NETWARE de NOVELL

<u>1 GENERALITES</u>

Netware est un N.O.S (*Network Operating System*) particulièrement bien implanté dans le domaine des serveurs Bureautique.

1.1 Versions :

Netware 2.2 : 5..100 utilisateurs, PC-286-2,5Mo min., arrêt en juin 94
Netware 3 : 5..250 utilisateurs, PC-386-4Mo min.
Netware 3.11, Netware 3.12 (trame 802.2)
Netware 4 : 5..x000 utilisateurs, PC-386-8Mo min., annuaire NDS
Netware 4.11 : idem + serveur Web
Netware 5 : 5..x000 utilisateurs, Gestion des domaines NT, TCP/IP natif

<u>1.2</u> Particularités de Netware 4 sur Netware 3 :

Sur Netware 4.x les divers objets du réseau (serveurs, utilisateurs, groupes, imprimantes ...) sont tous regroupés dans un <u>annuaire</u> arborescent de type X500 appelé **NDS** (*Netware Directory Service*). Cet annuaire peut être mondial et présent sur plusieurs serveurs (mise à jour automatique), le réseau est organisé *logiquement*. Un utilisateur pourra donc se connecter sur n'importe quel serveur, la définition de son « profil » étant unique.

Netware 3.x est orienté « serveur de fichiers », la définition des comptes utilisateurs est enregistrée dans une base de donnée (« *Bindery »*) propre à chaque serveur.

<u>droits sur les objets :</u>

Aux droits et attributs sur les fichiers et répertoires (similaires à Netware 3) s'ajoutent des **droits sur les objets** de la NDS. Les droits sur un objet définissent ce qu'un ayant droit peut faire et les droits de propriétés contrôlent l'accès des ayants droits aux informations de l'objet.

Il devient simple de créer par exemple un compte administrateur d'un conteneur permettant de sous-traiter l'administration de certaines branches...

<u>1.3</u> Structure de la NDS :

NDS : Netware Directory Service, Service d'annuaires Netware.

Arborescence : L'annuaire est arborescent avec 3 niveaux importants :

- *[root]* : Racine, c'est le sommet de la hiérarchie (icône = terre !).
- *Conteneurs* : Branches organisationnelles avec 3 types possibles : pays (optionnel), Organisation (au moins une), Unité organisationnelle (subdivisions).
- *Feuilles* : Divers objets du réseau.



Objets feuilles : Ressources du réseau :

- Utilisateur : Compte définissant les droits et propriétés d'un utilisateur.
- : Liste d'utilisateurs. • Groupe
- Serveur
- : Machine fournissant des ressources. • Volume : Espace disque.
- Imprimante : Imprimante (machine)
-



<u>1.4</u> Connexion d'une station :

Pour se connecter à un serveur Novell Netware 4, une station doit posséder une carte réseau avec ses « drivers » et une pile de protocoles IPX/SPX (ou TCP/IP pour Netware 5 et certains serveurs Netware 4).

Pour une station DOS on utilisera la même configuration que pour un serveur Netware 3.x. La commande « cx » permettra de préciser le contexte désiré.

Pour les stations Windows 95/98 ou NT on pourra utiliser les connexions « Microsoft » (voisinage réseau...) mais il est plus simple d'utiliser les clients Netware pour Windows (client 32 bits pour W95, client 2.5 pour NT..) qui offrent des fonctionnalités supplémentaires.

Un poste de travail sous NT-Workstation nécessite un « logon » local. Il est possible de synchroniser le « login » de Netware et le « logon » NT d'un utilisateur afin de rendre unique la procédure de connexion.

1.5 Volumes en réseau :

Sur un serveur Netware, la mémoire de masse est divisée en volumes (un disque peut être divisé en plusieurs volumes de même que plusieurs disques peuvent être assemblés en un seul volume). Les volumes sont désignés par un **nom**. Le volume SYS: est définit par défaut.

La syntaxe de désignation d'un fichier est : *Serveur**volume:répertoire*\...*fichier*

exemple : JUPITER\DATA:MRBT\DUPOND\TOTO.TXT

La commande CD permet d'affecter un volume au lecteur courant : CD APPLY:

La commande MAP affecte un nouveau lecteur : MAP G:=APPLY:

Avec « Netware tools » (client windows), choisir l'icône disque puis faire glisser le disque « ressource » voulu vers la lettre « drives » désirée...

<u>1.6</u> Utilitaires principaux :

NWADMIN : Administrateur graphique pour la création, modification, ajout d'objets (utilisateurs, groupes...). (*nwadmn3x.exe dans le volume SYS:PUBLIC*)
 PCONSOLE : Définition des imprimantes...

SYSCON, FILER... hérités de Netware 3 sont toujours fonctionnels.

TD : Parcours de la NDS existante

L'arborescence de l'annuaire permet une administration distribuée simplement. La notation est pointée avec niveau le plus élevé à droite : **admin.BALCON.MRBT.IO**

Le serveur de TP s'appelle « JUPITER », la racine de l'arbre a été appelée « IO » (satellite de Jupiter !), MRBT est un conteneur (Unité Organisationnelle), BALCON est un conteneur créé pour chaque élève de la classe, admin est un utilisateur du conteneur possédant tous les droits sur ce niveau.

TRAVAIL :

- Connectez-vous sur votre compte « admin » en n'oubliant pas de préciser votre contexte (.BACON.MRBT.IO par exemple).
- Lancez l'utilitaire « **NWADMIN** » (sur SYS:PUBLIC)
- Remontez au niveau le plus haut de l'arbre et notez les objets visibles. *Remarque : si vous n'avez pas accès directement à l'arbre « TREE_JUP » du TP, faire un clic-D sur le N rouge de la barre de tâche puis « connexion Netware » et définir TREE_JUP comme principale.*
- Modifiez le mot de passe du compte **admin** de votre conteneur.
- Donnez la liste des droits de ce compte...

Administrateur NetWare			
	× 🖞 📰 📼 📢 I	▶ # # #	
Image: Construction of the system Image: Construction of the system		[Root] (TREE_JUP)	
Arborescence :TREE_JUP	Admin.10	Sélectionné : 1	Subordonnés : 2
🔀 Démarrer 🛛 🗾 S3 VManager	Administrateur NetWare		3 14:49

L'environnement précise l'adresse de connexion en cours de l'utilisateur visualisé (on remarquera l'adresse MAC incluse dans l'adresse IPX) et le répertoire privé de l'utilisateur.

🔣 Utilisateur : adm	in		×
Environnement			
Langue : Adresse de	Francais		Environnement
réseau :	JIPX: 361BFD37:0000E822574B:4088		
Serveur par défaut :	JUPITER.IO	語	Restrictions de login
Répertoire privé :			Restrictions de mot de passe
⊻olume :	DATA.BALCON.MRBT.IO	12-	Restrictions des heures de
C <u>h</u> emin d'accès :	MRBT\BALCON		
			Restriction d'adresse de réseau
			Configuration des travaux d'impression
			Script de login
			Verrouillage en cas d'intrus
			Droits sur des fichiers et
OK Anr	uler Options de page	Aide	

2002

📴 Utilisateur : admin	×	🔜 Utilisateur : admin	×
Restrictions de login	Identification Environnement Restrictions de login Restrictions de mot de passe Restrictions des mot de login Restrictions des heures de login Restriction d'adresse de réseau Configuration des travaux d'impression Script de login Verrouillage en cas d'intrus Droits sur des fichiers et des rénertories et	Restrictions de mot de passe	Identification Environnement Restrictions de login Restrictions des mot de passe Restrictions des heures de login Restriction d'adresse de réseau Configuration des travaux d'impression Script de login Verrouillage en cas d'intrus Droits sur des fichiers et des répertoires
OK Annuler Options de page Aide		OK Annuler Options de page Aide	

Par sécurité on peut désactiver le compte, le limiter dans le temps ou dans le nombre de connexions simultanées. On observera la date de la dernière connexion... Les restrictions du mot de passe peuvent être individualisées.

Limitation de l'espace utilisable sur un volume par un utilisateur :

Par sécurité, on pourra limiter l'espace d'un utilisateur sur un volume (choix du volume, détails, limite d'espace, choix du contexte à parcourir, choix de l'utilisateur et onglet modifier...). Attention : cette limitation concerne un <u>utilisateur</u> quelque soit les sous-répertoires utilisés sur le volume, à ne pas confondre avec la limitation de la taille d'un répertoire qui est liée au <u>répertoire</u> quelque soit l'utilisateur qui y écrit !

📴 Volume : JUPITER_D	ATA				X
Limites d'espace utilisateur				[Identification
MRBT.IO	MRBT.IO			睛	Statistiques
Rechercher dans toute	l'arborescen	ce secondaire	b		Dates et heures
Nom de l'utilisateur	Limite	Espace utilisé	Espace disp	<u> </u>	
admin.AUBLIN.MRB	10000 Ko	4 Ko	9996 Ko		Limites d'espace utilisateur
admin.BALCON.MRI	10000 Ko	0 Ko	10000 Ko		Avants-droit du rép racine
🔺 admin.BOUDINOT.N	Illimité	4 Ko	196608 Ko		
a limitation d'es	l	l			Attributs
Utilisateur :	admin.BO	UDINOT.MRBT	.10		Voir aussi
Espace du volu	ime utilisé :	4 Ko			
📃 💆 🔽 Espace du v	/olume_limité				
Limite d'esp volume (Ko)	ace du :	10000		ЕI	
	OK	Annuler	Ajde	F-	
OK Annuler	Option	ns de page	Aide	-	

Création d'un administrateur de conteneur (à titre indicatif) :

Afin de sécuriser l'annuaire du serveur, on a créé un conteneur pour chaque élève avec un compte **admin** ayant tous les droits sur ce conteneur mais ne pouvant voir les autres conteneurs élèves. Un groupe **adminmrbt** définira les droits communs. A titre indicatif, voici la procédure suivie :

Procédure :

- Dans le conteneur MRBT : objet, créer, Unité org. ... (BALCON par exemple).
- Dans le conteneur BALCON, créer un utilisateur admin ...
- Sur BALCON, « ayant droits », ajouter l'admin créé avec tous les droits.
- Pour rendre le conteneur invisible aux autres : sur BALCON, « ayant droits », filtre de droits hérités, supprimer « parcourir » (par défaut, la visualisation peut se faire par héritage de [public] qui peut parcourir la racine de l'arbre).
- Donner les droits nécessaires aux répertoires : choisir le répertoire, « ayant droits », ajouter l'utilisateur..., donner les droits voulus (il faut posséder le droit de supervision pour pouvoir limiter la taille d'un sous-répertoire utilisateur).

TD : CREATION D'UN UTILISATEUR

TRAVAIL :

- Connectez-vous en administrateur dans votre Unité Organisationnelle.
- Créez un utilisateur (nom de compte dans un thème précisé lors du TP)
- Complétez les différents champs d'identification.
- Déclarez votre appartenance au groupe « MRBT » (par exemple).
- Créez un répertoire à votre nom de *login* dans **DATA:MRBT** (tests ultérieurs).
- Limitez l'espace sur le volume DATA à 1000ko.
- Connectez-vous sur votre compte,
 - Créez un petit fichier texte dans votre répertoire personnel.
 - Pouvez vous vérifier vos droits ?
 - Quels renseignements pouvez vous obtenir sur les autres comptes ?
 - A quels groupes appartenez-vous ?
 - Quels sont les droits de ces groupes ?
- Restrictions des connexions :
 - Comment limiter l'espace utilisable sur un volume réseau ?
 - Comment limiter les jours/heures de connexion d'un compte ?
 - Comment limiter dans le temps la connexion (jusqu'au 30 juin par ex.) ?
 - Comment restreindre la connexion d'un compte à une seule connexion simultanée ?
 - Comment obliger la connexion d'un compte à une station particulière ?

2002

2 REPERTOIRES ET FICHIERS

2.1 Droits sur les répertoires et fichiers :

Les **droits** (*« trustees »*) sur les répertoires et fichiers sont attribués à des **utilisateurs** ou des **groupes**. Lors du *login* l'utilisateur s'identifie (LOGIN_NAME) et le serveur connaît ses droits, il peut par son appartenance à certains groupes **hériter** de droits supplémentaires. Les outils permettant d'afficher ou modifier les droits sont : Nwadmin, SYSCON, FILER, RIGHTS, TLIST, GRANT ou même l'explorer de Windows.

Pour simplifier la gestion on donnera d'abord des droits aux Unités Organisationnelles (conteneurs) ou aux groupes. Par défaut (pas de filtrage posé), les droits d'un utilisateur sur une branche se propagent sur tous ses rameaux !

<u>Attention</u>: les droits accordés à [**Public**] sont attribués à tout utilisateur connecté au réseau et par forcément identifié (login) !

📴 Utilisateur : LESCOP	×			
Droits sur des fichiers et des répertoires				
⊻olumes :	Environnement			
CAMILLE_APPLI.ELECTRONIQUE	Restrictions de login			
	Montrer			
	<u>C</u> acher passe			
Fichiers et répertoires :	Restrictions des heures de			
Type Nom du volume Nom de répertoire ou 📥	Ajouter Bestriction d'adresse de			
CAMILLE_APPL \POST\ALCATEL	Supprimer réseau			
	Charin discrimination des travaux			
CAMILLE_DATA \PROFS\LESCOP	Lhemin d'acces			
	Script de login			
	Verrouillage en cas d'intrus			
J Superviseur J Creer J Ana	lyse de fichiers			
I IV Lire IV Effacer IV Con	trôle d'accès Droits sur des fichiers et des répertoires			
IV Ecrire IV Modifier Dro	its effectifs			
Adhesion au groupe				
OK Annuler Options de page	Aide			

2.1.1 Liste des droits : [SRWCEMFA]

S	Superviseur	Supervisor	peut accorder tous types de droits aux autres (non filtrable).	
R	Lire	Read	ouverture et lecture ou exécution.	
W	Ecrire	Write	ouverture et écriture.	
С	Créer	Create	création de sous-répertoires ou fichiers.	
Е	Effacer	Erase	effacer.	
Μ	Modifier	Modify	modifier les noms ou les attributs.	
F	Analyse de fichiers	File scan	lister les fichiers/répertoires (DIR).	
Α	Contrôle d'accès	Access control	modification du masque d'héritage et des ayants droits.	
[-RF-] droits minimums,				
[-RWCEMF-] droits du propriétaire d'un répertoire. (S et A non accordés par défaut)				

🔣 Directory: BOUDINOT	×	File: JUPITER/DATA:\MRBT\COURS\TPNOV4A.DOC	×
Informations		Informations	
Ko disponibles pour ce répertoire : 992	Identification	Taille : 12288 octets	itification
☑ <u>R</u> estreindre la taille	Informations	Créé : 23 /03 /98 08 : 29 : 10	rmations
Limite : 1024 Ko	Ayants-droit du répertoire	Propriétaire : Admin.10	roits du fichier
(Entrez la quantite par increments de 32 No.)	Attributs	Dernière 21 /03 /98	ttributs
<u>C</u> réé : 13 /03 /00 16 : 47 : 12		Modi <u>f</u> icateur: Admin.IO	
Propriétaire : admin.BOUDINOT.MRBT.IO			
Dernière modification : 27 /03 /00 ♥ 11 :47 :18 ♥		Dernier / / 🗮 :: 🗮	
Dernier / / 🛓 ::		Archiviste :	
Archiviste :			
OK Annuler Options de page Aide		OK Annuler Options de page Aide	

Les informations sur un répertoire permettent de préciser une limitation de taille éventuelle, le propriétaire... Celles sur un fichier précisent le propriétaire et le dernier modificateur du fichier !

📴 Directory: BOUDINOT	×		
Ayants-droit du répertoire Ayants-droit : ▲ admin.BOUDINOT.MRBT.IO BOUDINOT.MRBT.IO Ajouter Supprimer Droits d'accès Superviseur Lire Ecrire Créer Effacer Modifier Analyse de fichiers Contrôle d'accès	Identification Informations Ayants-droit du répertoire Attributs	Droits effectifs <u>A</u> vant-droit : adminmrbt.MRBT.II Droits effectifs Superviseur Lire Ecrire Créer	C Effacer Modifier Analyse de fichiers Contrôle d'accès Eermer <u>Ai</u> de

L'onglet « ayants droit » permet d'afficher la liste des objets désignés explicitement comme ayant des pouvoirs sur le répertoire/fichier désigné. D'autres utilisateurs peuvent <u>hériter</u> de droits sur ce répertoire en possédant des droits sur un niveau supérieur de l'arbre. A l'aide de l'onglet « droits effectifs » on peut vérifier les droits d'un objet que l'on sélectionnera dans la NDS sur le répertoire considéré.

2.1.2 Filtre d'héritage :

Les droits effectifs d'un utilisateur sont déterminés par les droits de l'utilisateur (« *User's trustee* ») auxquels s'ajoutent les éventuels droits du groupe ou hérités d'un embranchement de niveau supérieur, le tout filtré par un masque d'héritage (*IRM : Inherited Rights Mask*).

2002

Pour qu'un utilisateur désigné puisse seul accéder à un sous-répertoire, il faudra filtrer les droits de tous en décochant les cases du filtre d'héritage et nommer explicitement l'utilisateur comme ayant droit de ce sous-répertoire. Le droit de supervision n'est pas filtrable car l'administrateur doit pouvoir rétablir une situation que l'utilisateur aurait détruite accidentellement (via le droit « contrôle d'accès »).

<u>*Remarque*</u> : Si un utilisateur possède des droits sur un fichier éloigné, le chemin pour y parvenir lui sera visible même si « Analyse de fichier » est masqué.

2.2 Attributs des répertoires et fichiers

Les **attributs** (*« flag »*) des répertoires et des fichiers sont attachés aux répertoires et fichiers eux-mêmes. Ils sont prioritaires sur les **droits** (*« trustees »*) des utilisateurs ou groupes. Pour modifier les attributs, l'utilisateur doit posséder le droit [A] (*« contrôle d'accès »*) sur l'objet. Les outils pour afficher ou modifier les attributs sont : Nwadmin, FILER, FLAG, FLAGDIR ou même l'explorer de Windows.

File: JUPITER/DATA:\MRI	BT\COURS\TPNOV4A.DOC	×
Attributs Attributs de fichier Attributs de fichier Archivage souhaité Exécuter seulement Attributs Attributs de fichier Archivage souhaité Exécuter seulement Archivageable Caché Système Transactionnel Purge immédiate Non supprimable Non supprimable	Statut du fichier Fichier compressé Incompressible Fichier migré	Identification Informations Ayants-droits du fichier Attributs
Normenominable Ne pas migrer Compression immédiate Ne pas compresser Ne pas sous-allouer K. Annuler	Options de page Aide	2

Ro/Rw	Lecture seule	Read only/write	lecture seule ou lecture-écriture.
S	Partageable	Shareable	Partageable entre plusieurs utilisateurs.
Α	Archivage souhaité	Archive	Fichier modifié depuis le dernier backup.
X	Exécuter seulement	eXecute only	modification, copie, backup par le superviseur.
Н	Caché	Hidden	caché.
Sy	Système	System	caché, copie et effacement impossible.
Т	Transactionnel	Transactionnal	fichier TTS, (base données) assure que tous les chgts sont effectués.
Р	Purge immédiate	Purge	Destruction si effacé, récupération impossible.
Ra/Wa		Read/Write audit	pour audit (pas utilisé pour l'instant).
Ci		Copy inhibit	copie interdite.
Di	Non supprimable	Delete inhibit	Effacement interdit.
Ri	Non renommable	Rename inhibit	changement de nom interdit.
Dc	Ne pas compresser	Don't compress	Compression interdite.
Dm	Ne pas migrer	Don't migrate	Migration interdite.
Ic	Compression immédiate	Immediate Compress	Compression immédiate.
[Ro S A - H Sy T P Ci Di Ri] Protection max. (All), [Rw] Par défaut (Normal).			

2.2.1 Liste des attributs des	fichiers ·	Ro/Rw SAXHS	v T P Ra/Wa Ci Di Ril
<u>2.2.1</u> Liste des den touts des .			$y \perp \perp \mathbf{M} u / m u \cup D m m$

Remarque : Attribuer Ro ajoute systématiquement Di et Ri et Dc, Dm, Ic n'existent pas sur Netware 3.x

2.2.2 Attributs sur les répertoires :

Les attributs sur les répertoires sont limités à [Sy H P Di Ri Dc Dm Ic].

🔜 Directory: BOUDINOT	×
Attributs Attributs de répertoire Non supprimable Caché Purger	Identification Informations Ayants-droit du répertoire
 Non renommable Système Ne pas migrer Compression immédiate Ne pas compresser 	Attributs
OK Annuler Options de page Aide	

2.2.3 Utilisation de l'explorer de Windows :

Les utilisateurs ordinaires exploiteront le plus souvent l'explorateur de Windows pour rechercher, visualiser et modifier les droits et attributs des répertoires et fichiers.

Propriétés de Boudinot	Propriétés de Boudinot	? ×
Général Dossier NetWare Droits NetWare	Général Dossier NetWare Droits NetWare	
Ayants-droit : RWECMFA	BOUDINOT Novell	
Combiner divers Ayants-droit	Espace nom : DOS Propriétaire : admin.BOUDINOT.MRBT.IO	
EVAL5B EVAL6A B [®] EVAL6A B [®] MRBT Admin evaladmin LESCOP	Date de création : lundi, mars 13, 2000 4:47:12 Dernière mise à jour : lundi, mars 27, 2000 11:47:18 Dernière archive : Jamais archivé	
∠iputer Droits effectifs Lire Effacer Modifier Contrôle d'accès Ecrire Créer Analyse de fichiers Superviseur	Attributs :	9
OK Annuler Appliquer	OK Annuler App	iquer

TD : Droits d'accès sur les répertoires et fichiers

- Donnez la liste des répertoires que vous voyez dans les différents volumes.
- Pour chacun d'eux indiquez les droits que vous possédez et d'où vous les tenez (droits personnels ou héritage d'un groupe).
- Quels sont les droits des autres membres du groupe sur votre répertoire personnel ?
- <u>Modification des droits</u> : Sur le répertoire \MRBT les droits [-RWCEMFA] sont accordés à tous les membres du groupe. Les droits de ces mêmes membres sur votre répertoire (\MRBT\DUPONT par ex.) sont identiques par héritage. Limitez les droits des autres à ce répertoire. Comment pouvez vous le rendre invisible aux autres ?
- Modifier quelques attributs et vérifier la portée des modifications.
- Quelles différences pouvez vous observer sur les modifications de paramètres réalisables par l'explorer Windows et par Nwadmin ?

Sous DOS, les commandes FLAG et FLAGDIR sont parfois plus pratiques. La commande ATTRIB du DOS est reconnue mais ne peut agir que sur les 4 attributs compatibles DOS (ATTRIB -R toto.txt idem FLAG toto.txt +RW).

TD : Création d'une succursale

Objectif : Créer tous les objets nécessaires à une succursale de la société selon un cahier des charges.

<u>Matériel</u>: 1 PC avec connexion Ethernet, 1 serveur novell 4.1x avec une U.O. et son administrateur.

Cahier des charges :

Une société est divisée en 3 structures : Administration, comptabilité et service technique. Chaque personne de la société possède un compte avec un répertoire personnel (privé) qu'eux seuls peuvent utiliser (sauf indication contraire), l'accès aux logiciels de « MSOFFICE » et l'accès sans restrictions à un répertoire commun. Pour chaque structure de la société on a les particularités suivantes :

ADMINISTRATION :

- 1 patron limité, par sécurité, à une seule connexion. Il fait partie du groupe facture.
- 1 secrétaire, elle ne peut se connecter qu'aux heures ouvrables, son répertoire personnel sera limité à 5Mo et elle peut lire le répertoire du « patron ».

COMPTABILITE :

- 1 « rôle organisationnel » chargé d'administrer tous les objets de l'unité « comptabilité » (mini-administrateur).
- 1 groupe facture ayant accès a un répertoire particulier : « facture »
- 4 ou 5 personnes dont 2 font partie du groupe facture et 1 est titulaire du rôle organisationnel. Ils ont tous accès au logiciel « NOTES ».

SERVICE TECHNIQUE :

- 3 techniciens ayant accès au logiciel « PCPLUS ».

TRAVAIL A EFFECTUER :

- Connectez-vous en administrateur dans votre Unité Organisationnelle.
- Créez les répertoires communs dans votre répertoire sur le volume « DATA ».
- Créez une Unité Organisationnelle pour chaque structure, créez les différents comptes (avec répertoire personnel dont vous vérifierez le chemin d'accès) et autres objets Attribuez les droits et limitations ...
- Vérifiez les droits et possibilités des différents utilisateurs en vous connectant sous leur nom.