Création d'un site web avec identification NT

Site intranet avec identification NT

Dans de nombreuses entreprises fleurissent les intranet. Dans ces entreprises, la gestion des comptes est souvent faite via un domaine Windows (NT ou Active Directory). Pourquoi ne pas alors réutiliser ces comptes déjà existants

Nous allons donc voir comment permettre cela simplement et pouvoir s'en resservir dans nos applications.

Introduction

Dans de très nombreuses entreprises se mettent en place des intranet. Mais que sont ces "Intranet" ? A quoi servent-ils ? Serait-ce de nouveaux outils pour Big Brother ?

Rien de tout cela, un intranet est un site web interne à l'entreprise, il est dédié pour des applications liées à la vie des collaborateurs dans l'entreprise qui vont de la gestion d'absences (s'inscrivant dans des projets E-RH) au partage documentaire (s'inscrivant dans des projets du type Sharepoint) en passant par des outils de suivi de statistiques d'activités; etc ....

- **Définition d'un intranet (FR)**

Ces intranet, n'étant que des Site web, peuvent fonctionner sur toutes plateformes à partir du moment qu'un serveur web fonctionne. On trouve ainsi de nombreuses solutions dans le monde libre sur des plateformes du type APACHE-PHP-MySQL, ou encore bien d'autres variantes. Nous nous limiterons dans cet article sur la plateforme Windows avec son serveur web IIS : Internet Information Server.

Présentation

L'objectif de cet article est de permettre de monter facilement un IIS en utilisant la sécurité intégrée NT. En effet, dans des entreprises ayant déjà une gestion des comptes faite sous Windows. Sur un domaine NT, on crée des comptes qui permettront aux utilisateurs de se connecter sur leurs machines aux partages pouvant exister sur le réseau de l'entreprise. De ce fait plutôt que d'avoir plusieurs systèmes d'identification, il est plus simple de reprendre les Logins NT comme moyen d'identifier l'utilisateur sur le site Intranet.

Nous allons donc voir comment configurer un serveur IIS pour utiliser cette authentification, puis comment récupérer cet identifiant dans vos codes en ASP3 et ASP.NET.

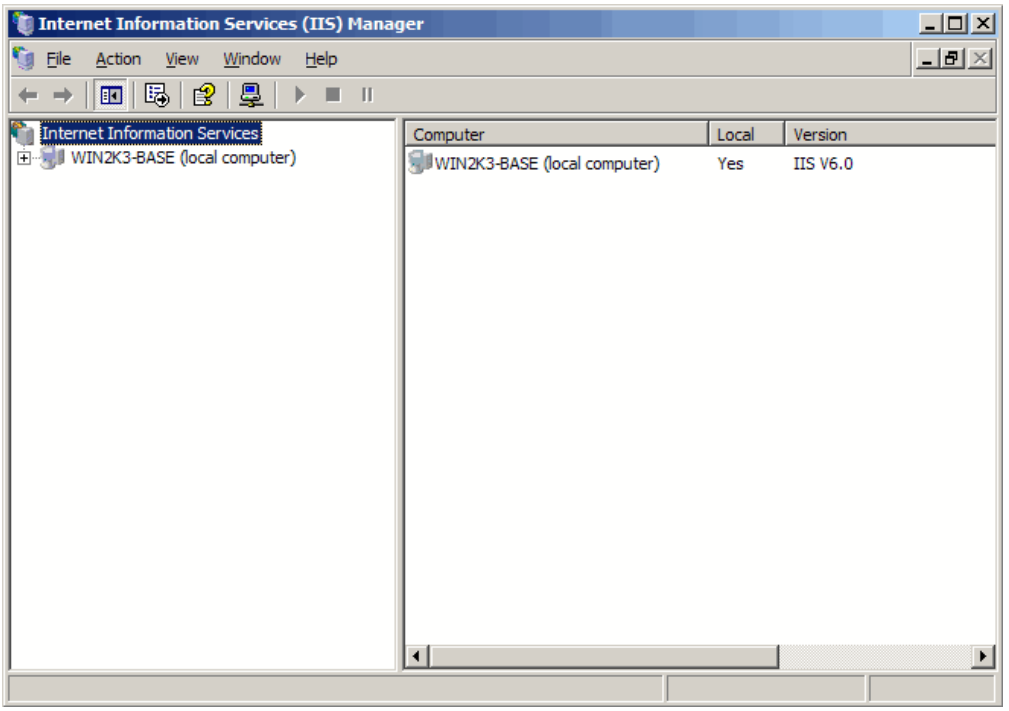
Création du Site intranet

Dans cette partie, nous verrons la configuration d'IIS pour une machine Windows. Je ferai mes captures d'écran sur une machine Windows 2003 US avec donc un IIS en version 6.
Les versions IIS 5 (sur Windows 2000) et 5.1 (sur Windows XP) sont sensiblement les mêmes pour cette configuration.

Pour faire cette configuration, il faut se connecter sur le serveur qui héberge cet Intranet. Ensuite il faut aller :

- Panneau de configuration (Control Panel)
- Outils d'administration (Administrative Tools)
- Services Internet (IIS) (Internet Information Services (IIS) Manager)

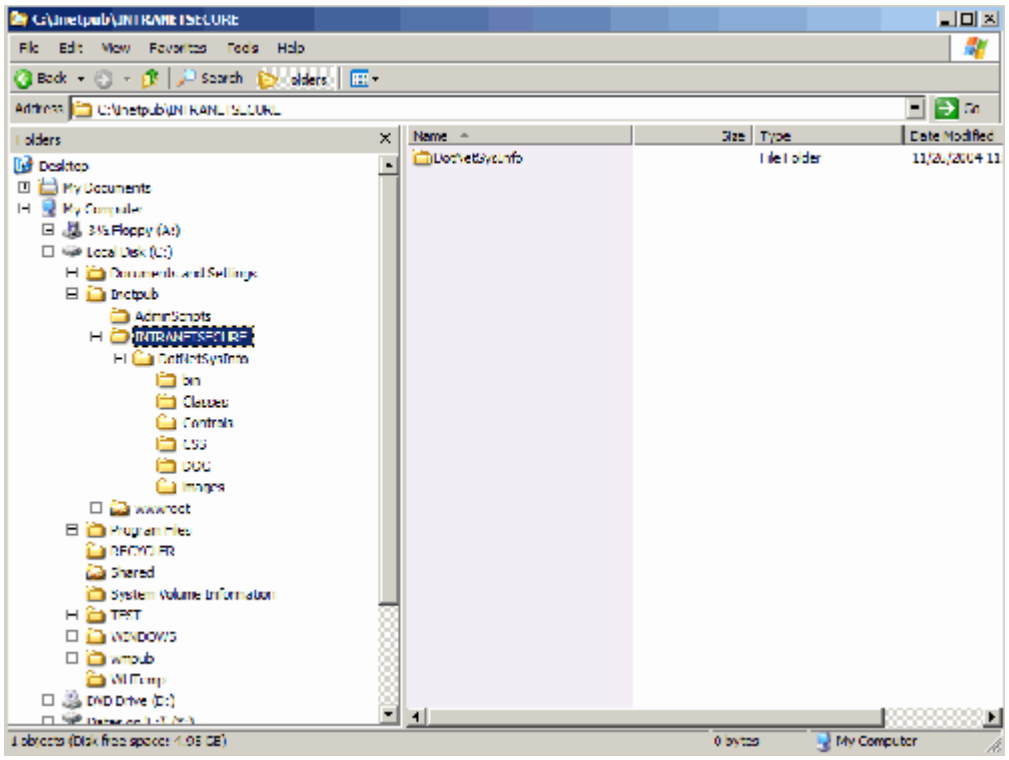
On obtient alors l'écran suivant :



Nous allons créer un nouveau site web sur ce serveur afin de montrer comment partir de zéro. Dans ce site nous placerons le projet que j'ai développé et qui est disponible ici :

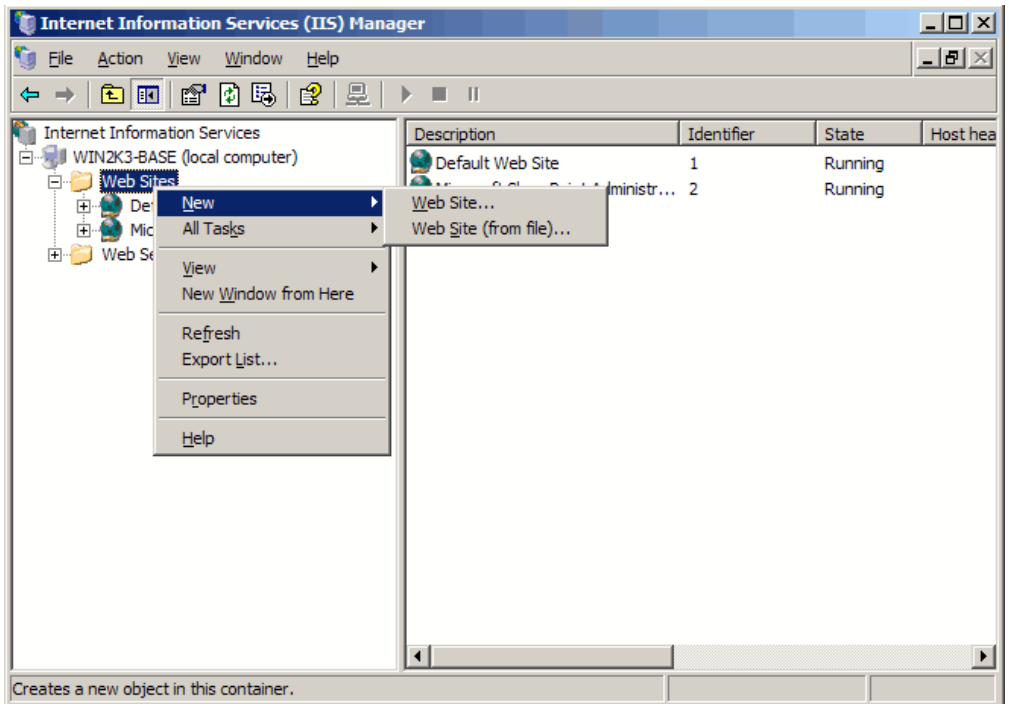
- **DotNet SysInfo (FR)**

De ce fait nous allons créer un répertoire sur le disque du serveur et placer dans celui-ci le projet précité.

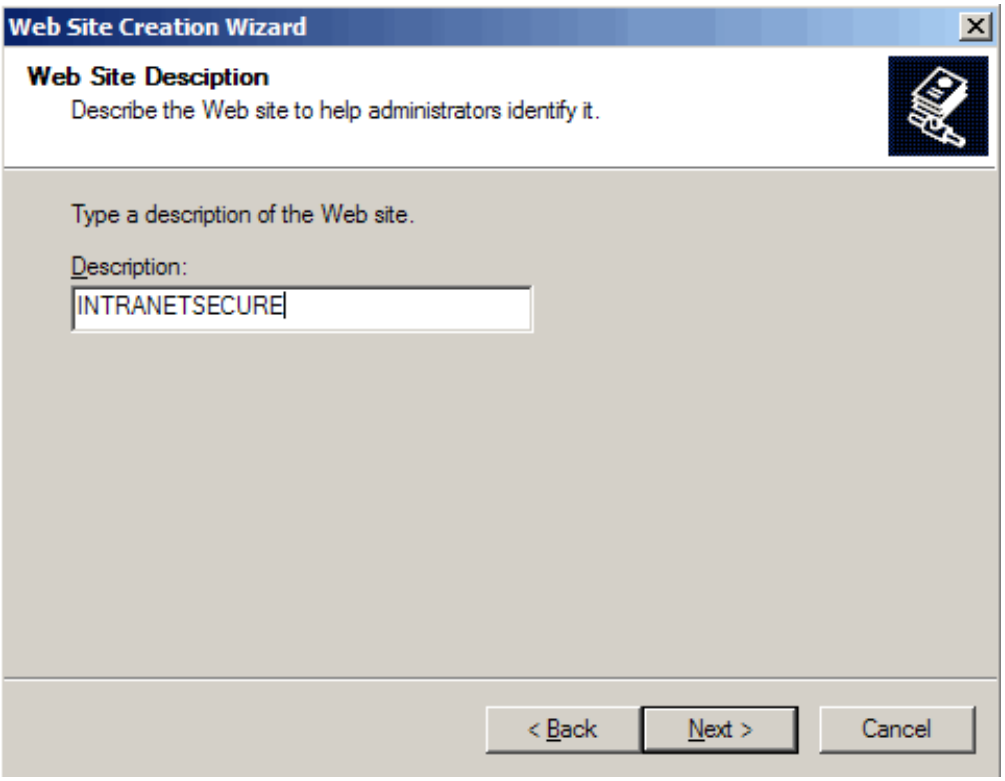


Attention : Dans notre exemple, le répertoire du site web Intranet est placé dans la même partition que le système (C:). Dans un cas de production, il faut absolument séparer les 2 parties. En effet, il faut séparer la partie OS de la partie donnée sur des machines de production, afin que, si l'OS a des problèmes de stabilité ou dans le cas d'une infection par virus, les données (dans notre cas, le site web) soient touchées le moins possible. Dans le même cadre, il faut aussi gérer plus finement les droits NTFS dans un cadre de production afin de ne pas donner tous les droits à tous les utilisateurs mais définir quels sont les comptes utilisés pour IIS et ASP.NET et de donner des droits limités à ces comptes.

Maintenant dans IIS Manager, nous allons créer ce nouveau site web.

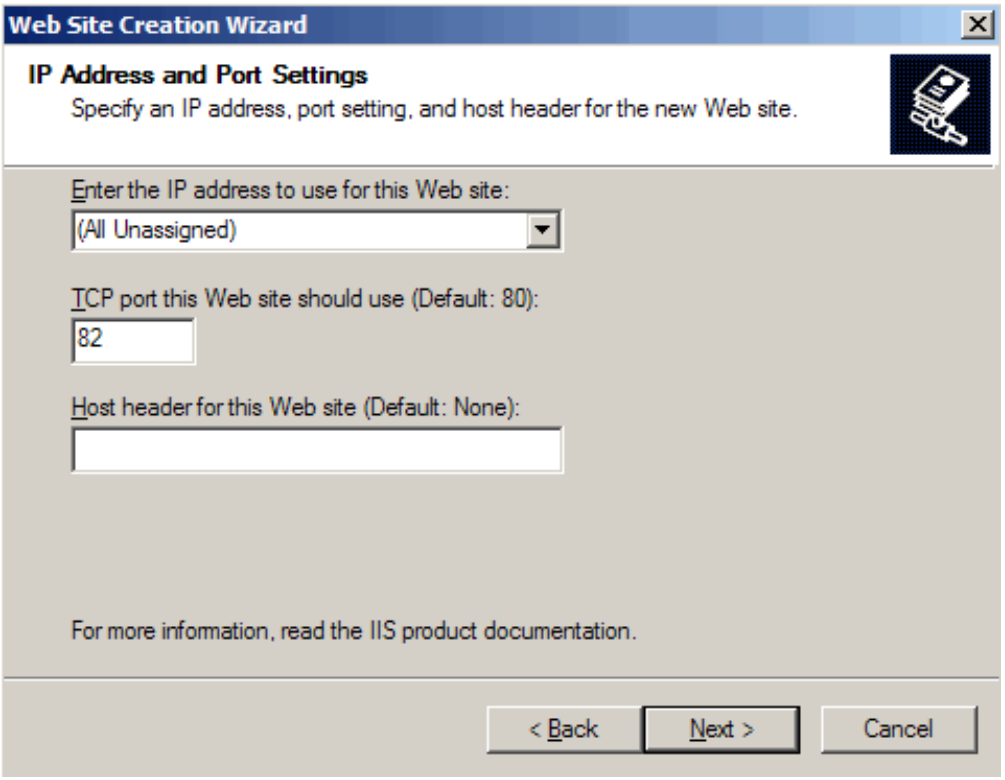


Le nom du site permet de le différencier des autres sites hébergés sur le serveur WEB. Dans notre cas, nous l'appellerons INTRANETSECURE.



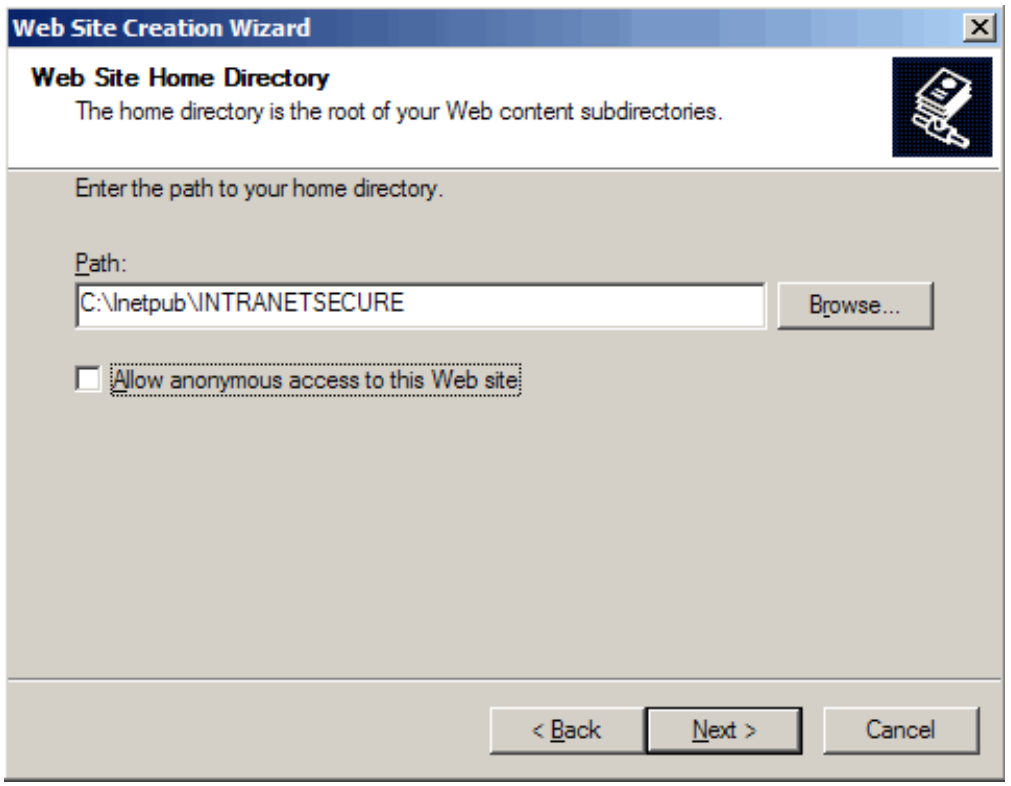
Ce site supportera toutes les IP possibles mais nous le placerons pour notre exemple sur un Port différent : 82.

Attention : Le choix du port 82 est uniquement destiné pour cet exemple, mais n'est en rien obligatoire et est même plutôt déconseillé dans un cadre de production. En effet, dans un cadre de production, il vaut mieux ajouter plusieurs adresses IP sur le serveur WEB et faire le « socket pooling », voir une détection par rapport au "Host Header".

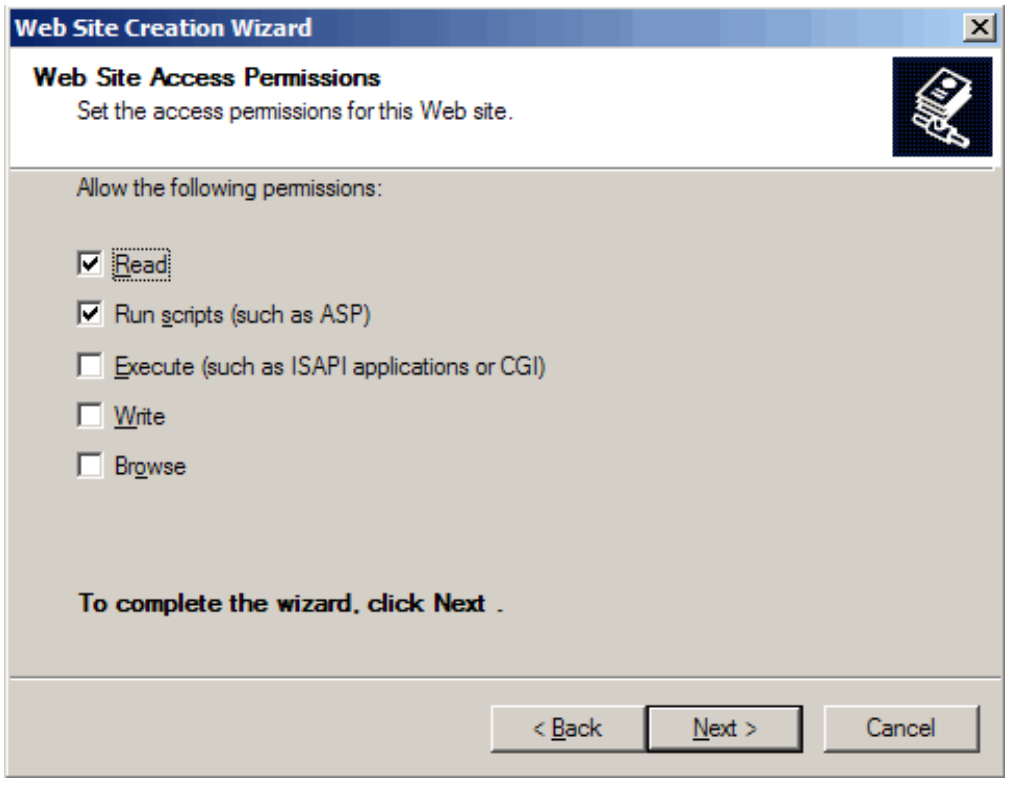


Attention : Dans un cas de production, il est conseillé de faire du « socket pooling », c'est-à-dire d'attribuer une IP donnée pour ce site WEB et non de faire comme dans notre exemple qui laisse toutes les IP possibles fonctionner avec ce site web.

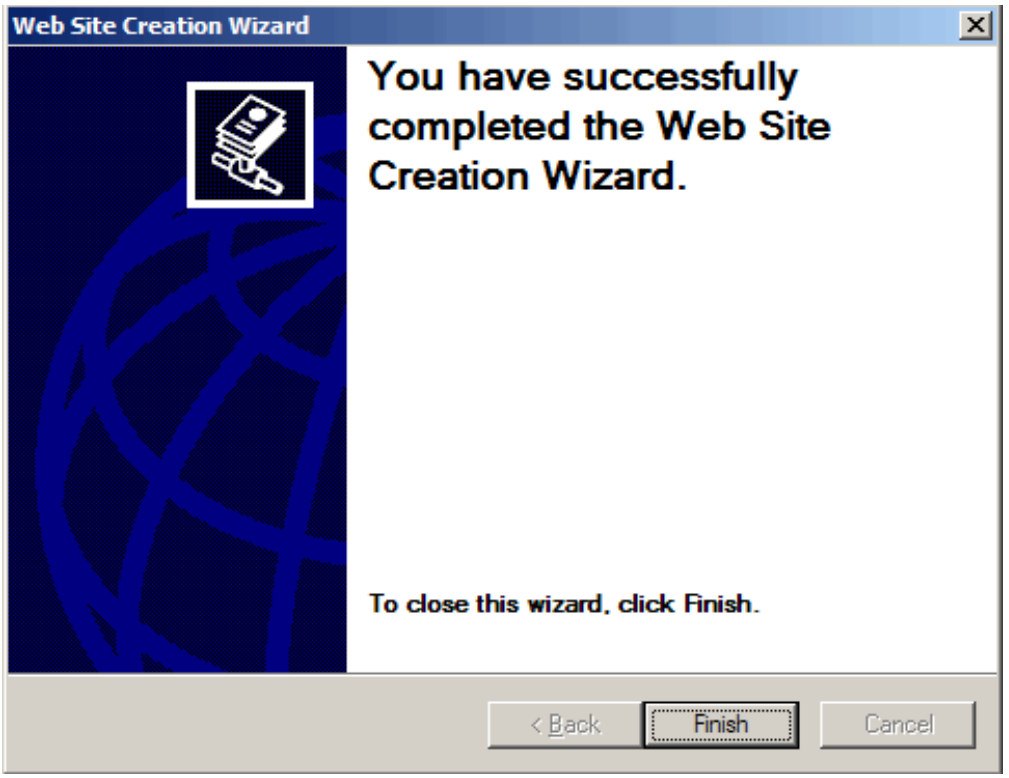
A ce stade, nous donnons le répertoire que nous avons créé comme répertoire par défaut de notre nouveau site web. Il faut décocher la case "Allow anonymous access to the web site" afin d'interdire les accès anonymes, ce qui implique que les utilisateurs devront s'identifier pour accéder à ce site Intranet.



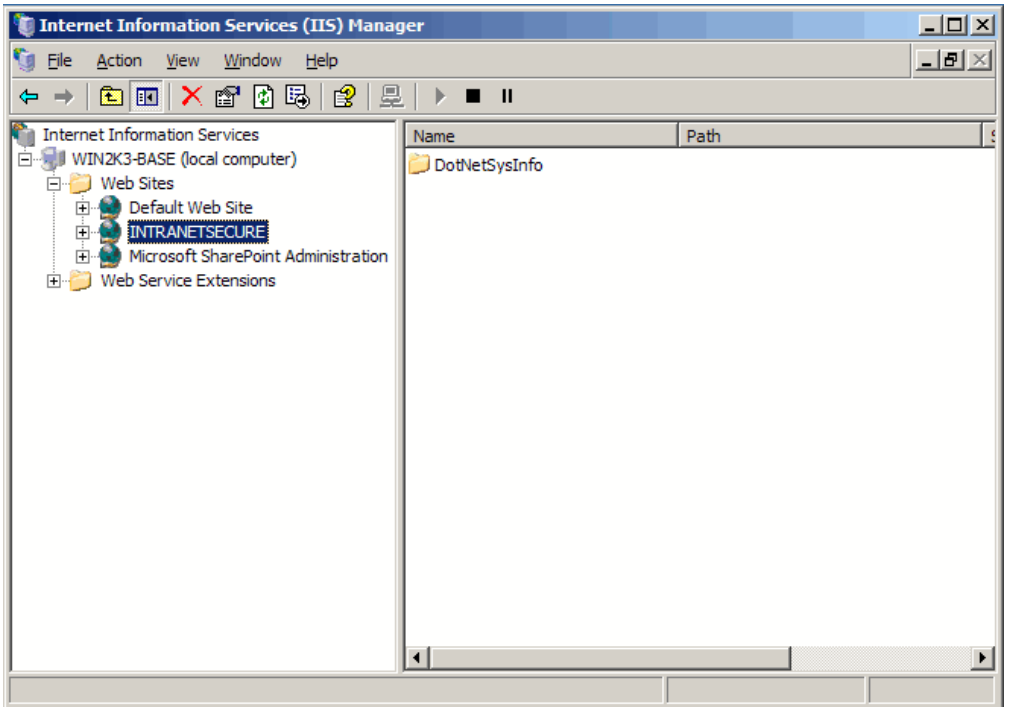
Nous laissons la configuration par défaut (autorisation des pages ASP, désactivation des CGI, du listage des répertoires et de l'écriture).



La création de notre site intranet est maintenant finie.



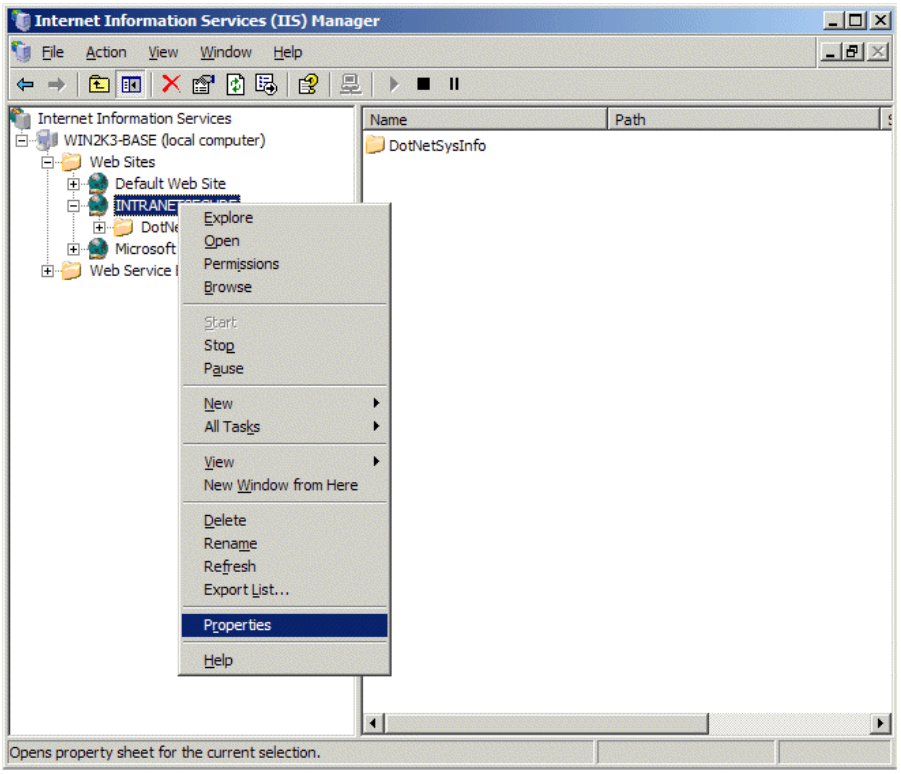
On voit maintenant notre nouveau site web apparaître dans la liste des sites hébergés par le serveur.



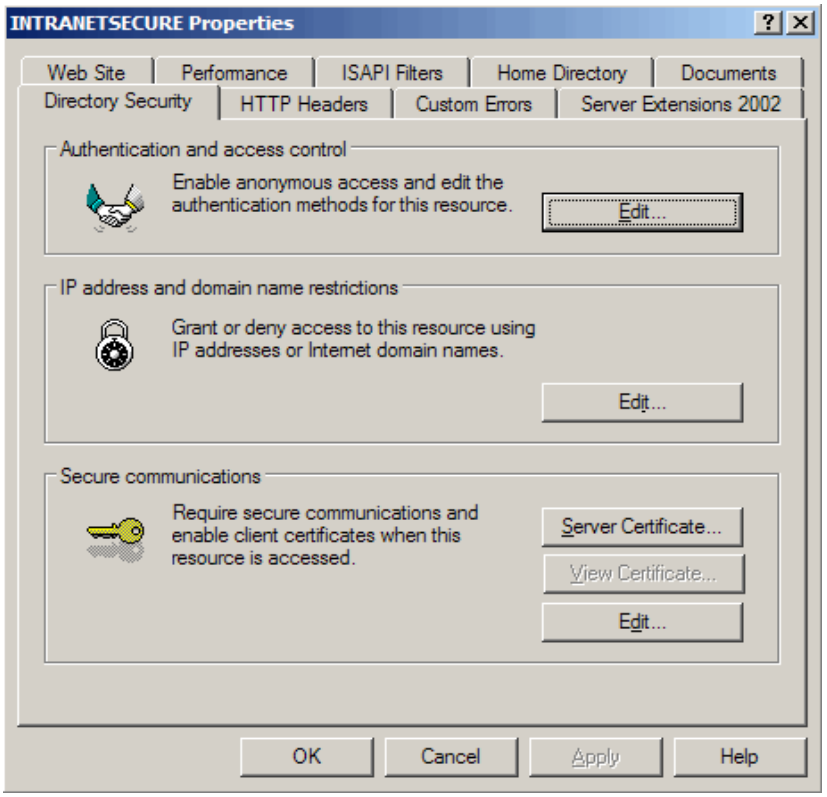
Voyons maintenant la configuration de ce site.

Configuration du site intranet

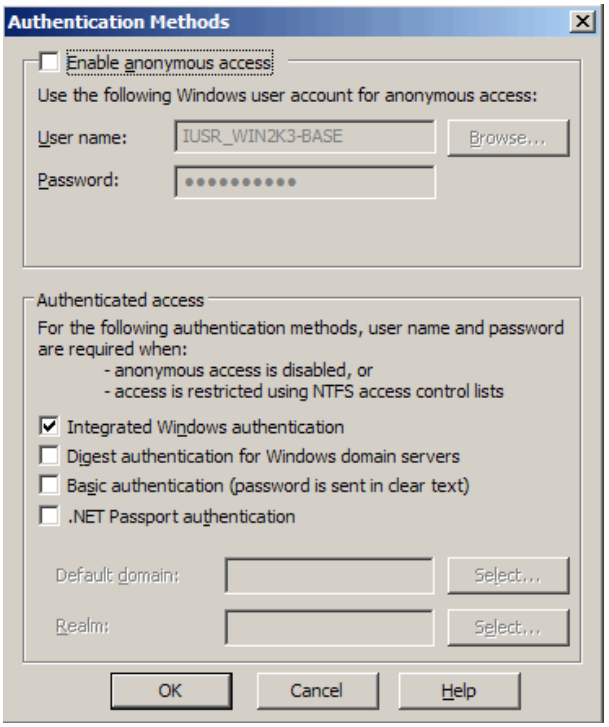
Maintenant que notre site web intranet est créé, nous allons voir la configuration de celui-ci de façon plus fine afin de détailler les options possibles pour le sujet qui nous importe. Pour cela, il faut cliquer avec le bouton droit de la souris sur notre nouveau site web et choisir Propriétés (Properties en US).



Dans cette boîte de dialogue nous allons directement prendre l'onglet "Directory Security" ou "Sécurité du Répertoire".



Cette partie permet de définir qui va être autorisé à accéder à ce site web. Nous pouvons limiter l'accès par la définition des adresses IP ou Domaine qui seront soit autorisés (granted) soit interdit (Denied). Ceci sera un filtrage par les IP. Ce n'est pas le sujet de cet article mais il faut savoir que cela existe. Nous allons cliquer sur le premier bouton, dans la partie "Authentication and Access Control", sur "Edit". Nous obtiendrons alors l'écran suivant.

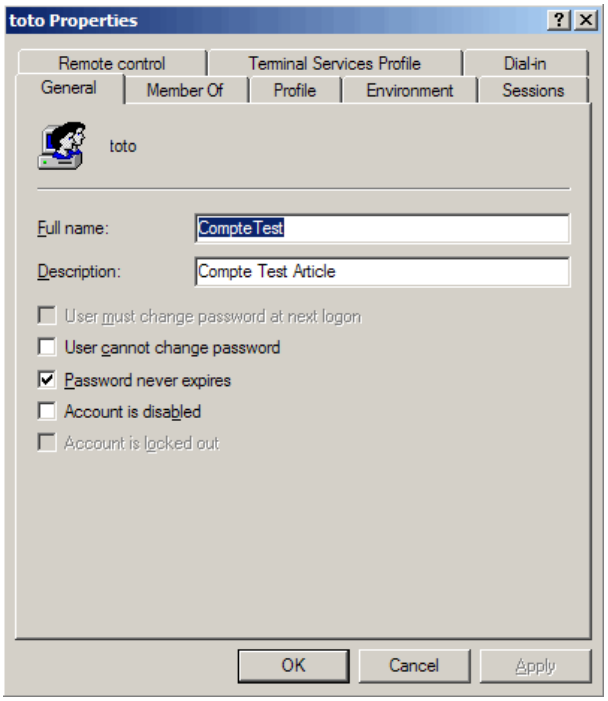


Dans cette fenêtre, nous avons dans la partie haute le fait d'accepter (ou non) les connexions anonymes en spécifiant le compte qui sera utilisé si une connexion anonyme s'établit. C'est de la que vient le compte exécutant une page quelconque (or page ASP.NET). Par défaut, il s'agit des comptes créés sur le serveur lors de l'installation d'IIS (IUSR_NomduServer). Dans notre cas, les connexions anonymes sont interdites, donc l'option est décochée.

En dessous de cette partie apparaît ce qui nous intéresse, l'utilisation des comptes NT avec une nouveauté par rapport aux précédentes versions d'IIS.

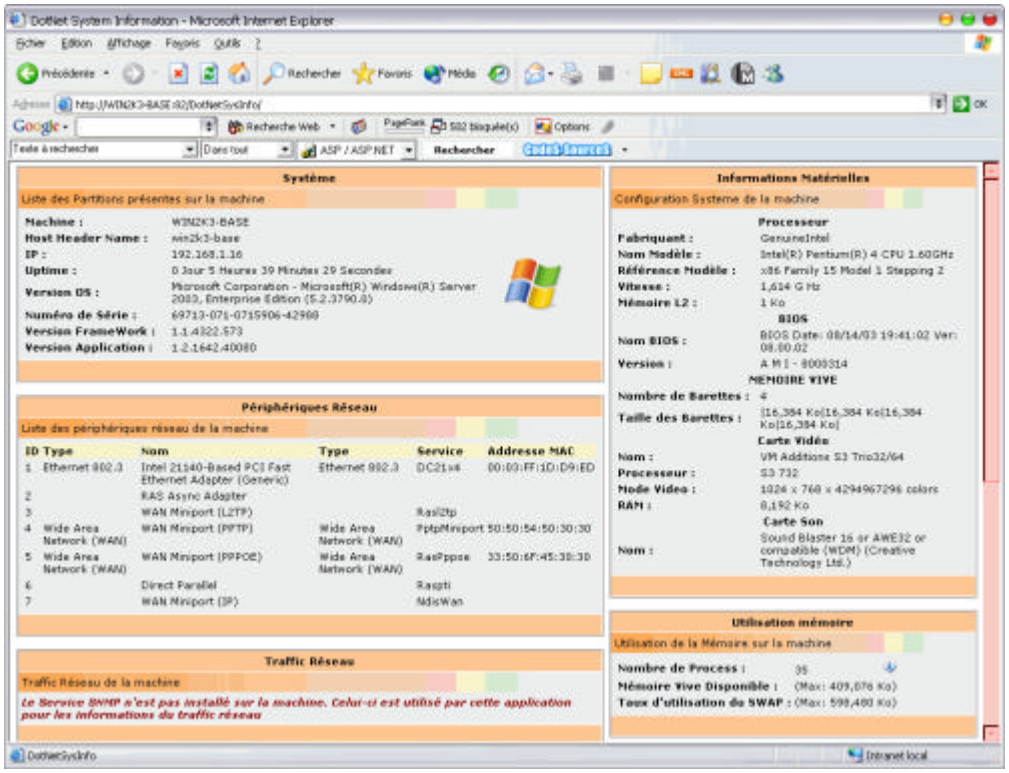
- La première ligne signifie que nous allons utiliser la sécurité intégrée de Windows. Elle permet donc de récupérer automatiquement l'identité de l'utilisateur connecté sur sa machine quand celui-ci a configuré sa machine pour (souvent la zone de sécurité intranet sur Internet Explorer).
- La seconde ligne spécifie que nous utiliserons les comptes du domaine et dans le cas ou elle est cochée, cette option active les champs du bas demandant le nom du domaine
- La troisième ligne spécifie le la façon de faire circuler cette identification. Par défaut, le mot de passe est crypté, mais en cochant cette case, vous demandez au serveur IIS de faire circuler le mot de passe en clair. Ceci est intéressant dans un cas précis, ou vous souhaitez stocker ce mot de passe dans une base de données par exemple. Il permet aussi de pouvoir construire des lien de cette façon : http://LeLogin:LeMotdePasse@LeServeurWEB/LeSousiteWEB/.
  Ce choix est tout de même très dangereux car le mot de passe devient visible dans l'application que le client vient consulter et si un développeur malveillant tombe la dessus, il peut récupérer tous les mot de passe. Ces logins et mots de passe sont aussi stockés en clair dans les logs d'IIS ce qui est aussi une faille de sécurité.
- La dernière ligne est spécifique à IIS 6 (sur Windows 2003), et permet d'utiliser l'identification via les comptes .NET PassPort

Dans notre démonstration, nous allons cocher la première ligne. Cela indiquera au navigateur qui va se connecter au site qu'il devra utiliser un compte reconnu par le serveur. De ce fait avec cette option tout compte appartenant au serveur lui même peut accéder à ce site web. Pour le montrer, j'ai créé un compte sur le serveur web que j'ai nommé "toto".



Lorsque je me connecte à ce site (http://WIN2K3-BASE:82/DotNetSysInfo/) j'obtiens une fenêtre me demandant de m'identifier, j'utilise alors le compte toto que je viens de créer.

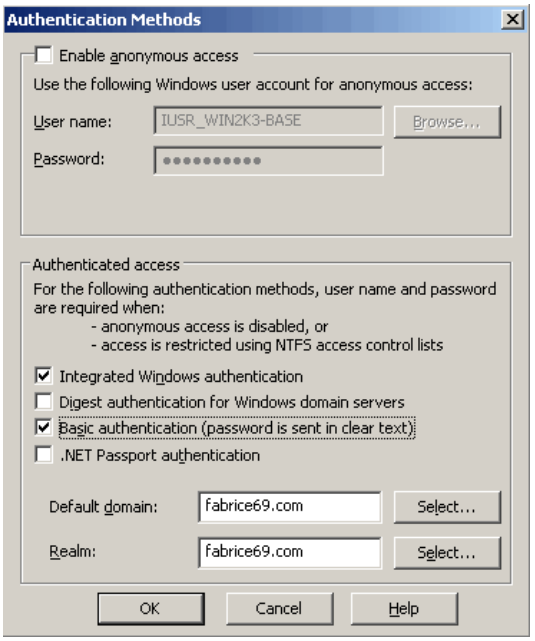
Le serveur ayant alors vérifié que le compte que j'ai utilisé est un compte connu pour lui m'autorise à entrer sur ce site.



Cette option est la première mais reste dangereuse pour un site qui nécessite une authentification, car l'utilisateur malveillant pourrait prendre un compte qui n'est pas sur le domaine mais est connu du serveur pour entrer sur celui-ci.

Nous allons donc voir comment bloquer l'identification uniquement aux comptes du domaine. Pour ceci, je vais faire rejoindre le Domaine Active Directory FABRICE69 au serveur Windows 2003, puis redémarrer le serveur et nous allons pouvoir faire ce blocage.

Une fois le redémarrage effectué, retournons dans l'onglet de Sécurité du Répertoire de notre site web intranet. Nous pouvons alors activer la troisième case à cocher et sélectionner le domaine sur lequel nous sommes rattaché (fabrice69.com). Il faut aussi penser à donner les droits d'accès au répertoire du site pour les utilisateurs du domaine, sinon ceux-ci ne pourront pas accéder à ce répertoire et donc au site web.



A partir de maintenant, si l'on retourne sur notre site web intranet, nous obtenons la fenêtre suivante :

Celle-ci refuse totalement le login que nous avons créé précédemment et n'attend qu'un login existant sur le domaine (Active Directory) "fabrice69.com". Le remplissage des domaines par défaut n'est pas obligatoire, mais elle permet de bloquer l'identification de l'utilisateur. De plus pour le confort de l'utilisateur, cette option lui évite de compléter la partie du domaine dans son navigateur internet.

Si vous ne cochez pas la première ligne, les utilisateurs devront forcément s'identifier manuellement en accédant à votre site intranet, vous ne pourrez donc pas utiliser la configuration client que le présente dans la suite de cet article.

Attention : La seconde option fonctionne uniquement sur des domaine Active Directory (2000 ou 2003) et ne fonctionnent pas sur des domaines NT4. Pour ceux-ci, il faut choisir la troisième ligne (authentification basique en sélectionnant le Domaine). Il exige aussi que les clients utilisent une version égale ou supérieur à Internet Explorer 5.

Le cas de l'authentification via PassPort .NET n'étant pas le sujet de cet article, je ne le détaillerai pas.

Maintenant que nous avons configuré notre serveur IIS pour notre site web afin qu'il n'utilise que les comptes de l'Active Directory, voyons comment obtenir ces logins dans notre code.

Utilisation de cette identification dans le code

Maintenant que nous avons configuré notre serveur IIS, nous allons voir comment récupérer dans un code ASP3 et un code ASP.NET (sous VB.NET) ce login.

Code sous ASP3

En ASP3, nous avons une liste de variables qui sont transportées lors de la connexion à la page web qui sont les Variables d'environnement (Request.ServerVariables). Vous trouverez la liste des variables disponibles ici :

- **ASP et les variables d'environnement (FR)**

Nous nous fixerons sur celui permettant d'obtenir le Login courant :

- Request.ServerVariables("logon_user")

De ce fait, le code permettant d'afficher ce login est très simple :

```
<%
Response.Write "Login courant : "& Request.ServerVariables("logon_user")
% >
```

```
<%
Dim LeloginCourant As String = System.Web.HttpContext.Current.User.Identity().Name().ToString
Httpcontext.Current.response.Write(LeLoginCourant)
% >
```

Attention : ce code renvoie tout le Login, c'est à dire DOMAIN\LOGINNT. Si vous ne souhaitez que le login, il faut utiliser le code suivant :

```
<%
Dim IDSlashas integer = 0
Dim LeloginCourant As String = String.Empty
IDSlash = System.Web.HttpContext.Current.User.Identity().Name().IndexOf("\")

LeloginCourant = System.Web.HttpContext.Current.User.Identity().Name().Substring(IDSlash + 1)

Httpcontext.Current.response.Write(LeLoginCourant)
% >
```

Maintenant, il ne vous reste plus qu'à développer votre application liée aux comptes de ce domaine.

Voyons comment améliorer et simplifier l'utilisation de cet intranet pour les collaborateurs de la société.

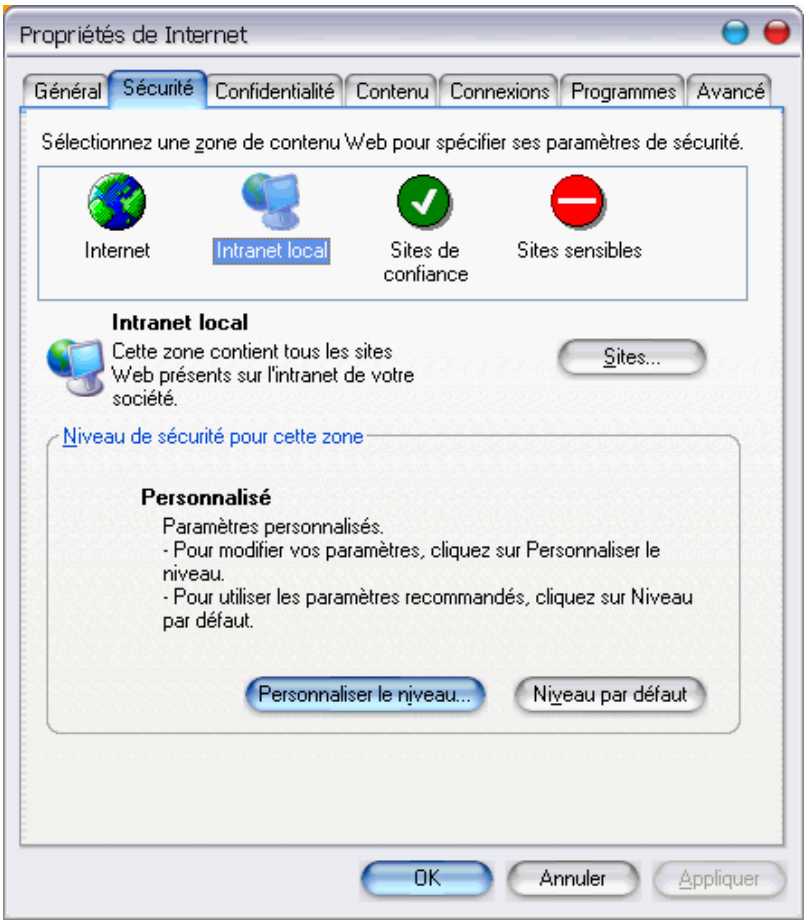
Configuration des postes clients

Voyons pour finir comment simplement configurer les postes clients afin que les utilisateurs de l'entreprise (tel que la secrétaire de base) n'ai pas à taper ce login/mot de passe, mais qu'il soit directement récupéré par le poste.

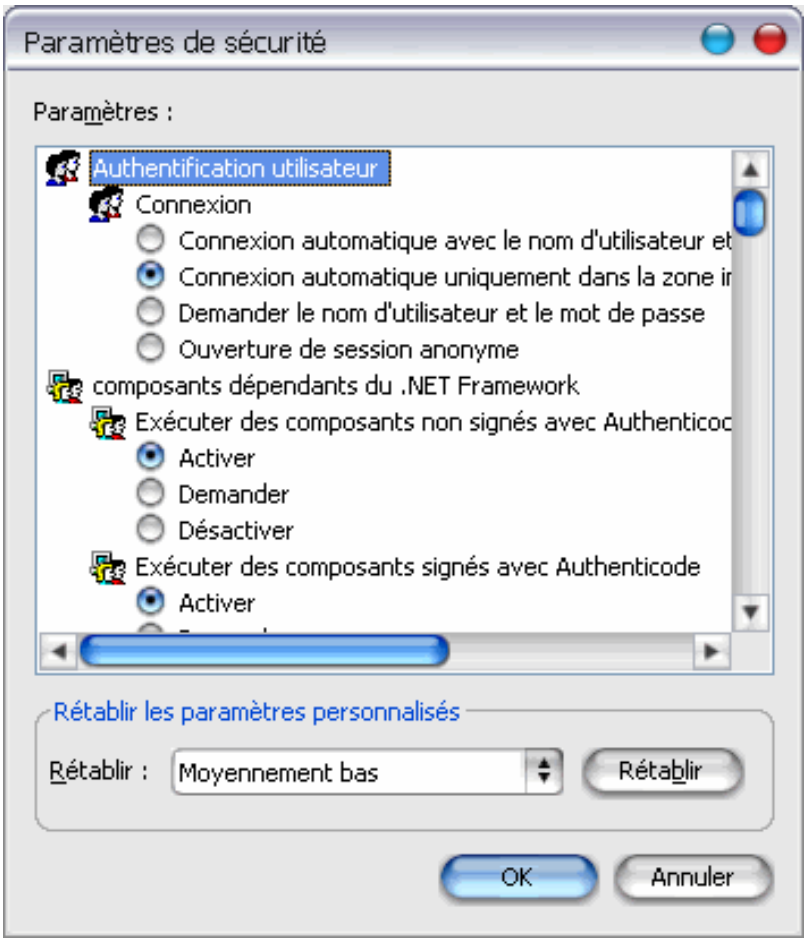
En effet, lorsqu'un utilisateur se connecte sur sa station le matin elle rentre une fois son Login NT et le mot de passe associé. Il est donc perturbant pour ces utilisateurs de devoir retaper ce couple Login/Mot de passe à chaque fois qu'ils ouvrent leur Internet Explorer pour aller sur l'intranet de la société.

Ceci se fait avec les options de sécurité de Microsoft Internet Explorer. Pour modifier celles-ci donc, il faut ouvrir les Propriétés d'Internet Explorer : Panneau de Configuration > Options Internet.

Choisir l'onglet Sécurité, parmi la liste des possibilités de configurations nous choisirons "Intranet Local" :



Dans cet écran, il faut déjà cliquer sur "Sites", puis "Avancé ..." afin de rajouter l'url de notre nouveau site Intranet. Puis valider pour revenir à l'écran de configuration de la sécurité. Il faut aller alors sur "Personnaliser le Niveau" :



Il faut alors vérifier dans la partie "Connexion", que la seconde ligne soit cochée.

Ainsi on spécifie au client Internet Explorer que celui-ci doit :

- Vérifier que le site sur lequel on se connecte est bien présent dans la liste des sites intranet définis
- Fournir automatiquement le Login et Mot de passe courant à ce site intranet

Vous n'avez plus qu'à valider et fermer la fenêtre. Ensuite pour contrôler, ouvrer l'Internet Explorer sur le site intranet en question.

Vous pourrez voir que le Login et Mot de passe ne seront plus demandés à l'utilisateur du poste que vous venez de modifier.

Conclusion

A cette configuration du site intranet, nous pouvons aussi dire que l'utilisation du cryptage est aussi très utile dans les cas des extranet voir de certains gros intranet (société multi sites distant), il est en revanche plus discutable dans les petites structures. Quoi qu'il en soit le passage du protocole HTTP vers HTTPS doit être étudié suivant le besoin de l'entreprise.

Pour ceux qui voudraient plus d'informations sur le protocole HTTPS, voici quelques liens intéressants :

- **Certificats self-signed avec IIS (FR)**
- **Introduction à SSL (FR)**
- **Accès aux sites W3 sécurisé (https) (FR)**
- **HTTPS sur IIS (FR)**
- **Mise en place du SSL avec IIS 5.0 dans un domaine Windows 2000 (FR)**

La sécurité est un sujet très vaste, mais la base de la construction d'un intranet d'entreprise est de savoir qui est l'utilisateur connecté afin de lui afficher les informations en relation avec son statut et sa fonction. Une secrétaire n'a pas les mêmes droits et devoir qu'un directeur.

Cette première configuration permet aussi de faciliter la vie des utilisateurs qui risque de se servir le plus des applications que vous aller leur développer. Si vous n'avez pas d'idée des applications qui sont possibles dans un Intranet, je vous conseille de consulter ces articles qui ne sont pas du tout écrit pas des informaticiens mais donnent la vision des Ressources Humaines :

- **L'intranet RH, un incontournable ou un simple outil ? (FR)**
- **Il faut bâtir un intranet à sa mesure, une étape à la fois (FR)**
- **Informatique et Ressources Humaine, Etat des lieux (FR)**
- **Informatique intranets et Self Services Ressources Humaines (FR)**

J'espère que cet article vous aura servi. Voila quelques articles ou exemples sur ce sujet :

- **Internet Information Services version 5.0, Livre blanc (FR)**
- **Méthodes d'authentification IIS (FR)**
- **Mécanismes d'authentification HTTP/HTTPS (FR)**
- **Authentification IIS (FR)**
- **Vulnérabilité dans l'authentification par formulaires dans ASP.NET 1.0 et 1.1 (FR)**
- **Windows Server 2003 Security Guide (US)**
- **Windows Server 2003 (FR)**
- **Internet Information Services (US)**
- **IIS 6.0 - Guide de l'Administrateur (FR)**

En vous souhaitant de bons projets de développement.

Romelard Fabrice (alias F___)