>		
	Les Compétent		
	<< subbutter		
	Une liaison de sites doit contenir au moins deux sites.		

et dans les propriétés on planifie quelques économies...



On oublie pas de poser un Contrôleur de domaine dans chaque site:





Windows NT 2000 travaux pratiques

TRANSFERT DE MAITRE D'OPERATION

Objectif:

Imaginons par exemple le transfert de l'Emulateur CPD depuis un contrôleur nommé serveur2 vers un contrôleur nommé serveur1.

On est sur le CD serveur 2

Dans la mmc **Utilisateurs et ordinateurs Active Directory** on essaye déjà de se connecter sur le serveur sur lequel on souhaite effectuer le transfert, c'est à dire pour nous **serveur1**

🐗 Utilisateurs et ordinateurs Active Directory	
🛛 🥪 Console Eenêtre ?	
$ \begin{tabular}{ c c c c } \hline \underline{Action} & Affichage \\ \hline \hline \underline{Action} & \hline \hline \underline{C} \\ \underline{C} \\ \hline \underline{C} \\ C$	整 🎽 🏹 🍕 🗑
Arbre	Utilisateurs et ordinateurs Active Directory
Utilisateurs et ordinateurs Active Directory [serveur2.domaine2.edu]	Nom T
i∰ domaine2.edu	Se connecter au domaine
🕀 📖 Builtin	Se connecter au contrôleur de domaine
	Maîtres d'opérations
on obtient alors	
Se connecter au contrôleur de domaine	
Domaine : domaine2.edu	
Contrôleur de domaine actuel : serveur2.domaine2.edu	
Remplacer par : serveur1.domaine2.edu	
Contrôleurs disponibles dans domaine2.edu :	
Nom	Tous les CD du
serveur1.domaine2.edu Premier-Site-par-defaut	Domaine
serveur2.domaine2.edu Premier-Site-par-defaut	— apparaissent
Tout contrôleur de domaine ouv	• •

étant maintenant placé sur le CD sur lequel on souhaite transférer le maître d'opération

∫ ⊈onsole Eenêtre ?	,	
$ $ Action Affichage $ $ $\leftarrow \rightarrow $ $ $] 喝 😰 🛛 🥶 塑 🎽 🖓 🍕 💆	
Arbre	Utilisateurs et ordinateurs Ac	
Utilisateurs et ordinateurs Active Directory [serve	sur1.domaine2.edu]	On demande
🗄 🗊 domaine2.edu	Se connecter au domaine	Maîtroo
	Se connecter au contrôleur de domaine	Maines
	Maîtres d'opérations	d'opérations





Windows NT 2000 travaux pratiques Cabaré Michel C.U.E.F.A. S4 T.P. v1.4 On vérifie bien ce que l'on veut faire, Et on demande Modifier

Maître d'opérations	1
RID CDP Infrastructure	
Le maître d'opérations émule les fonctions d'un contrôleur de domaine principal pour les clients fonctionnant avec une version antérieure à Windows 2000. Un seul serveur du domaine remplit ce rôle. Maître d'opérations :	
serveur2.domaine2.edu	
Pour transférer le rôle de Maître d'opérations à Modifier l'ordinateur suivant, cliquez sur Modifier.	┫ ╺━━━━
serveur1.domaine2.edu	

Un fois l'opération réalisée, refaite là dans l'autre sens pour retrouver la situation initiale

Essayez pour le contrôleur de schéma !





CREATION D'UN DOMAINE ENFANT

Création du C.D. "enfant.dom1.com" sur serveur S4 :

Il faut bien sûr que l'on ait de la connectivité IP et que l'on ait comme adresse de serveur DNS un serveur DNS du domaine parent...

Ensuite on peut lancer le **DCpromo**

\wedge
H.
ntrôleur
de domaine Jomaine.

ici on demande

	Assistant Installation de Active Directory	x
	Créer une arborescence ou un domaine enfant Vous pouvez créer une nouvelle arborescence de domaine ou un nouveau c	domaine enfant.
	Voulez-vous créer une nouvelle arborescence de domaine ou un nouveau do enfant dans une arborescence de domaine existante ?	omaine
	C Créer une nouvelle arborescence de domaine	
	Si vous ne voulez pas que le nouveau domaine soit enfant d'un domaine sélectionnez cette option. Cela créera une nouvelle arborescence de don séparée de toute arborescence existante.	existant, naine
	Vous pourrez alors choisir de placer la nouvelle arborescence de domaine forêt existante, ou de créer une nouvelle forêt.	e dans une
	O Oréer un nouveau domaine enfant dans une arborescence de domaine es	xistante
	Si vous voulez que le nouveau domaine soit enfant d'un domaine existant sélectionnez cette option. Par exemple, vous pourriez créer un nouveau o appelé siege.exemple.microsoft.com qui serait un enfant du domaine monentreprise.com.	t, Jomaine
	Assistant Installation de Active Directory	×
	Informations d'identification réseau Fournissez un nom d'utilisateur réseau et un mot de passe.	
	Entrez le nom d'utilisateur, le mot de passe et le domaine d'utilisateur du comp que vous souhaitez utiliser pour cette opération.	ite réseau
On précise	e Nom d' <u>u</u> tilisateur : administrateur	
domaine	Mot de passe :	
"parent"	Domaine : dom1.com	
	Morosoft	ichel Page 9

travaux pratiques

C.U.E.F.A. S4 T.P. v1.4

et on donne ensuite le nom du domaine "enfant"

Ir	Istallation d'un domaine enfant Sélectionnez le domaine parent et spécifiez un nom pour le nouveau domaine enfant.
	Entrez le nom DNS complet du domaine parent (par exemple : siege.exemple.microsoft.com).
	Domaine parent :
	dom1.com Parcourir
	Entrez le nom du nouveau domaine enfant (par exemple : ventes).
	Domaine enfant :
	enfant
-	Non DNS complet du nouveau domaine :

un nom netbios va être proposé,

Nom de domaine NetBIUS		\sim
Spécifiez un nom NetBIOS pou	ur le nouveau domaine.	1. Ale and the second s
Ceci est le nom que les utilisate identifier le nouveau domaine. entrez un nouveau nom.	eurs de versions précédentes de Windows utiliseront pour Cliquez sur Suivant pour accepter le nom affiché ou	

et tout l'assistant depromo est désormais classique pour aboutir au résumé final....

Assistant Installation de Active Directory	x
Résumé Vérifiez et confirmez les options que vous avez sélectionnées.	
Vous avez choisi de :	
Configurer ce serveur en tant que premier contrôleur de domaine dans un nouveau domaine.	
Le nom du nouveau domaine est "enfant.dom1.com"	
Le nom NetBIOS du domaine est "ENFANT"	
Ce nouveau domaine est un domaine enfant du domaine "dom1.com"	
Emplacement de la base de données : C:\WIN2000\NTDS Emplacement du fichier journal : C:\WIN2000\NTDS Emplacement du dossier Sysvol :C:\WIN2000\SYSVDL	
Pour modifier une option, cliquez sur Précédent. Pour continuer, cliquez sur Suivant.	

la création du domaine enfant se fait de manière automatique,

- ce serveur devient CD,
- et les relations d'approbations entre le domaine enfant et le domaine parent sont automatiquement construites., à savoir :
 - o le domaine enfant approuve le domaine parent
 - o le domaine parent approuve le domaine enfant



Vérification des relations d'approbations :

si tout se passe bien, lorsqu l'on ouvre la session sur le serveur CD du domaine enfant, on peut ouvrir la session sur un des deux domaines existants...

on peut vérifie dans outils d'administration / Domaines et approbations active directory

⁴ Domaines et approbations Active Directo	ory
$]$ Action Affichage $] \leftarrow \rightarrow $ im \blacksquare	8 Ø B 2
Arbre	Nom

SI on demande les propriétés de dom1.com

	Comaines et a	approbations Active Direct	tory	
	Action Afficha	ige] ⇐ ⇒ 🗄 💽	r 5. 2	
	Arbre		Nom	Туре
	ିଞ୍ଚ Domaines et ap	probations Active Directory	Penfant.dom1.com	domainDNS
	enfani	Gérer		
		Affichage 🕨 🕨		
		Exporter la liste		
		Propriétés		
V ∣		Aide		

naines approuvés pa	ir ce domaine :			
Nom de domaine	Relation	Transitif		Ce domaine : dom1.com
enfant.dom1.com	Enfant	Oui	Ajouter	Domaine Enfant : enfant.dom1.com
			Modifier	Type d'approbation : Parent-enfant
			Supprimer	Direction de l'approbation :
				Bidirectionnel : les utilisateurs de ce domaine peuvent s'authentifi
)omaines qui approuver	nt ce domaine :			Bidirectionnel : les utilisateurs de ce domaine peuvent s'authentifi l'autre domaine et les utilisateurs de l'autre domaine peuvent s'aut dans ce domaine.
omaines qui approuver Nom de domaine	nt ce domaine : Relation	Transitif		Bidirectionnel : les utilisateurs de ce domaine peuvent s'authentifi l'autre domaine et les utilisateurs de l'autre domaine peuvent s'aut dans ce domaine.
omaines qui approuver Nom de domaine enfant.dom1.com	nt ce domaine : Relation Enfant	Transitif Oui	Ajouter	Bidirectionnel : les utilisateurs de ce domaine peuvent s'authentifi l'autre domaine et les utilisateurs de l'autre domaine peuvent s'aut dans ce domaine. Transitivité de l'approbation :
omaines qui approuver Nom de domaine enfant.dom1.com	nt ce domaine : Relation Enfant	Transitif Oui	Ajouter Modifier	Bidirectionnel : les utilisateurs de ce domaine peuvent s'authentifi l'autre domaine et les utilisateurs de l'autre domaine peuvent s'aut dans ce domaine. Transitivité de l'approbation : Cette relation d'approbation est transitive. Les utilisateurs de dom approuvés indirectement au sein de l'entreprise peuvent s'authen auprès du domaine qui approuve.
omaines qui approuver Nom de domaine enfant.dom1.com	nt ce domaine : Relation Enfant	Transitif Oui	Ajouter Modifier Supprimer	Bidirectionnel : les utilisateurs de ce domaine peuvent s'authentifi l'autre domaine et les utilisateurs de l'autre domaine peuvent s'aut dans ce domaine. Transitivité de l'approbation : Cette relation d'approbation est transitive. Les utilisateurs de doma approuvés indirectement au sein de l'entreprise peuvent s'authen auprès du domaine qui approuve.





Windows NT 2000 travaux pratiques Cabaré Michel C.U.E.F.A. S4 T.P. v1.4 Annuler

Appliquer

ΟK

Gestion de zone DNS :

Maintenant réfléchissons : on a un domaine enfant, mais ce domaine ne dispose pas de son propre serveur DNS, il utilise le serveur DNS du domaine parent....

Ce qui pose un certain problème de fiabilité, ou de dépendance...

தீ DNS
🚊 <u>2</u> , <u>C</u> onsole <u>F</u> enêtre <u>?</u>
Action Affichage $4 \Rightarrow 1$
Arbre
훗, DNS
🖻 📑 51
🚊 💷 Zones de recherche directes
🖻 👘 dom1.com
📺 🧰 msdcs
tcp
udp
The Cones de recherche inversée

Pour délégué une zone vers un serveur DNS du domaine enfant, il va falloir suivre un mode opératoire précis :

- 1. Création d'une délégation pour le domaine enfant sur le serveur racine (parent)
- 2. Installation d'un serveur enfant dans le domaine enfant
- 3. Création d'une zone appropriée sur ce serveur
- 4. Reparamétrage du serveur DNS enfant

Création d'une délégation sur le serveur DNS racine :

Sur le serveur DNS parent, que l'on appelle également serveur racine (à ne pas confondre avec la zone DNS racine ".") il faut créer une délégation correspondant au domaine enfant.

Cela correspond à une zone que l'on ne souhaite plus prendre en charge, car elle va être gérée a terme sur le

serveur DNS du domaine enfant.

On se place sur notre zone parent et on demande via le menu contextuel Nouvelle délégation....



Un assistant déclenche se et demande le nom du domaine enfant

	Assistant Nouvelle délégation	x
and the second	Nom du domaine délégué Spécifiez le nom du domaine que vous voulez créer.	
puis il taut donner l'adresse IP du serveur DNS qui va héberger la zone enfant via Ajouter	L'autorité pour le domaine que vous créez sera déléguée à une zone différente. Domaine délégué : enfant Nom de domaine pleinement qualifié : enfant.dom1.com	





Windows NT 2000 travaux pratiques

Cabaré Michel C.U.E.F.A. S4 T.P. v1.4

	Assistant Nouvelle délégation		x	l
	Serveurs de noms Vous pouvez sélectionner un o déléguée.	ou plusieurs serveurs de noms pour héberger la z	zone	
	Spécifiez les noms ou les adre: comme hôte pour la zone délé	sses IP de tous les serveurs DNS que vous voul guée.	ez utiliser	
	Nom de serveur	Adresse IP		
	Ajouter Modifier	Supprimer		
		Nouvel enregistrement de ressource Serveur de noms (NS)	-	<u>?</u> ×
Il faut rentrer ici un du serveur DNS, on trouver (résoudre)	nom adresse IP ne peut pas le 	Nom du serveur : s4 Adresse IP : 192 .168 .1 .34 Ajouter	Parcourir	Résoudre

de manière à obtenir



Lorsque l'on valide ensuite l'assistant, après rafraîchissement de notre serveur DNS on obtient



Désormais, à ce niveau, on ne tient plus compte de ce qui se trouve dans la zone enfant, celle-ci étant gérée sur un autre serveur DNS (pour nous ici S4), on ne fait que renvoyer les demandes de résolution. On dit que notre serveur **ne fait plus autorité pour cette zone**...



Installation du serveur DNS enfant :

Sur le serveur CD de la zone enfant, (pour nous S4), il faut donc installer un serveur DNS **faisant autorité** pour la zone enfant...

• L'installation d'un serveur DNS est classique, et la création d'une nouvelle zone aussi

Arbre		
P, DNS ⊡… 📑 S4		🤃
Zones de recherche directes		
🗄 💼 Zones de recherche inversé	Nouvelle	e zone

on demande de créer une **zone principale**, en spécifiant bien son nom complet...(pour nous **enfant.dom1.com**)

Assistant Nouvelle zone	×
Nom de la zone Quel nom voulez-vous donner à la nouvelle zone ?	
Entrez le nom de la zone (par exemple, ''exemple.microsoft.com.'') :	
Nom : enfant.dom1.com	

le reste se valide avec les options par défaut classiques.

 La zone étant crée, il va falloir lui autoriser les mises à jour dynamique, et l'intégrée à Active Directory...

Arbre	
DNS 54 54 54 54 54 54 54 54 54 54	Nom de fichier zone : enfant.dom1.com.dns
	jour dynamiques ?

• Il faut ensuite modifier le serveur s4 pour qu'il se référence lui-même comme étant son propre serveur DNS...(adresse IP DNS...)

A l'heure actuelle, notre serveur DNS va prendre en charge tous les enregistrement de la zone enfant, mais il ignore tout de la zone parent...

 Il faut ensuite indiquer au serveur DNS enfant l'adresse du serveur DNS parent comme redirecteur à utiliser...

Propriétés de 54		? ×	1			
Indications de racine Interfaces	Enregistrement An Redirecteurs	alyse Sécurité Avancé		ll faut	donner	ici
Les redirecteurs aident à n'a pas répondu.	résoudre les requêtes DNS a s	uxquelles ce serveur		l'adresse DNS de parent, p	du serv e la za pour nou	veur one s S1
Pour ajouter un redire Ajouter. Adresse IP : 192 .168 .1 .30	cteur, entrez son adresse IP, Ajouter	puis cliquez sur				

puis redémarrer...





test des zones DNS parent et enfant :

Si on se résume,

On a un **domaine parent**, nommé **dom1.com**.

le serveur DNS installé sur une machine nommée S1 d'adresse 192.168.1.30 a une zone principale intégrée à active directory

Sur cette zone on a une délégation pour une zone nommé **enfant**

on a un **domaine enfant**, nommé **enfant.dom1.com.**

le serveur DNS installé sur une machine nommée S4 d'adresse 192.168.1.34 a une zone principale intégrée à active directory

Sur ce serveur on a des redirecteurs actifs, pointant vers le serveur DNS parent en 192.168.1.30

Tests sur la zone parent

On peut déjà tester le fonctionnement du serveur DNS via l'onglet Analyse...



Propriétés de S1

Puis on va utiliser nslookup

la résolution de S1 sur lui-même devrait donner

> s1 s1 Serveur : s1.dom1.com Addresses: 192.168.3.1, 192.168.1.30 Nom : s1.dom1.com Addresses: 192.168.3.1, 192.168.1.30

la résolution de S2 (autre machine du domaine dom1.com) devrait donner

> s2 s1 Serveur : Addresses:	s1.dom1.com 192.168.3.1,	192.168.1.30
Nom : s Address: :	2.dom1.com 192.168.1.32	







Arbre	
₽ , DNS ∃ : □(51 → Canes de recherche directe: → Canes → Canes

Arbre
DNS 54 - Diversity State - Di

? ×

par contre il est normal que si on tente de résoudre S4 l'on ait ...



il faut tester S4.enfant ou S4.enfant.dom1.com (en spécifiant le domaine)

> s4.enfant s1 Serveur : s1.dom1.com Addresses: 192.168.3.1, 192.168.1.30	On d
R'ponse ne faisant pas autorit'ÿ: Nom : s4.enfant.dom1.com Address: 192.168.1.34	auqu

On a cette info depuis un serveur auquel on a délégué...

Tests sur la zone enfant

On peut tester le fonctionnement du serveur DNS via l'onglet Analyse...

Puis on peut utiliser nslookup

la résolution de S4 sur lui-même devrait donner

> s4 s4 Serveur : s4.enfant.dom1.com Address: 192.168.1.34	
Nom : s4.enfant.dom1.com Address: 192.168.1.34	

par contre il est normal que si on tente de résoudre **S2** (une machine du domaine parent) l'on ait tout de suite la réponse. (on utilise un système de redirection pour tout appel non résolu...)

> s2 s4 Serveur : s4.enfant.dom1.com Address: 192.168.1.34
R'ponse ne faisant pas autorit'ÿ: Nom : s2.dom1.com Address: 192.168.1.32



CREATION D'UN DOMAINE DANS LA FORET

Création du C.D. "dans la forêt dom2.com" sur serveur S5:

Il faut bien sûr que l'on ait de la connectivité IP et que l'on ait comme adresse de serveur DNS un serveur DNS du domaine voisin...

Lors de l'assistant DC promo, on réponds alors ainsi :

ssistant Inst	tallation de Active Directory	×
Créer une Vous p	arborescence ou un domaine enfant ouvez créer une nouvelle arborescence de domaine ou un nouveau domaine enfant.	
Voulez- enfant (vous créer une nouvelle arborescence de domaine ou un nouveau domaine dans une arborescence de domaine existante ?	
Créi	er une nouvelle arborescence de domaine	
Si v séle sép	vous ne voulez pas que le nouveau domaine soit enfant d'un domaine existant, ectionnez cette option. Cela créera une nouvelle arborescence de domaine arée de toute arborescence existante.	
Vou forê	us pourrez alors choisir de placer la nouvelle arborescence de domaine dans une it existante, ou de créer une nouvelle forêt.	
O Cré	er un nouveau domaine enfant dans une arborescence de domaine existante	
Si v séle app mor	vous voulez que le nouveau domaine soit enfant d'un domaine existant, actionnez cette option. Par exemple, vous pourriez créer un nouveau domaine velé siege exemple microsoft.com qui serait un enfant du domaine nentreprise.com.	
ssistant Inst	tallation de Active Directory	×
Créer ou r Spécifie	ejoindre une forêt ez l'emplacement du nouveau domaine.	
Voulez-	vous créer une nouvelle forêt ou rejoindre une forêt existante ?	
O Cré	er une nouvelle forêt d'arborescences de domaines	
Sélé si vi com	ectionnez cette option si ceci est le premier domaine dans votre organisation ou ous voulez que la nouvelle arborescence de domaine que vous créez soit nplètement indépendante de votre forêt actuelle.	
Place	cer cette nouvelle arborescence de domaine dans une forêt existante	
Sélé arbo dom	ectionnez cette option si vous voulez que les utilisateurs dans la nouvelle orescence de domaine aient accès aux ressources des arborescences de naine existantes, et vice versa.	

Evidemment il faut connaître un compte d'administrateur du domaine racine de la forêt

Assistant Installation de	Active Directory	x
Informations d'identi Fournissez un nom o	fication réseau l'utilisateur réseau et un mot de passe.	
Entrez le nom d'utilis que vous souhaitez	ateur, le mot de passe et le domaine d'utilisateur du compte réseau utiliser pour cette opération.	
Nom d'utilisateur :	administrateur	
Mot de passe :	NHNH	
Domaine :	dom1.com	





Windows NT 2000 travaux pratiques Cabaré Michel C.U.E.F.A. S4 T.P. v1.4

Nouvelle arb Spécifiez l'	prescence de domaine Implacement et le nom de la nouvelle arborescence de domaine.	A.
Entrez le no	m DNS complet de la nouvelle arborescence :	
dom2.com		
Le nom DN siege.exem	S du nouveau domaine doit être un nom DNS complet, tel que ole:microsoft.com.	
	tion de Astive Diverteur.	

ous avez choisi de : `onfigurer ce serveur en tant que premier contrôleur de domaine d'une nouvelle		
rborngarer de servour en rain que prenner connoieur de dontaine d'une nouveile rborescence de domaines.	Ē	
e nom du nouveau domaine est "dom2.com"		
e nom NetBIOS du domaine est "DOM2"		
e nouveau domaine a un lien de confiance avec le domaine "dom1.com"		
implacement de la base de données : C:\WIN2000\NTDS implacement du fichier journal : C:\WIN2000\NTDS implacement du dossier Sysvol :C:\WIN2000\SYSVDL		
	-	

le reste est tout à fait standard...

la création du domaine dans la même forêt se fait de manière automatique,

- ce serveur devient CD
- et les relations d'approbations entre les deux domaines de la forêt sont automatiquement construites., à savoir :
 - o le domaine racine approuve le domaine parent
 - o le domaine parent approuve le domaine enfant
- le serveur ayant le rôle de contrôleur de schéma et de Maître d'attribution de nom de domaine est "dupliqué" sur le nouveau CD du nouveau domaine (mais l'original reste sur le CD d'origine...)

Vérifions les relations d'approbation :

Depuis un CD du domaine racine, on peut voir

on peut vérifier dans outils d'administration / Domaines et approbations active directory

Comaines et approbations Active Directory					
Action Affichage ← → mm mm mm	" 🗗 🖧 😰				
Arbre	Nom	Туре			
Comaines et approbations Active Directory	🗊 dom2.com	domainDNS			
dom2.com	🗊 dom1.com	domainDNS			
dom1.com					


SI on demande les propriétés de dom1.com

omanioo approar	és par ce domaine :		Ce domaine : dom1.com
Nom de domaine	Relation	Transiti	
Jom2.com	Racine d'arborescence	Oui Ajouter	Autre domaine : dom2.com
		Modifier	Type d'approbation : Racine d'arborescence
		Supprimer	Direction de l'approbation :
omaines qui appro Nom de domaine	ouvent ce domaine : Relation		l'autre domaine et les utilisateurs de l'autre domaine peuvent s'authentif dans ce domaine. Transitivité de l'approbation :
lom2.com	Racine d'arborescence	Ajouter	Cette relation d'approbation est transitive. Les utilisateurs de domaines approuvés indirectement au sein de l'entreprise peuvent s'authentifier auprès du domaine qui approuve.
			Pour vérifier et, le cas échéant, réinitialiser cette relation d'approbation, cliquez sur Vérifier.

Localisation des maîtres d'opération :

On se trouve dans le cas où on a une forêt à 2 domaines, par conséquent

- les 2 rôles Contrôleur de schéma et Maître d'attribution de nom de domaine doivent <u>être restés sur le 1° CD du domaine</u> (serveur \$1) racine de la forêt dom1.com
- les 3 rôles Emulateur CPD, RID et maître d'infrastructure pour le domaine dom1.com <u>n'ont pas bougé</u> du serveur 1° CD du domaine (serveur S1)
- les 3 rôles **Emulateur CPD**, **RID** et **maître d'infrastructure** ont <u>étés crées</u> sur le 1° CD du domaine (**serveur \$5**) qui a rejoint la forêt...

Vérifions :

le rôle **Contrôleur de schéma** <u>depuis le CD sur S5 (par exemple)</u> pour le nouveau domaine rallié dans la forêt, on exécute la mmc **Schéma Active directory**

/● /í而 Console1	Changer le contrôleur de schéma	? X
🗍 Console Fenêtre ? 🗍 🗋 🚔 🔚 💷	Traitement en cours :	
🖮 Racine de la console	s1.dom1.com	_
Action Affichage Eavoris ← → Im Im Im Arbre Favoris Nom Racine de la console ■© Schéma Active Directory □ g Schéma Active Directory	Maître d'opérations actuel Le contrôleur de schéma gère les modifications du schéma. Seul un serveur de l'entreprise peut jouer ce rôle.	
Changer de controleur de domaine Changer de controleur de domaine Maître d'opérations	Le serveur est actuellement en ligne	
	s1.dom1.com	

on constate qu'il est toujours sur **S1**

(et pour le transférer il faut appartenir au groupe maître de schéma)



le rôle Maître d'attribution <u>depuis le CD sur S5 (par exemple)</u> on exécute la mmc Domaine et approbation Active Directory

Commaines et approbations Active Directory	
\underline{A} ction Affichage $\underline{A} \leftarrow \rightarrow \underline{B}$ \underline{B} \underline{B}	
Arbre Nom Image: Second constraints Image: Second constraints Image: Second constraints Image: Second constraints	aine
on constate qu'il est toujours sur S1	Modifier le maître d'opérations ? × Le maître des opérations d'attribution de noms de domaine vérifie que les noms de domaines sont uniques. Seul le contrôleur de domaine dans l'entreprise prend ce rôle en charge. Maître des opérations d'attribution de noms de domaine : Maître des opérations d'attribution de noms de domaine : \$1.dom1.com
(on pourrait le transférer)	Pour transférer le rôle de maître d'attribution de noms de Modifier domaine à l'ordinateur suivant, cliquez sur Modifier. s5.dom2.com Fermer

les 3 rôles **Emulateur CPD**, **RID** et **maître d'infrastructure** pour le domaine **dom2.com** on exécute <u>depuis le CD sur S5</u> la mmc **Utilisateur et ordinateur Active Directory**

🐗 Utilisateurs et ordinateurs Active Directory		
] 🧔 <u>C</u> onsole <u>F</u> enêtre <u>?</u>	Maître d'opérations	Maître d'opérations
Action Affichage ↓ ↔ ↓ ▲rbre	RID CDP Infrastructure Le maître d'opérations gère l'allocation des pools	RID CDP Infrastructure Le maître d'opérations émule les
Utilisateurs et ordinateurs Active Directory [s5.dom2.com] Délégation de contrôle Rechercher Se connecter au domaine Se connecter au constrôleur de demaine	controleurs de domaine. Un seul serveur du dom Maître d'opérations : s5.dom2.com	principal pour les clients fonction Windows 2000. Un seul serveur Maître d'opérations : s5.dom2.com
Maîtres d'opérations	Pour transférer le rôle de Maître d'opérations à l'ordinateur suivant, cliquez sur Modifier. s5.dom2.com	Pour transférer le rôle de Maître (l'ordinateur suivant, cliquez sur M s5.dom2.com
on constate qu'ils sont crées sur S5		

les 3 rôles **Emulateur CPD**, **RID** et **maître d'infrastructure** pour le domaine **dom1.com** on exécute <u>depuis le CD sur S1</u> la mmc **Utilisateur et ordinateur Active Directory**



R N



Windows NT 2000 travaux pratiques Cabaré Michel C.U.E.F.A. S4 T.P. v1.4

Page 110

L'UTILITAIRE DCDIAG

Récupération de l'utilitaire dcdiag :

On récupère cet utilitaire dans un fichier

Gudiag_setup.exe 188 Ko Application

puis on l'installe en l'auto-décompressant, ce qui amène un éxécutable et une notice d'installation ...

Nom 🛆	Taille	Туре
dcdiag.exe	213 Ko	Application
🗒 dcdiag_license.txt	13 Ko	Texte seulement
🚰 dcdiag_setup.exe	188 Ko	Application
SupportToolDownloadReadme.htm	7 Ko	Microsoft HTML Doc

Quelques test possibles :

Voici quelques test possibles à imaginer avec cet utilitaire...

Création du premier Contrôleur de domaine dans une nouvelle forêt Active Directory

dcdiag /test:dcpromo /dnsdomain:example.microsoft.com /newforest



Test de l'enregistrement DNS dynamique

dcdiag /test:registerindns /dnsdomain:example.microsoft.com





Ajout d'un contrôleur de domaine supplémentaire à un domaine existant (réplique du contrôleur de domaine)

dcdiag /test:dcpromo /dnsdomain:example.microsoft.com /replicadc



Ajout d'un domaine enfant à un arbre dans une forêt Active Directory existante

dcdiag /test:dcpromo /dnsdomain:test.example.microsoft.com /childdomain

Ajout d'un nouvel arbre de domaine à une forêt Active Directory existante

dcdiag /test:dcpromo /dnsdomain:test.example.microsoft.com /newtree forestroot:example.microsoft.com

C:\test>dcdiag /test:dcpromo /dnsdomain:dom2.com /newtree /forestroot:dom1.com Starting test: DcPromo The DNS configuration is sufficient to allow this computer to be promoted as the first DC in the dom2.com Active Directory domain.
Messages logged below this line indicate whether this domain controller will be able to dynamically register DNS records required for the location of this DC by other devices on the network. If any misconfiguration is detected, it might prevent dynamic DNS registration of some records, but does not prevent successful completion of the Active Directory Installation Wizard. However, we recommend fixing the reported problems now, unless you plan to manually update the DNS database.
This domain controller cannot register domain controller Locator DNS records. This is because it cannot locate a DNS server authoritative for the zone dom2.com. This is due to one of the following:





INSTALLATION MUETTE DEPUIS CD

Objectifs et fonctionnalités :

On veut réaliser une installation de Windows NT 2000 Professionnel à l'aide du CD mais sans que aucune question ne se pose à "l'installateur".

On va par conséquent créer un fichier winnt.sif et winnt.bat via le programme Setup manager wizard

On l'exécutera ensuite par le biais de winnt.bat

Il faut qu'aucune question ne se pose lors de l'installation, et que la configuration donnée au final à notre poste Nt2000 soit la suivante :

•	personnalisation au nom de :	cabaré – tormation
•	nom machine :	postentauto
•	mot de passe de l'administrateur :	zk29
•	paramètres TCP-IP par défaut :	(client DHCP +, rés microsoft)
•	connexion Groupe de Travail :	Formation
•	heure :	Greenwich

Serait il difficile de laisser en libre saisie uniquement le nom machine ?

Réponse :

Le mode Masquer les pages convient







en prenant soin de ne pas renseigner la boite de dialogue Noms des ordinateurs lors de la création du fichier winnt.sif

Assistant Gestion d'installation Windows 2000	×
Noms des ordinateurs Assigner un nom à chaque ordinateur de destination.	
Entrez le nom de chaque ordinateur de destination, puis cliquez sur Aj	outer.
Pour importer les noms d'ordinateurs à partir d'un fichier texte (1 nom d ligne), cliquez sur Importer.	'ordinateur par
Nom de l'ordinateur :	
	Ajouter
Ordinateurs à installer :	
	Importer
	Supprimer
Créer automatiquement les noms d'ordinateurs en utilisant le nom d	l'organisation

Attention à bien indiquer le bon nom de fichier

🔍 As	sistant Gestion d'installation Windows 2000
N	om du fichier de réponse Le fichier de destination est sauvegardé sous le nom et l'emplacement que vous avez spécifiés.
	L'Assistant Gestion de configuration a créé un fichier de réponse avec les paramètres que vous avez fournis. Entrez un emplacement et un nom pour ce fichier de réponse.
	Emplacement et nom de fichier :
	A:\winnt.sif Parcourir
	Si plusieurs noms d'ordinateur ont été spécifiés, l'Assistant crée un fichier .udf. Selon le type de fichier de réponse créé, l'Assistant peut aussi créer un exemple de fichier .bat.
	Si le fichier de réponse est destiné à être utilisé pour effectuer une installation sans assistance en démarrant directement à partir du CD-ROM de Windows, le fichier doit être nommé winnt.sif et être placé sur une disquette.

Et à vérifier dans winnt.bat le chemin du CD sur la machine de destination...

	🔊 winnt.bat - Bloc-notes	
	Fichier Edition Format ?	
	\$et AnswerFile=.\winnt.sif set SetupFiles=H:\i386	
→	H:\i386\winnt32 /s:%SetupFiles% /unattend:%AnswerFile%	

