La carte routière vers *Active Directory*

Implanter le service de répertoires actifs de Windows 2000

Par : Nelson Ruest et Danielle Ruest
nruest@msn.com et danrue@reso-net.com
Les Entreprises Résolutions

La dernière édition de l'Info-Québec a présenté les nouveautés de Windows 2000 et un aperçu du potentiel d'Active Directory. Maintenant, il faut passer à la carte routière d'Active Directory afin de profiter pleinement de ce potentiel.

Windows 2000 apporte tellement de nouveautés et d'améliorations que son implantation préconise une réévaluation de nos approches informatiques. Ainsi la charpente informatique, le cadre de gestion des technologies distribuées, les projets de déploiement, tous doivent être bien saisis afin de profiter à fond de ses nouvelles capacités.

Aucun des éléments de Windows 2000 n'est plus critique que le service de répertoire actif, soit *Active Directory*. Celui-ci forme le point de départ pour toute évolution informatique basée sur Windows 2000.

Active Directory, c'est la création d'un espace virtuel sécuritaire, où les gens peuvent interagir soit entre eux, soit avec les composantes informatiques, le tout, selon les règles d'affaires de l'organisation.

Établir cet espace afin qu'il reflète la structure de l'organisation, les règles fonctionnelles d'interactions entre les unités organisationnelles, les liens géographiques de l'organisation, avec le but de remplir la mission de l'organisation et de lui permettre d'évoluer à son rythme et au besoin; tel est le défi.

Un peu de formation ... établir un vocabulaire commun

Quelques concepts particuliers sont essentiels afin de bien saisir Active Directory :

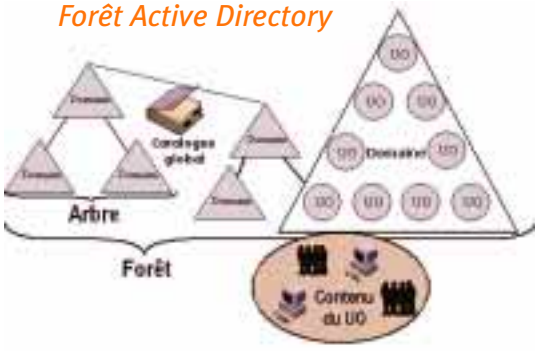
1. Une forêt forme la structure de base d'*Active Directory*. Elle regroupe des arbres, des domaines, des unités organisationnelles et des sites. Normalement, une forêt est constituée des éléments administratifs d'une seule organisation.
2. Un arbre est une collection de domaines et d'unités organisationnelles reflétant la structure géographique ou administrative de l'organisation.
3. Un domaine est une unité logique définissant une frontière de sécurité. Le concept de domaines dans Windows 2000 est similaire, mais pas identique à celui de Windows NT.
4. Une unité organisationnelle est un regroupement logique au sein d'un domaine. L'unité organisationnelle forme une frontière d'administration.
5. Un site est un regroupement physique de composantes logiques. Les sites sont utilisés pour former la topologie de réplication d'*Active Directory*.
6. Un lien de confiance sert à établir la topologie de réplication entre les contrôleurs de domaines dans Windows 2000.
7. Un lien de confiance transitif est un lien automatique au sein d'un domaine.
8. Un lien de confiance explicite est un lien manuel établit entre deux forêts ou une forêt Windows 2000 et un domaine Windows NT.
9. Un contrôleur de domaines est un serveur qui gère les composantes d'*Active Directory*.
10. Le service de catalogue global sert à localiser les éléments composant *Active Directory*. Il sert de source pour la recherche de ces éléments, de gestionnaire pour les groupes universels d'utilisateurs et entreposer le schéma et la configuration d'*Active Directory*.

Active Directory, c'est quoi?

L'implantation de Windows 2000 comprend plusieurs étapes, mais aucune n'est plus critique que la planification et l'implantation d'*Active Directory*. Il ne faut pas toutefois paniquer, car *Active Directory* forme un espace virtuel qui, une fois conçu, permet sa restructuration. Si vous n'êtes pas satisfaits de votre conception d'espace logique dans Active Directory, vous pourrez toujours la reconfigurer — pas sans impacts, mais sans avoir à tout recommencer.

Selon Larousse : « Un répertoire est une table, un carnet où les matières sont rangées dans un ordre qui les rend faciles à trouver. » Il ne faut pas confondre un répertoire avec un annuaire, qui lui est un « ouvrage publié...donnant la liste...des abonnés à un service... ». Oui, le service de répertoires de Windows 2000 comprend les fonctions d'un annuaire, mais ses capacités vont beaucoup plus loin.

Forêt Active Directory



Une forêt Active Directory forme une représentation virtuelle de l'environnement informatique d'une organisation.

En informatique, on trouve des services d'annuaires dans des logiciels de courrier électronique tels *Lotus Notes* ou *Microsoft Exchange*.

Le service de répertoire actif est un service du réseau qui entrepose de manière structurée les informations des ressources du réseau et les rend accessible aux utilisateurs et aux applications. C'est un service multifonction comprenant l'intégration des applications, de l'infrastructure et des services de sécurité ainsi que la gestion des ressources et des utilisateurs.

Il y a trois composantes fondamentales dans *Active Directory* :

- L'espace de nommage, qui a pour objectif d'offrir une vue unifiée du réseau;
- La structure logique, qui comprend la structure des objets, de l'organisation et la relation des objets dans la structure; et
- La structure physique, qui permet la localisation des sites géographiques et la définition des opérations entre les éléments physiques de l'infrastructure.

Nommer son espace

Active Directory est étroitement relié à la dénomination DNS d'une organisation. Normalement, une organisation doit se doter d'une dénomination interne et externe. La dénomination externe est celle qui est disponible au publique. Elle doit être enregistrée officiellement au sein d'organisations internationales de nommage. Un exemple de cette dénomination est WWW.Reso-Net.COM, le nom commercial du site Internet des Entreprises Résolutions. Il y a plusieurs types de noms Internet, COM, EDU, NET, ORG, GOV, CA, QC.CA, etc... Chacun doit être enregistré afin d'éviter les collisions de noms (imaginez si deux organisations utilisent le même nom, impossible de trouver l'une ou l'autre par l'entremise de votre fureteur Internet!).

Trois stratégies de nommage se présentent pour Active Directory :

1. Le même que sur Internet — Cette approche rend les choses simples pour les utilisateurs car ils n'ont qu'un seul nom à retenir, mais elle les rend difficiles pour les administrateurs car ils auront de la difficulté à identifier si l'espace à gérer est interne ou externe. En effet, cette approche pourrait constituer une brèche de sécurité car il est difficile d'identifier si une intrusion provient de l'interne ou de l'externe.
2. Une branche située sous le nom Internet — Encore une fois, cette approche est simple pour les utilisateurs mais complexe pour les administrateurs. Elle peut constituer une brèche de sécurité.
3. Un nom séparé à l'interne — Cette approche est l'approche recommandée. Utiliser un nom séparé rend les tâches de gestion et de sécurisation beaucoup plus faciles. Et, si le nom utilisé se rapproche du nom externe, il ne causera pas de difficultés aux utilisateurs. Par exemple, si une organisation transige sur Internet en tant que Reso-Net.COM, elle pourrait avoir un nom interne de Reso-Net.NET. Ces noms sont différents mais ils se rapprochent l'un de l'autre. Il est clair pour les utilisateurs qu'ils transigent soit à l'externe ou à l'interne.

Il est important d'utiliser un nom officiel à l'interne et de s'assurer que ce nom est enregistré auprès des autorités officielles!

Il se peut fort bien que l'organisation doive un jour ouvrir ses portes à des intervenants externes, soit par l'entremise de fusions, soit par l'entremise de partenariats. Dans une telle situation, le nom interne sera exposé à Internet. Si le nom n'est pas officiel et autorisé, l'organisation peut se retrouver dans une situation fâcheuse.

Les éléments d'Active Directory

Le schéma définit tous les objets logiques de AD soit, les classes d'objets, les objets eux-mêmes, leurs attributs et les règles de création et de manipulation.

La configuration est l'entreposage de la structure physique soit les sites, les domaines, les contrôleurs de domaines et les services disponibles.

Les domaines font l'entreposage de tous les objets locaux soit les utilisateurs, les groupes, les ordinateurs et les unités organisationnelles. Ils sont aussi le fournisseur d'authentification.

Le DEVIS© Active Directory

Établir un DEVIS© pour *Active Directory* consiste à découvrir, évaluer, valider, implanter et supporter cette technologie. Ce DEVIS© doit se concentrer sur quatre éléments principaux :

1 Le premier niveau de découpage d'*Active Directory* se concentre sur l'élaboration de l'espace de nommage. Celui-ci formera la constitution de la forêt organisationnelle (voir Un peu de formation…). *Active Directory* est étroitement relié au protocole TCP/IP et par le fait même, à la structure de nommage DNS d'une organisation. Ainsi, plusieurs d'entre vous pourrons tout simplement réutiliser la structure de nommage DNS existante au sein de votre organisation (voir Nommer son espace…).

2 Le deuxième niveau de découpage est la structure des domaines, les frontières de sécurité et des unités organisationnelles, les frontières d'administration. Ici, il sera important d'impliquer gestionnaires, administrateurs, ainsi que technologues car les règles organiques de l'organisation doivent y être inclus.

3 La gestion de l'espace de nommage est le troisième élément. Celui-ci se concentre sur les services de nommage tels DNS, l'attribution automatique d'adresses TCP/IP avec DHCP, et si le réseau le demande, la gestion des noms pré-Windows 2000 avec le service WINS. Cet élément doit aussi comprendre la disponibilité des services aux utilisateurs. Ainsi, le positionnement de serveurs de catalogue global, de contrôleurs de domaines et la gestion du temps dans le réseau seront aussi à considérer.

4 Finalement, la topologie de réplication doit être élaborée afin de s'assurer que les données sont à jour dans chacun des sites de l'organisation. *Active Directory* est une base de données distribuée. Cette base de données est entreposée dans des contrôleurs de domaines, mais puisqu'elle est constituée de données locales au domaine et globales à la forêt, aucun de ces derniers ne détient une copie complète. Il faut donc s'assurer que la réplication d'informations soit configurée de telle manière à rendre les informations disponibles sans toutefois utiliser toute la bande passante du réseau étendu.

Ces quatre éléments formeront le « blueprint », le plan d'action pas à pas, de votre implantation. Pensez-y bien car ce « blueprint » devra permettre l'évolution à long terme de votre réseau Windows 2000.

Étude de cas : Premier niveau de découpage

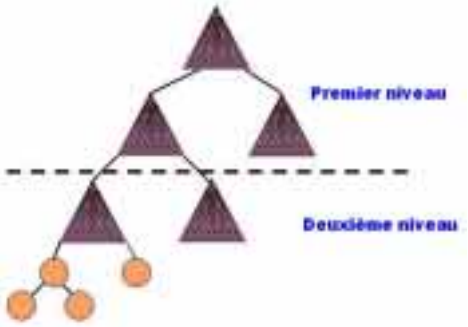
Prenons par exemple une organisation qui désire établir un premier niveau de découpage : la forêt et les arbres. Cette organisation est composée de plusieurs branches différentes distribuées sur un territoire géographique étendu et regroupant plusieurs dizaines de milliers d'employés. Ces branches sont de tailles variées (entre 50 et 5 000 utilisateurs par branche) et chacune a un conseil administratif. De plus, certaines branches ont plusieurs points d'opération. Quelle serait la structure idéale de premier niveau de découpage?

Afin d'élaborer la solution, il faut revoir le fonctionnement d'*Active Directory*. Ce service supporte l'implantation de plusieurs forêts, d'une forêt de plusieurs arbres, ou d'une forêt d'un seul arbre. Les règles d'opérations implantées dans une forêt ne transigent pas dans une autre forêt même si celles-ci sont reliées ensembles car les liens entre forêts ne sont pas transitifs (c'est à dire, automatiques). Donc le coût de gestion de multiples forêts est beaucoup plus élevé que celui d'une seule forêt. Les forêts multiples sont vraiment réservées pour des organisations partenaires ou des fusions d'organisations, ce qui n'est pas le cas ici.

La mise en place d'une forêt avec multiples arbres préconise que chacun de ces arbres utilise un espace de nommage différent. Par exemple, les organisations Reso-Net.NET et Resolutions.NET devraient s'intégrer dans une forêt de deux arbres à moins qu'une d'entre elles soit prête à modifier son espace de nommage. Ainsi chacun des arbres sera géré séparément car les politiques et les stratégies implantées avec *Active Directory* découlent selon leur point d'application. Cette approche n'est pas valide ici car notre organisation cible utilise déjà un seul espace de nommage.

La meilleure solution pour cette organisation est l'implantation d'une forêt d'un seul arbre. L'organisation utilise déjà un seul espace de nommage pour le réseau interne. Plusieurs des branches transigent sur l'Internet avec des noms indépendants, mais ces noms sont externes, ce qui n'a pas d'impact sur la structure *Active Directory*. En utilisant un seul

Découpage de premier niveau



Le découpage de premier niveau détermine le degré d'administration requis pour la forêt. Plus il est simple, moins l'administration sera lourde.

La mise à jour ou une nouvelle installation

Une des questions les plus importantes auxquelles les administrateurs de réseaux Microsoft doivent faire face avec Windows 2000 est : Doit-on effectuer une mise à jour de Windows NT ou doit-on faire une nouvelle installation de Windows 2000? Cette question est importante, voir critique, car le comportement de Windows 2000 diffère dans les deux cas.

Mise à jour de Windows NT	Nouvelle installation de Windows 2000
• Les profils d'utilisateurs demeurent dans WINNT\Profiles.	• Les profils sont entreposés dans Documents and Settings facilitant leur identification et protection.
• Les disques NTFS demeurent en format de base.	• Les disques NTFS sont convertis à des disques dynamiques permettant à Windows 2000 un contrôle total.
• La configuration de la sécurité demeure une configuration de base.	• Toutes les fonctions de sécurité sont disponibles.
• Permet une récupération facile des informations des utilisateurs.	• Demande une approche plus rigide afin d'assurer la protection des données car le disque dur est effacé.
• Coût moins élevé à court terme.	• Coût plus élevé à court terme.
• Coût de gestion plus élevé car cette approche impose des limites sur l'évolution de Windows 2000.	• Coût moins élevé de gestion car toutes les capacités de Windows 2000 peuvent être implantées.

La meilleure approche s'avère donc une approche mixte — une approche qui utilise une nouvelle installation, mais qui récupère les informations et la structure existante. Cette approche est simple. Il s'agit d'effectuer des copies de sécurité des données existantes sur les serveurs; effectuer une nouvelle installation qui réinitialise tous les disques d'un serveur; et récupérer les informations incluant leurs propriétaires et la sécurité qui les entoure.

arbre, l'organisation pourra assurer l'indépendance de ses branches (par l'entremise d'attribution de domaines) tout en garantissant une standardisation minimum au sein de son réseau Windows 2000. L'administration de la forêt est simplifiée car il n'y a qu'une seule racine à la forêt—toute politique globale peut être appliquée à cette racine. Tous les objets peuvent être nommés de la même manière tout en identifiant leur localisation. Les utilisateurs peuvent être identifiés avec un nom différent de la racine du réseau, par exemple, leur nom de courriel externe par l'entremise du concept de nom principal d'utilisateur.

L'utilisation d'un seul arbre permettra à l'organisation de restructurer les composantes de l'arbre plus tard si elle se rend compte que la structure implantée dans un premier temps n'est pas adéquate car *Active Directory* permet un simple déplacement d'objets au sein du même arbre.

Étude de cas : Deuxième niveau de découpage

Pour le deuxième niveau de découpage, les domaines et les unités organisationnelles, prenons une organisation de plus petite envergure. Au premier niveau de découpage, cette organisation a opté pour une forêt d'un seul

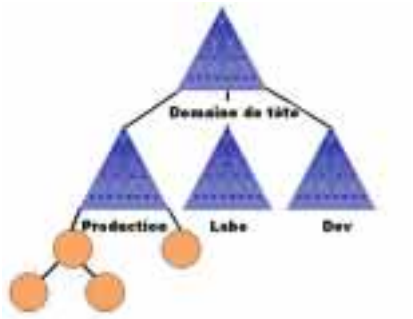
arbre car son espace de nommage était déjà unifié et elle n'utilise qu'un seul domaine (une seule frontière de sécurité) dans Windows NT. Mais comme tout organisation utilisant NT, ils ont souvent fait face à des situations où un seul domaine ne répondait pas tout à fait à leurs besoins.

Plusieurs organisations seraient prêtes à passer à une seule forêt d'un seul arbre avec un seul domaine. Cette solution est de loin la plus simple à implanter. Il est vrai que si le domaine unique ne satisfait pas les besoins de l'organisation, ils pourront toujours le modifier plus tard, mais il est aussi vrai que mieux vaut planifier correctement que corriger par après.

Considérons le besoin de cette organisation. Comme toute organisation d'envergure moyenne, elle doit se doter de plusieurs environnements — un environnement d'essais, de développement, de production. De plus, chacun de ces environnements doit représenter la réalité. Si elle se dote d'une forêt d'un arbre et d'un domaine, l'organisation se trouvera à gérer plusieurs forêts éventuellement car chacun des environnements sera une forêt.

De plus, le premier domaine d'une forêt Windows 2000 devient propriétaire de plusieurs éléments critiques à la forêt. Ce domaine de tête peut en effet demeurer vide afin de protéger ces éléments et de s'assurer que l'accès à ces éléments est réservé à un groupe restreint d'administrateurs ferrés. L'utilisation d'un domaine de tête vide et de sous domaines de production, de développement et d'essais rend identique la structure de chaque domaine et diminue grandement les efforts de gestion que l'organisation devra supporter plus tard.

Découpage de deuxième niveau



Le découpage de deuxième niveau doit représenter la réalité informatique. L'étude de cas représentée ici se concentre sur l'attribution de domaines non pas d'unités organisationnelles.

L'implantation d'Active Directory

Quelle que soit l'approche utilisée, implanter *Active Directory* c'est utiliser une série de règles d'opération et d'utilisation et de les appliquer à notre situation. Une règle qui s'avère très importante et même essentielle est la règle minimaliste : Commencez toujours avec le plus petit élément; si vous pensez forêt, utilisez un arbre; si vous pensez arbre, utilisez un domaine; si vous pensez domaine, utilisez une unité organisationnelle, et ainsi de suite.

Considérant la différence entre les concepts de Windows NT et ceux de Windows 2000, il est important de réaliser que nous ne savons pas tout sur ce système. Il est donc utile de viser plus petit que grand car il est toujours plus facile de graduer un élément dans *Active Directory* que de le diminuer.

Les exemples cités ici ne couvrent pas les quatre étapes de planification d'*Active Directory* car le sujet est trop long pour l'inclure au complet. Ils démontrent par contre, le processus à utiliser. Une autre décision sera l'exécution d'une mise à jour ou d'une nouvelle installation. Cette décision est importante car elle a des impacts immédiats. Pour en savoir plus sur ce processus, voir La mise à jour ou une nouvelle installation…

Et maintenant que l'*Active Directory* est conçu et implanté, vous pouvez tirer profit de ses avantages. Le prochain article examinera donc le retour sur investissement découlant de l'implantation de Windows 2000 et de l'utilisation de ses technologies de gestion des changements et des configurations.