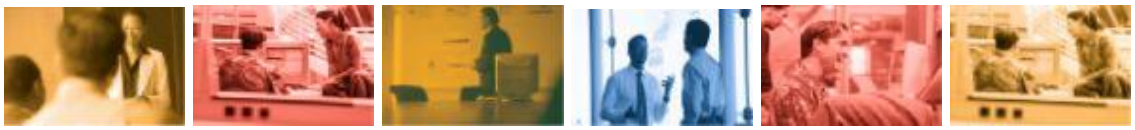

Microsoft – Technopoche

Migration de Windows NT4 vers Windows 2000 (Glenn Pittaway)

Microsoft
Auteur : Glenn Pittaway
Date de révision : le 18 avril 2001
Version : 1.2

Concepts de sécurité et migration

Sécurité de NT

Authentification

Les objets comme les groupes, les utilisateurs et tous les principaux de sécurité sont identifiés de manière unique par leur SID (Security Identification).
Lors de sa connexion un utilisateur va recevoir un jeton d'accès. C'est un conteneur virtuel qui regroupe le SID de l'utilisateur ainsi que les SID des groupes dont il est membre.

Autorisation

A chacun des objets du système auxquels peut avoir accès un utilisateur est associé une ACL (Access Control List), c'est une liste qui contient les SIDs des groupes et utilisateurs ayant des droits sur lui-même ainsi que les droits qui leurs sont associés.
Lors d'une tentative de lecture, le système va comparer les SIDs du jeton d'accès de l'utilisateur à ceux contenu dans l'ACL.

Exemple :

Imaginons un système avec deux domaines, un domaine de comptes (DomCompte) et un domaine de ressources (DomRessource). L'utilisateur Bob appartient au domaine DomCompte, son jeton va ainsi comporter 1 SID : celui de Bob.
Sur la machine DocServ1 de DomRessource on a créé un groupe local TechEditors, on a placé dans ce groupe Bob. On a aussi partagé un dossier sous le nom Docs et on a attribué au groupe TechEditors les droits d'accès complet.
Lorsque Bob va vouloir accéder à Docs, DocServ1 va vérifier si son SID fait parti de l'ACL de Docs ou si son SID fait partie d'un des groupes locaux référencé dans l'ACL. C'est le cas, Bob va pouvoir accéder au répertoire partagé.

Comment fonctionne SIDHistory ?

Autorisation et migration

La restructuration d'un système d'information (fréquent lors de la migration vers Windows 2000) peut entraîner des mouvements d'utilisateurs d'un domaine à un autre. Le changement de domaine d'un utilisateur va provoquer un changement de son SID.
Le SIDHistory va permettre de maintenir les attributs d'accès aux ressources malgré ce changement d'identificateur.
Cet attribut est activé par Active Directory Migration Tool, ClonePrincipal ou MoveTree.

Exemple (suite) :

Imaginons que l'on ait déplacé Bob du domaine DomCompte vers un domaine Active Directory nommé DomWin2K. Dans ce cas son SID a été modifié, mais, avec SIDHistory, l'ancien est conservé. Cela va permettre à Bob de continuer à utiliser le partage Docs bien que ce serveur ne connaisse pas le nouveau SID de Bob.

Terminologie et Migration

La mise à niveau

Dans ce cas vous allez garder la même structure des domaines. C'est la méthode la plus simple.

Exemple :

Vous avez 4 domaines, un domaine de comptes et 3 domaines de ressources qui approuvent le domaine de comptes. Dans ce cas la migration est simple : mettez à jour les domaines en conservant leur rôle. Le domaine de comptes reste un domaine de comptes et les domaines de ressources des domaines de ressources. Le seul changement sera pour les relations d'approbations qui deviendront transitives et bidirectionnelles.

La restructuration

Appelée aussi consolidation des domaines, cette évolution implique un déplacement de comptes utilisateurs et de comptes machines entre les domaines. Typiquement, cette manipulation a lieu quand on veut passer de domaines mixtes (ressources et comptes) à des domaines avec un seul type de compte (machines ou utilisateurs). Cela permet de reconsidérer l'architecture afin de mettre en place une architecture idéale.

Pourquoi restructurer ?

Parce que la structure NT existante ne correspond pas à la structure 2000 désirée. En effet la structure NT originale a été altérée au fur et à mesure par l'ajout de domaines correspondant à des nouvelles structures (filiales, services nouveaux, etc.).
Parce qu'on veut migrer graduellement tout en conservant la possibilité de revenir en arrière en cas de problème.

Pour cela une nouvelle API a été écrite : DsAddSidHistory. Elle permet d'ajouter le SID du compte source à l'attribut SIDHistory du nouveau compte. Pour cela certaines conditions doivent être remplies : il faut que la manipulation reste à l'intérieur de la même forêt, que le SID soit unique, que la personne soit administrateur du domaine source et destination et que l'audit soit activé dans les deux domaines.

Planification de la restructuration

Mise à niveau

Quel OS vers quel Windows 2000 ?

Windows 9x	**è**	**Windows 2000 Professionnel**
Windows NT4/3.51 Workstation	**è**	**Windows 2000 Professionnel ou Windows 2000 Server**
Windows NT4/3.51 Server	**è**	**Windows 2000 Server ou Windows 2000 Advanced Server**
Windows NT4 Entreprise Edition	**è**	**Windows 2000 Advanced Server**

La mise à jour depuis Windows 3.x, Windows NT Workstation 3.5 et Back Office Small Business Server 4.5 n'est pas supportée.

Les différentes étapes

Le PDC en premier

Lors de la migration du PDC vers Windows 2000, l'Active Directory va être rempli avec le contenu de l'ancienne base SAM de Windows NT. Le serveur est alors en mode mixte (il supporte des BDC NT4). Il émule un PDC pour les contrôleurs secondaires ainsi la réplication a encore lieu. L'ajout de BDC (NT4) est toujours possible. Si le serveur Windows 2000 tombe, la promotion d'un BDC est aussi possible. Enfin les SIDs sont conservés.

Les BDC ensuite

Une fois le PDC migré, on peut commencer à migrer les BDCs vers Windows 2000. Deux options sont possibles : en faire des DC ou des serveurs membres. On peut, sous 2000, changer le rôle d'un serveur sans réinstallation. Avec l'utilitaire dcpromo il est possible de faire d'un DC un serveur membre et d'un serveur membre un DC du même domaine ou d'un nouveau domaine de la forêt. On ne peut pas, par contre, transformer un DC d'un domaine en un DC d'un autre domaine, il faut passer par l'étape serveur membre.

Pour installer Windows 2000 sur un BDC si le PDC ne peut pas être migré : le débrancher du réseau, le promouvoir en PDC, le migrer vers Windows 2000 en DC puis exécuter dcpromo pour le rétrograder en serveur membre.

Le basculement en mode natif

Les raisons de rester en mode mixte

Si certains des BDCs sont encore sous Windows NT4, si certaines des applications installées sur un PDC ou un BDC ne supportent pas Windows 2000 ou si l'on souhaite pouvoir revenir à l'état antérieur, il faut rester en mode mixte. Le passage en mode natif est irréversible.

Le basculement en mode natif

Une fois cette manipulation effectuée, deux nouveaux types de groupe sont disponibles : les groupes universels et les groupes locaux à un domaine. La limite de taille de la base SAM est supprimée (le nombre de compte est alors théoriquement illimité). L'imbrication de groupes devient possible. La réplication est désormais de type multi maître entre les DC (domain controlers) de l'AD.

Ordre de mise à niveau des domaines

Le premier domaine qui sera créé a un rôle particulier : il s'agit du domaine racine de la forêt. En cas de disparition de ce domaine; l'ensemble de la forêt devra être réinstallé. Généralement le domaine racine est un domaine de comptes.
Une fois le domaine racine créé, les autres domaines de comptes sont à mettre à jour. Ceci dans le but de pouvoir utiliser la délégation d'administration ainsi que les GPO (Group Policy Object) pour l'ensemble de la forêt.
Enfin, la mise à niveau des domaines de ressources peut être faite.

Les domaines de comptes

En premier lieu, le domaine racine. En cas de perte de ce domaine l'ensemble du système sera à réinstaller. Il est peut-être intéressant de créer un domaine vide (avec seulement deux DC) sur lequel aucune manipulation ne sera à effectuer pour éviter tout problème.
Ensuite, commencer par les domaines où il y a le moins de risques afin de minimiser les risques et les éventuelles interruptions de service.
Ensuite, des domaines avec peu d'utilisateurs afin, toujours, de minimiser l'impact d'un éventuel problème.
Enfin, les domaines cibles de la restructuration, ceux possédant un grand nombre de comptes qu'il va falloir déplacer.

Les domaines de ressources

Leur migration va permettre de dépasser le nombre maximum d'objets imposé par la base SAM et d'utiliser la délégation administrative sur ces domaines.

Plusieurs plan de migrations sont possibles : créer un nouveau domaine dans la même forêt, créer un domaine dans une nouvelle forêt ou transformer les domaines existants en OU (Organizational Unit).

En premier lieu commencer par les domaines des applications basées sur l'Active Directory (Exchange principalement). Ensuite les domaines avec beaucoup de stations de travail afin de pouvoir tirer pleinement parti d'Intellimirror. Enfin terminer par les domaines impliqués dans la restructuration.

Serveurs membres et stations de travail

Leur mise à niveau est simple puisqu'ils n'interviennent pas dans l'authentification.

Cela va permettre d'utiliser l'authentification Kerberos, le déploiement d'applications grâce à IntelliMirror, et les stratégies de sécurité (GPO).

Cependant, il faut commencer par les serveurs RAS et finir par les serveurs LMRepl export.

Considération de restructuration

Inter-forêt ou intra-forêt

Le clonage est possible seulement lors d'une migration inter-forêt

Il n'y a pas de destruction donc on a la possibilité de revenir en arrière (l'objet source existe encore). La migration incrémentielle est facile et l'ancien SID est enregistré dans SIDHistory. Par contre les mots de passe ne sont pas conservés de même que le GUID (Globally Unique Identifier).

Le déplacement d'objet est seulement possible lors d'une migration Intra-forêt

Dans ce cas, il y a destruction, l'objet source est déplacé. Pour cette même raison on ne peut pas revenir en arrière. La migration incrémentielle est difficile. Par contre l'ancien SID est toujours sauvegardé dans SIDHistory, le GUID est préservé, de même que les mots de passe.

Préparation

Profils

Les profils sont indexés en utilisant le SID des utilisateurs dans la clé de registre HKLM\Software\Microsoft\WindowsNT\CurrentVersion\ProfileList.

Trois options sont possibles : créer de nouveaux profils vierges dans le nouvel environnement, copier les profils ou enfin partager les profils en entre les deux environnements.
Dans tous les cas, il faudra porter attention aux éventuelles applications s'appuyant sur les profils.

Stratégies

Lors du démarrage du poste client, si le compte machine appartient à un domaine NT la partie machine de la stratégie système va s'appliquer (quelque soit l'OS), si le compte machine est dans un domaine 2000, la partie machine de la stratégie système va s'appliquer si l'OS est un NT, si l'OS est un 2000 celle de la GPO va s'appliquer.
De même lors du login, la partie utilisateur de la GPO ou de la stratégie va s'appliquer.

Pour l'instant, la migration des stratégies système n'est pas supportée. Avant de migrer il faut les désactiver.

Général

Attention à quelques points : Pstore n'est pas géré lors d'une migration. De même pour l'EFS, il faut décrypter les fichiers avant migration, la clé de cryptage dépendant du compte machine.

Pour plus de renseignements, voir le Customer Migration Cookbook" (disponible d'ici peu sur le web).

Scénarios de migration supportés

Inter-forêt

Migration de comptes utilisateurs incrémentielle de Windows NT 4.0 vers Windows 2000.
Migration de ressources incrémentielle de Windows NT 4.0 vers Windows 2000.
Migration de comptes utilisateurs incrémentielle entre des domaines Windows 2000.
Migration de ressources incrémentielle entre des domaines Windows 2000.

Intra-forêt

Migration de comptes utilisateurs incrémentielle entre des domaines Windows 2000.
Migration de ressources incrémentielle entre des domaines Windows 2000.

Migration de comptes utilisateurs Inter-forêt

Migration des domaines de comptes vers Windows 2000 sans impact sur l'environnement de production NT

Incorporation des domaines Windows 2000 "grassroots".

Les outils requis sont l'ADMT (Active Directory Migration Tool), ClonePrincipal et Netdom.

La démarche est la suivante :
Créer la forêt Windows 2000 puis établir des relations d'approbation afin que les ressources soient toujours accessibles (relation NT donc unidirectionnelle du domaine de ressources NT vers le domaine de comptes Windows 2000). Cloner ensuite les groupes globaux et enfin les comptes des utilisateurs. Pour terminer mettre hors service le domaine de compte NT.
Dans ce cas, le retour en arrière est toujours possible : rien n'a été supprimé. Il suffit de réactiver le domaine de compte NT pour revenir à l'état précédent.

Migration de comptes machines Inter-forêt

Restructurer le domaine de ressources dans une OU Windows 2000

Cela implique de rétrograder les BDCs en serveurs membres.

Les outils requis sont l'ADMT (Active Directory Migration Tool), ClonePrincipal et Netdom.

La démarche est la suivante :
Vérifier que la forêt a bien été créée, établir une relation d'approbation du domaine de ressource qui va accueillir la nouvelle OU vers le domaine de compte pour maintenir l'accès aux ressources. Cloner ensuite les groupes locaux partagés. Rétrograder alors les BDC du domaine de ressources en serveur membre puis déplacer les serveurs dans la nouvelle OU et enfin mettre hors service l'ancien domaine de ressources.

Liste de tests à entreprendre

Migration

Avant toute manipulation sur un serveur il faut tester les sauvegardes et le plan de récupération pour le cas on un problème surviendrait pendant les procédures d'upgrade. Il faut identifier les points qui pourraient s'avérer bloquants suite au passage en mode natif ainsi que toutes les altérations possibles de la production.

Pour cela tester la possibilité de migration du PDC (hardware, logiciels, etc...), de même avec les BDC. Tester également si les utilisateurs peuvent encore ouvrir leur session et accéder aux ressources.

Restructuration

Avant toute manipulation sur un serveur il faut tester les sauvegardes et le plan de récupération pour le cas on un problème surviendrait pendant les procédures d'upgrade. En profiter pour identifier et éventuellement choisir les outils nécessaires. Identifier les dysfonctionnements qui pourraient survenir à la production.

Pour cela tester les relations d'approbation avec la forêt cible ainsi que l'accès aux nouveaux groupes. Vérifier si le rétrogradage des PDC/BDCs en serveurs membres est possible et comment elle s'effectue. Tester également le changement de domaine ainsi que le bon fonctionnement des security principals migrés. Enfin tester que les droits des utilisateurs (logon ou accès aux ressources) sont corrects.

Clean Up

SIDHistory reste un outil de transition, bien que la période de transition puisse être définitive, il convient de mettre à jour les ACL. En effet le jeton d'accès est plus gros et les ACLs ne

peuvent plus être résolues. Pour remplacer les anciens SIDs par les nouveaux il faut utiliser l'ADMT.

Les outils

L'ADMT (Active Directory Migration Tool)

Il s'agit d'un produit sous licence Mission Critical Software (MCS). Il se présente sous la forme d'un Snap-in (composant logiciel enfichable) pour Microsoft Management Console (MMC).

L'interface graphique propose un certain nombre d'assistants pour différentes migrations : Migration de comptes utilisateurs, migration de groupes et migration de comptes machines.

Il est disponible sur Internet depuis le site Windows Update : http://windowsupdate.microsoft.com.

Ressource Kit "Support Tools" Ils se trouvent sur le CD Windows 2000 dans le répertoire support\tools.

Il s'agit de ClonePrincipal, d'un objet COM et d'exemples de scripts à adapter en fonction des scénarios supportés, de Netdom ainsi que de MoveTree.

Configuration de l'environnement

Pré requis de DsAddSidHistory

Pour pouvoir l'utiliser il faut les droits administrateur sur le domaine source et le domaine cible, le domaine source doit approuver le domaine cible. Il faut ajouter la valeur TcpipClientSupport dans le registre du domaine source sous la clé HKLM\SYSTEM\CurrentControlSet\Control\Lsa. Il faut créer un groupe local NomDomaineSource$$$ sur le domaine source et enfin activer l'audit succès/échec sur la gestion des comptes (Windows 2000).

Complément d'information

Planning Migration from Windows NT to Windows 2000 :
http://www.microsoft.com/windows2000/library/planning/activedirectory/plandommig.asp

Guide de déploiement Windows 2000 :
http://www.microsoft.com/windows2000/library/resources/reskit/dpg/default.asp