70-068

Windows NT Enterprise
Support Technique Avancé

ESSENTIEL

PARIS ACADEMY OF COMPUTER SCIENCE
SUPINFO Paris
ECOLE SUPÉRIEURE D'INFORMATIQUE

Ecole Supérieure d'Informatique de Paris
23, rue Château Landon
75010 – PARIS

www.supinfo.com
www.laboratoire-microsoft.org

Caractéristiques

Statut	Interne ✍	Document de travail ✍	Livrable contactuel ✍
Réf. fichier	PC Word 2000 : Support Technique Avancé.doc		

Mise à jour

Ver	Modification
0.9	Version initiale
1.0	Ajouts paramètres audits

Liste de diffusion

Organisme	Nom des destinataires	Nombre	Objet de la diffusion
ESI SUPINFO	LABORATOIRE MICROSOFT	1	Pour validation

Niveau de diffusion : Laboratoire
Confidentialité : Confidentiel Laboratoire

Historique du document

Version	Créé le	Par	Vérifié par	Livré le
0.9	29/12/2000	Ali NEDJIMI	JL. MOUREAUX	01/2001
1.0	17/01/2000	Ali NEDJIMI	JL. MOUREAUX	01/2001

TABLE DES MATIERES

RELATION D'APPROBATION

✍ Points clés

✍Les relations d'approbation ne peuvent se faire qu'entre domaines NT.

✍Elles rendent possible l'accès universel (inter-domaines) : 1 seul compte et un seul mot de passe.

✍Un domaine approuvé = domaine de compte.
Un domaine autorisé à approuver = domaine de ressources.

✍Le domaine autorisé à approuver doit importer les groupes globaux ou les utilisateurs globaux du domaine approuvé dans ses groupes locaux et attribuer des permissions locales aux groupes .

✍Administration distante : le groupe global des administrateurs du domaine (du domaine approuvé) n'est pas ajouté au groupe local des administrateurs. Cependant c'est le cas pour l'ajout d'un ordinateur membre du domaine où le groupe global Administrateur du Domaine est ajouté au groupe local Administrateurs (idem pour le compte Invité).

Authentification de transfert

Il y a **authentification de transfert** lorsque :

- ?? un utilisateur du domaine approuvé ouvre une session depuis le domaine autorisé à approuver.
- ?? on accède à une ressource du domaine autorisé à approuver (en utilisant 'se connecter en tant que').

✍Une relation d'approbation peut être : soit unidirectionnelle, soit bidirectionnelle.

✍Le mot de passe demandé lors de la mise en place (autorisé à approuver) n'est utilisé qu'une seule fois.

✍Il ne doit pas y avoir de '*connecter en tant que*' actif lors de la mise en place d'une relation d'approbation.

✍Une relation d'approbation est non transitive : si A approuve B et B approuve C, A n'approuve pas C pour autant. La transitivité des relations d'approbations apparaît sous Windows 2000.

✍Une relation d'approbation (voir avec l'observateur d'événement et la réinstaller) est rompue quand :

- 1 des domaines est renommé
- le service 'accès réseau' est défectueux
- le lien physique est rompu

✍Seuls les clients NT ont la possibilité de choisir le domaine (approuvé) à l'ouverture de session (depuis le domaine autorisé à approuver).

✍Sur le domaine autorisé à approuver, il est possible de donner accès aux utilisateurs du domaine approuvé en activant le compte invité sans mot de passe (et donc sans importer les comptes du domaine approuvé).

MODELE DE DOMAINE

Il existe quatre stratégies pour les modèles de domaine :

Domaine unique	Si l'on veut privilégier la **simplicité** (pas de relation d'approbation). Si il y a moins de 40 000 utilisateurs, besoin d'une administration centralisée des comptes et des ressources.
Domaine maître unique	Relation d'approbation unidirectionnelle (le nombre de domaine de ressources est supérieur au nombre de domaines de comptes). Utile pour un nombre d'utilisateur pas trop important, **administration des comptes centralisée, administration des ressources décentralisée.** Les groupes globaux sont dans le domaine maître uniquement.
Domaine avec plusieurs maîtres	Si l'on privilégie l'adaptabilité (relation d'approbation bidirectionnelle entre les domaines maîtres). Si le nombre d'utilisateur est important (nombre d'approbations = P*(P-1)+(R*P) où P est le nombre de domaines maîtres et R est le nombre de domaines ressources).
Approbation totale	(relation d'approbation bidirectionnelle) Le nombre d'approbations sera : n*(n-1) où n est le nombre de domaines.

STRUCTURE DU SERVICE D'ANNUAIRE

La limite de la taille de l'annuaire est de **40 Mo** ce qui correspond à plus de **40 000** comptes utilisateurs + ordinateurs.

Taille	Type de compte
1 Ko	Utilisateur
0.5 Ko	Ordinateur
0.5 Ko + 12 o	Utilisateur (en Groupe global)
0.5 Ko + 36 o	Utilisateur (en Groupe local)

Il faut un Contrôleur Secondaire de Domaine pour ***2 000 comptes utilisateurs***.

Taille mémoire recommandée = 3 x taille SAM. Pour 10 000 utilisateurs, cela donne un SAM de 15 Mo, donc, 48 RAM. Ne pas confondre avec la taille du Pagefile minimum qui doit être égale à 4 x la taille du registre.

AUDIT ET ANALYSE DE L'ACTIVITE

Les ressources principales pour l'audit sont : **mémoire**, **processeur**, **sous-système disque**, **sous-système réseau**.

Les outils NT pour l'audit : moniteur réseau, analyseur de performance, gestionnaire de serveur, Diagnostic NT (winmsd).

Les ressources sollicitées par l'environnement serveur :

- de fichiers et impression : mémoire (cache) et processeur (connexion réseau) (pour IIS : augmenter valeur clé MemoryCacheSize (4 Go maxi)),
- d'applications : processeur et mémoire,
- de domaine : mémoire et sous-système réseau.

La mémoire paginée = mémoire virtuelle pour les applications.

Mémoire non paginée = les données ne peuvent pas être écrites sur le disque dur.

1 – Activité client

?? ***DHCP*** (utilisé pour acquisition/renouvellement de bail)

- bail : on peut allonger la durée de bail si beaucoup d'adresses sont disponibles.
- seuil : augmenter (nombre de tentatives, le temps d'attente).

?? ***WINS*** (inscription/renouvellement/conversion/libération). Les clients WINS peuvent être de plusieurs types : W95, NT, W3.11+TCP/IP 32, LanMan Dos

- désactiver services superflus.
- allongement de la durée de vie du cache Netbios (clé CacheTimeOut).
- utiliser LMHOSTS.

?? ***Session de fichier***
(conversion d'adresse MAC (ARP)/session TCP/session Netbios/négociation. SMB/connexion ressource/transfert de données/fermeture session)

- suppression des protocoles non indispensables,
- proximité clients/serveurs.

?? ***Validation d'accès*** (recherche de serveur par diffusion, mailslots Netlogon, valider une demande d'ouverture de session (connexion IPC$), fermeture de session)

- on a besoin d'un BDC pour 2000 comptes, paramètre service serveur : débit maximum pour les applications (plus d'accès simultanés), proximité BDC, taille RAM =2.5 x taille SAM.

2 – Activité Client-Serveur

?? ***Exploration de client*** ((browser)annonce d'hote/12mn, extraire liste exploration de sauvegarde, élection, extraire liste serveurs, extraire liste ressources)

- désactiver le service serveur si il n'y a pas de partage,
- clé **MaintainServerList**,
- clé **BackupPeriodicity (12mn)**,
- éliminer les protocoles superflus.

?? ***DNS*** : appel possible vers autre serveurs DNS ou WINS

- Eviter les appels vers d'autres serveurs DNS ou WINS,
- affectation client du meilleur DNS,
- augmenter le TimeToLive du cache DNS = enregistrement SOA **(60 mn)**,
- augmenter le TimeToLive pour les entrées WINS dans le cache (10 mn).

?? ***Intranet*** (connexion site (TCP)/demande page (HTTP)/sécurité stimulation/réponse (authentification cryptée))

- taille des pages Web,
- réutiliser les graphiques,
- augmenter cache client,
- éviter les authentifications.

3 – Activité entre serveurs

?? ***Synchronisation des comptes***

- diminuer la valeur de la clé **ReplicationGovernor (100 % = 128 Ko)**,
- augmenter la valeur de la clé **ChangeLogSize (64 Ko)**,
- changer la valeur de la clé **PulseConcurrency (10 CSD maj simul.)**, augmenter pulse (5 mn vérification si mise à jour).

?? ***Approbation*** : mise en place/importation de comptes/authentification de transfert

- réduction du nombre d'approbations, utiliser les groupes

?? ***Explorateur de serveur*** : annonce de domaine entre explorateur maître (15 mn), explorateur maître de domaine interroge le serveur WINS pour liste domaines (12 mn), 1 explorateur maître de domaine/domaine = PDC,
clé **MaintainServerList** = 'yes' sur un contrôleur NT.

- o Réduction du nombre de protocoles,
- o Désactiver service serveur si pas de partage,
- o Valeur de la clé **MasterPeriodicity (12 mn)**,
- o Valeur de la clé **BackupPeriodicity (12 mn)**

?? ***Duplication WINS*** : PUSH (envoi quand n mises à jour)/PULL (demande périodique des mises à jour).

- o augmenter notification de duplication poussée quand 20 mises à jour, mise en place période de demande de modification tirée (toutes les 30 mn).

?? ***Duplication de répertoires*** : exportateur = NT Server uniquement, importateur = NT (WKS, Server, Membre) et lan man OS2 server. Cela nécessite la possibilité de résoudre les noms NetBios en IP = client WINS ou LMHOSTS.

- o positionner la clé replicator/parameter **Interval (5mn)** vérifier si il y a des modifications,
- o positionner la clé **Pulse (2 mn)** importateur contacte exportateur. Si il n'y a aucune modification au bout de 2*5 mn,
- o positionner GuardTime (temps de stabilité mini avant duplication), si duplication avec server WINS distant RAS : PULL seulement (sur le poste distant).

?? ***DNS*** : transfert de zone, enregistrement SOA/propriétés de la zone.

- o Intervention (vous pouvez boire des rafraîchissements (60 mn),
- o Intervention avant nouvelle tentative (si échec, 10 mn),
- o heure d'expiration (t-vie DNS secondaire si plus de mise à jour).

ANALYSEUR DE PERFORMANCES

Le nom du programme est **perfmon.exe** en version NT 4 ou Windows 2000. Il dispose de plusieurs modes de travail : modes graphe/journal/alerte. On peut demander à espacer l'échantillonnage afin d'éviter la surcharge du réseau. Il est possible d'enregistrer l'environnement et de l'exporter (.csv, .tsv) vers Excel par exemple pour en faire un graphe.

?? ***compteurs mémoire*** : il indique le nombre de **pages/s (5 maxi ou pic 20)**, cache défaut/s, octets disponibles (4 Mo mini), octets dédiés (taille RAM maxi) octets de réserve non paginée (pas d'augmentation)

- ajout de mémoire,
- recherche processus responsable de la pagination/fuite.

?? ***compteurs processeur*** : il indique le pourcentage de **temps proc. (75 maxi)**, %temps privilégié (75 maxi), temps utilisateur (75 maxi), le nombre **interruptions/s (3500/pentium 90)**, **système/longueur file proc (2 maxi)**, queue de travail du serveur/longueur queue (2 maxi).

- ajout d'un deuxième processeur si serveur est serveur d'application,
- mettre un processeur plus performant si serveur est un serveur de fichiers,
- répartition de charge de traitements.

?? ***compteurs disques*** (activés par diskperf /y ou /ye si RAID) : il indique le **% de temps du disque (50 maxi)**, ainsi que la longueur de la file d'attente (2 maxi). Il indique aussi la moyenne par disque d'octets/transfert (élevée), octets disque/s (élevée).

- contrôleur plus rapide,
- ajout de disque si RAID,
- répartition de charge traitements.

?? ***compteurs réseau*** : pour un serveur : total des octets (élevée), nombre d'ouverture de session/s (élevée), total.

?? ouverture de session (élevée) **segment réseau (ajoutés par l'agent moniteur)** : **%utilisation de réseau (30 maxi) interface réseau (ajoutés pour TCP/IP par service SNMP)** : octets envoyés (élevée), total des octets (élevée).

- ajout de CSD,
- problème de résolution de noms NetBios,
- segmenter le réseau,
- limiter le nombre de protocoles,
- ajout de carte,
- cartes/routeurs plus performants.

?? il existe aussi des compteurs Netbeui,NWlink et TCP/IP

?? il est possible de faire un enregistrement différé des compteurs de Performance Monitor grâce à la commande at..."monitor start/stop".

MONITEUR RESEAU

Il permet de faire des graphes, d'avoir des statistiques par session, par station avec des filtres de capture/affichage, et des statistiques totales. La capture permet d'être affichée en résumé, en détail ou en hexadécimal.

Version NT4 (simple) : le moniteur réseau ne permet que de voir les trames vers et à partir de l'ordinateur local.

La version serveur de NT4 permet de voir le flux des workstations qui ont l'agent de moniteur réseau (service 'Agent et outils du moniteur réseau').

Pour la version SMS (complète) : il y a capture distante (sur une workstation avec l'agent du moniteur réseau installé), ce qui permet de sortir du segment local. Cependant, cela utilise plus de bande passante, protocole PGBP, modification et retransmission de trame.

PARAMETRES de CONFIGURATION

Pour le lancer : panneau de configuration/services/serveur/propriété :

- minimiser la mémoire : **10 connexions simultanées** + applications bureautiques locales
- équilibrer : **64 connexions simultanées** maxi
- débit maximum pour le partage fichier (défaut) : utile pour les environnements de serveur de fichier avec un nombre important de clients (ex : Access (non client/serveur), IIS).
- débit maximum pour application réseau : utile pour les environnements de serveur d'application ou quand une mémoire cache minimum est souhaitée (ex : Exchange), NT server contrôleur (authentification).

RAPPEL SUR L'OPTIMISATION DE LA SYNCHRONISATION D'UN ANNUAIRE

Pour *synchroniser un annuaire* : clé .../netlogon/parameters :

- sur CPD : positionner les clés **PulseConcurrency**=10 (nombre de mises à jour simultanées de Contrôleur Secondaire de Domaine) ; et **ChangeLogSize**=64 (Ko taille journal des modifications -> synchronisation totale si plein)
- sur CSD : positionner la clé **ReplicationGovernor** = 100 (% tampon de 128 Ko -> bande passante)

Configurer netlogon pour la synchronisation entre les heures de charge (avec les commandes **at regini fic script** et **net start netlogon**)

DEPANNAGE

Utiliser **GETSID** (depuis le *Kit de Ressources Technique)* pour vérifier si un Contrôleur Secondaire de Domaine a changé de domaine (interdit).

Utiliser **regback.exe**/**regrest.exe** (*Kit de Ressources Technique*) : sauvegarde du registre (ou rdisk /s, ou NTbackup).

Pour avoir l'aide sur le registre : utiliser **regback.exe**/**regrest.exe** (*Kit de Ressources Technique*).

L'utilitaire de diagnostic NT s'appelle **winmsd** (*Kit de Ressources Technique*), il génère un rapport msdrpt.txt. La génération du rapport est possible à distance.

TDISHOW (*Kit de Ressources Technique*) permet de savoir si TDI a été correctement chargé.

Services : csrss.exe (ss win32), lsass.exe, smss.exe (session manager) sont ainsi lancés au démarrage en fonction des valeurs : **dependongroup**/service (ref clé : servicegrouporder), type (1=noyau 2=sys 10/20=Win32) et **start** (0=amorçage 1=sys 2=auto 3=à la demande 4=désactivé).

Les commutateurs de boot.ini : /debug /maxmem:n /noserialmice:comx,y /basevideo /sos.

Pour vérifier si les pilotes sont chargés, on utilise Drivers.exe (*Kit de Ressources Technique*).

Kernel debugger : dépannage via cable null modem, il faut : i386kd.exe + RAS + remote.exe et interrupteur /debug ou /crashdebug dans le fichier boot.ini.

Memory.dmp : (**dumpchk** (vérification du fichier de dump)/**dumpexam** (Analyse du fichier)/**dumpflop** (charge sur une disquette)).

crash system : **memory.dmp** (system/propriété/écrire), crash d'application : **user.dmp** (**drwtsn32**). C'est l'utilitaire *crashdump* qui fait la capture de la mémoire.

Ecran bleu démarrage (cf. Cours de Support Technique) :

- création fichier d'échange
- lancement de ***bootexecute*** (conversion NTFS…)
- création de liaisons symboliques

REGISTRE

HLM/CurrentControlSet/services/**Netlogon**/parameters = synchronisation.
HLM/CurrentControlSet/services/**browser**/parameters = explorateur de répertoire.
HLM/CurrentControlSet/services/**replicator**/parameters = duplicateur de répertoire.