مكتب التكوين المهني وإنعاش الشغل
OFPPT
Office de la Formation Professionnelle et de la Promotion du Travail
www.tri.on.ma
www.tri.0fees.net

ISTA Mohamed EL FASSI - Errachidia

Filière : Techniques de Réseaux Informatiques

Support de formation

Module N° 26 :

Installation d'applications propres à Internet

Partie I : Les serveurs Web et FTP

Elaboré par : A. EL GHATTAS

Novembre 2008

www.tri.0fees.net

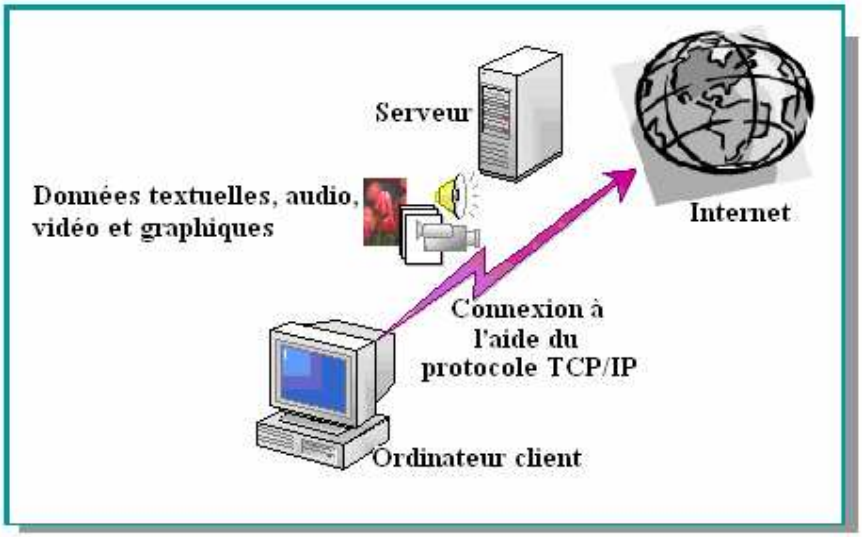
super.adnane@hotmail.fr

I. Services Web

1. Introduction

Pour comprendre la terminologie et les concepts relatifs aux services Web, vous devez d'abord vous familiariser avec la structure d'Internet et les technologies qui y sont déployées.
Les technologies développées pour héberger des services Internet peuvent aussi être déployées au sein d'une entreprise. Pour ce faire, vous pouvez créer un réseau intranet pour tirer parti des avantages des services Internet au sein du réseau de l'entreprise.
Vous devez également comprendre comment les ordinateurs trouvent les adresses des autres ordinateurs connectés à Internet pour leur envoyer des informations. L'adressage des ordinateurs sur Internet est effectué en utilisant un système de dénomination convivial appelé dénomination de domaine.

2. Internet



Un nombre très important de grandes entreprises, d'universités et d'administrations, ainsi que des millions de particuliers, placent des informations sur Internet pour les partager avec le public.

2.1. Structure d'Internet

Internet permet à des personnes du monde entier d'échanger des informations sur leurs ordinateurs, à savoir du texte, des documents de traitement de texte, des images, des vidéos, des sons et des programmes informatiques. Même si certaines entreprises peuvent développer des outils ou des programmes destinés à Internet, aucun individu ni aucune entreprise ne contrôle ni ne régit Internet. Toutefois, des entreprises privées possèdent la *dorsale* d'Internet (le support physique sur lequel le trafic Internet est généré).
Les ordinateurs connectés à Internet utilisent une architecture de type client-serveur. En d'autres termes, un serveur distant transmet des fichiers et des services à l'ordinateur client local de l'utilisateur. La vitesse à laquelle l'ordinateur client peut accéder aux services fournis par le serveur dépend de la technologie utilisée. Grâce aux améliorations technologiques permanentes, la vitesse et les mécanismes d'accès sont de plus en plus performants et permettent de télécharger, ou de récupérer, rapidement des quantités d'informations importantes à partir du serveur.

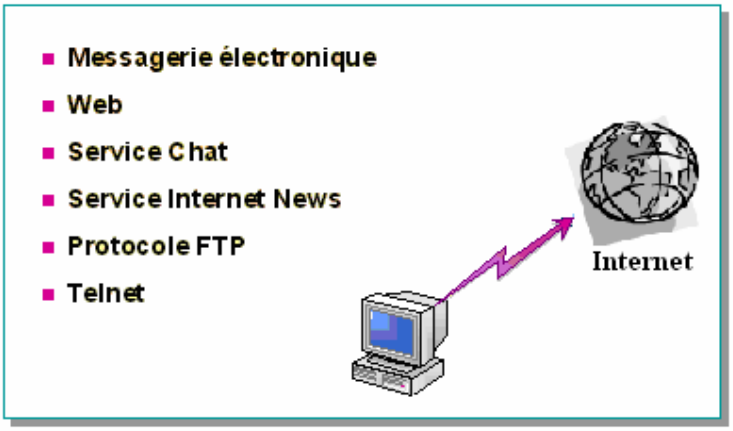
2.2. Protocole TCP/IP

Le protocole TCP/IP est la pile de protocoles standard utilisée pour établir des communications sur Internet. La pile de protocoles TCP/IP est composée des protocoles de niveau inférieur TCP et IP et de protocoles de niveau supérieur comme les protocoles HTTP (*Hypertext Transfer Protocol*), FTP (*File Transfer Protocol*) et SMTP (*Simple Mail Transfer Protocol*). Les protocoles TCP et IP fournissent des fonctionnalités de bas niveau nécessaires à de nombreuses applications, alors que les protocoles HTTP, FTP et SMTP permettent d'accéder aux services de niveau supérieur, par exemple le transfert de fichiers entre des ordinateurs, l'envoi de courrier électronique ou l'identification de la personne qui a ouvert une session sur un autre ordinateur. En raison de la large gamme de ses fonctions, vous devez donc installer et configurer le protocole TCP/IP sur tous les ordinateurs qui accèdent à Internet.

2.3. Adresses publiques et privées

Outre le fonctionnement du protocole TCP/IP, vous devez donc également savoir comment les ordinateurs sont affectés d'adresses IP pour accéder à Internet. Les adresses IP sont allouées par un organisme appelé IANA (*Internet Assigned Numbers Authority*). Les adresses allouées par cet organisme peuvent recevoir du trafic à partir d'autres sites Internet, et sont appelées adresses publiques. Pour la plupart des particuliers et des petites entreprises standard, les adresses publiques sont allouées par un *fournisseur de services Internet* (ISP, *Internet Service Provider*), c'est-à-dire une société qui gère une plage d'adresses publiques, et offre des accès à Internet.
Pour que plusieurs ordinateurs d'une petite entreprise puissent communiquer sur Internet, chacun d'eux doit disposer de sa propre adresse publique. La demande d'adresses publiques est supérieure au nombre d'adresses publiques disponibles qui peuvent être allouées. Pour résoudre cette lacune, l'organisme IANA a mis en place un système de réutilisation des adresses, qui consiste à réserver des groupes d'adresses IP, appelées adresses privées, aux réseaux privés connectés à Internet. Les adresses privées ne peuvent pas recevoir directement du trafic à partir des sites connectés à Internet.

3. Services Internet



Les services Internet les plus utilisés sont la messagerie électronique, le Web, le service Chat, le service Internet News, le protocole FTP et Telnet.

- **Messagerie électronique**

La messagerie électronique est le service Internet le plus utilisé. Elle permet d'envoyer des messages à tout utilisateur connecté à Internet.

- **Web**

Le Web est le terme qui décrit l'ensemble des documents hypertexte et des contenus multimédias, reliés par des liens, disponibles sur Internet. Les documents hypertexte sont des fichiers qui sont mis en forme pour être utilisés sur Internet. Pour rechercher, repérer, afficher et télécharger des informations à partir d'Internet, vous devez utiliser un navigateur Web, par exemple Microsoft Internet Explorer.

- **Service Chat**

Les programmes Chat vous permettent de participer à des discussions en temps réel avec une ou plusieurs personnes sur Internet.

- **Service Internet News**

Internet News est un service qui héberge de groupes de discussion électronique par le biais desquels les participants peuvent partager des informations et des opinions. Un client de News, par exemple Microsoft Outlook® Express, permet d'accéder à ces groupes.

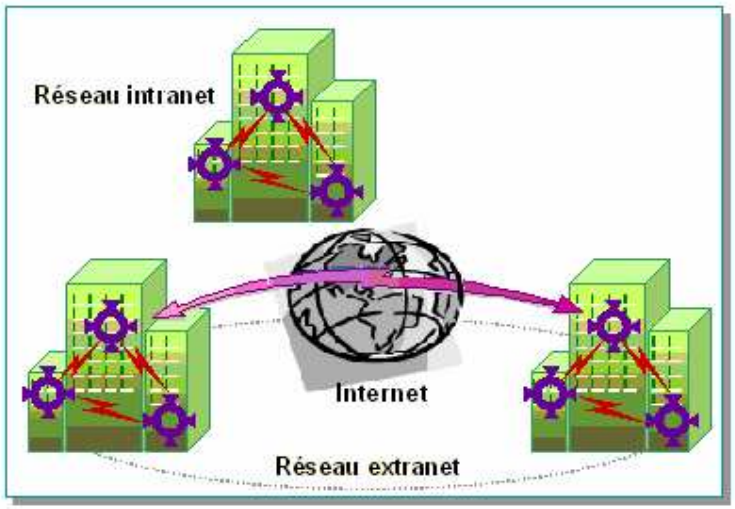
- **Protocole FTP**

Le protocole FTP est un service, comprenant un serveur, qui permet de transférer des fichiers du serveur à un ordinateur client. Les utilisateurs peuvent télécharger des fichiers à partir du serveur FTP à l'aide d'un utilitaire client FTP.

- **Telnet**

Telnet permet d'ouvrir une session à distance sur un ordinateur, puis de travailler sur cet ordinateur. En ouvrant une session à distance sur cet ordinateur, les utilisateurs peuvent accéder à des services ou à des ressources dont ils ne disposent pas sur leur poste de travail.

4. Réseaux intranets



Vous pouvez déployer les technologies développées pour Internet sur un réseau local (LAN, *Local Area Network*), afin d'y diffuser des informations, par exemple des mises à jour d'un catalogue ou des informations d'une base de données. Pour ce faire, vous devez installer le logiciel serveur Internet sur l'un des serveurs du réseau local.

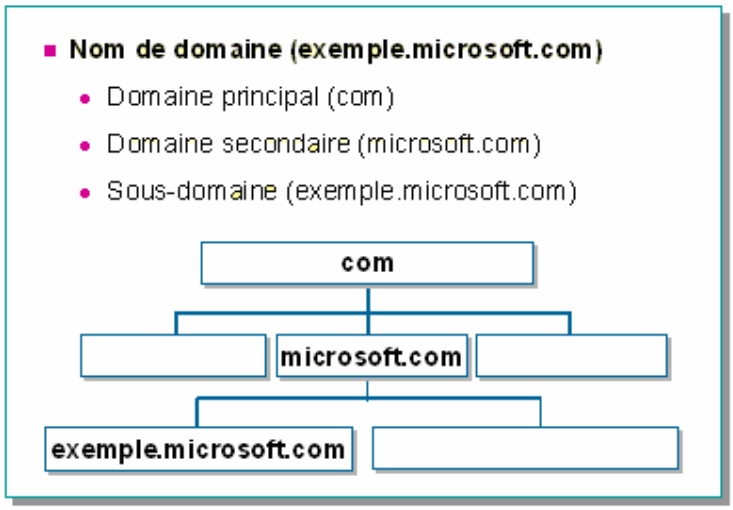
4.1. Définition d'un réseau intranet

Un réseau *intranet* est un réseau, interne à une entreprise, qui utilise les technologies Internet pour améliorer les communications internes, publier des informations ou développer des applications. Pour utiliser les applications Internet gratuites ou peu onéreuses sur un réseau intranet, chacun des ordinateurs du réseau doit prendre en charge le protocole TCP/IP. Un réseau intranet peut être privé, auquel cas il n'est pas connecté à Internet, ou public, auquel cas il l'est.

4.2. Extension des réseaux intranet en un réseau extranet

Vous souhaitez permettre à des utilisateurs autorisés figurant au nombre de vos clients, distributeurs, fournisseurs et autres partenaires, d'accéder à votre réseau intranet. Par exemple, une société souhaite partager des informations professionnelles avec ses distributeurs et ses clients en leur accordant un droit d'accès limité à son réseau intranet. Internet vous permet d'étendre l'accès au réseau intranet à des utilisateurs autorisés. Ce type de réseau intranet, partiellement accessible aux seuls utilisateurs autorisés, par le biais d'Internet est appelé réseau *extranet*. Il est plus facile et plus économique d'installer un réseau extranet par le biais d'Internet que d'installer une liaison de communication dédiée entre deux entreprises. Toutefois, un réseau extranet est moins sécurisé qu'un réseau intranet privé, car des utilisateurs non autorisés peuvent y accéder.

5. Dénomination de domaine



Des millions d'ordinateurs sont connectés à Internet. Il était donc nécessaire de disposer d'un système d'adressage offrant une méthode facilement mémorisable pour les repérer. Un nom de domaine satisfait à cette demande. Il utilise en effet des noms conviviaux et non de longs numéros.

5.1. Noms de domaine

L'adresse utilisée au niveau des ordinateurs pour identifier de façon unique un ordinateur particulier sur Internet est appelée adresse IP. Une adresse IP est composée de quatre ensembles de numéros, séparés par des points. Par exemple : 131.107.1.7 .
Si une application n'a aucune difficulté avec ce système d'adressage numérique, pour les utilisateurs, il est en revanche plus facile de mémoriser des noms de domaine conviviaux, par exemple .microsoft.com. Toutefois, pour qu'un ordinateur puisse se connecter à Internet, il est

nécessaire de mapper, ou de résoudre, son nom de domaine sur une adresse IP unique. Un système de classification, appelé système de nom de domaine (DNS, *Domain Name System*) mappe les noms de domaine sur des adresses IP. Lorsque vous utilisez un nom de domaine pour vous connecter à un ordinateur sur Internet, un serveur DNS résout ce nom en adresse IP. Le serveur utilise le mappage pour trouver l'adresse IP de l'ordinateur cible, et la substitue au nom convivial pour établir une connexion à l'ordinateur sur Internet.

Le système DNS identifie de façon unique les ordinateurs connectés à Internet en fonction d'une hiérarchie qui comprend un domaine principal, un domaine secondaire, et souvent un ou plusieurs sous-domaines. Le domaine principal est basé sur des codes génériques ou sur des codes de pays. Les domaines principaux génériques indiquent le type de l'entreprise. Le tableau suivant répertorie les domaines principaux génériques et les types d'entreprises qui leur correspondent :

Code générique	**Description**
com	Entreprises commerciales
edu	Enseignement
gov	Administrations américaines
int	Associations internationales
mil	Organisations militaires américaines
net	Centres assurant le support technique du réseau
org	Autres organisations

Les domaines principaux basés sur des codes de pays sont des codes à deux lettres, par exemple MA pour le Maroc. Le tableau suivant répertorie quelques exemples de domaines principaux basés sur des codes de pays, et les pays auxquels ils correspondent :

Code de pays	**Pays**
ar	Argentine
au	Australie
be	Belgique
br	Brésil
ca	Canada
dz	Algérie

Le domaine secondaire représente le nom d'une entreprise, d'une institution ou d'une organisation. Il est séparé du nom de domaine principal par un point (appelé « dot »). microsoft.com est un exemple de domaine secondaire. Un particulier ou une petite entreprise utilisent en général un nom de domaine et une adresse IP, mais les grandes entreprises achètent souvent un groupe d'adresses IP et créent des sous-domaines. Par exemple, microsoft.com est un nom de domaine, et exemple.microsoft.com est un sous-domaine du domaine principal de Microsoft.
L'ICANN (*Internet Corporation for Assigned Names and Numbers*) est l'organisme chargé de gérer l'affectation des noms de domaine.

5.2. Les URLs

Internet donne accès à un grand nombre de choses différentes: un serveur (c'est-à-dire un ordinateur), une boîte aux lettres (c'est-à-dire une personne), ou encore des données (c'est-à-dire de l'information). Il est donc nécessaire de disposer d'un moyen de contacter quoi que ce soit de disponible sur Internet. Ce moyen est donné par ce que l'on appelle en anglais «*Uniform Resource Locator*», et abrégée URL. Dans le public, le terme «adresse Internet» est souvent utilisé abusivement pour dénoter un URL.

Pour différencier un URL du texte environnant, on utilise la notation en vigueur sur Internet: chaque URL est placé entre les signes < (plus petit que) et > (plus grand que). Ces délimiteurs ne font pas partie de l'URL. Lors de l'utilisation d'une telle adresse, il est important de ne pas taper les symboles < et >.

Voici quelques exemples d'URLs, avec une description de ce qu'ils désignent:

<http://host.domain.org/repertoire/index.html>: une page WWW

<mailto:errachidi.rachid@menara.ma>: une adresse de boîte aux lettres (e-mail)

<ftp://ftphost.domain.org/>: un serveur FTP

<news:comp.sys.mac.programmer.tools>: un forum de discussion

Un URL permet donc de désigner des choses complètement différentes. La principale différence est la première partie: «http://», «mailto:», «ftp://», «news:» ou encore «file://». Cette partie permet de savoir quel protocole ou quel programme est adéquat pour traiter chaque cas. Il est parfois nécessaire de préciser le chemin d'accès du service ou du fichier, à la suite du nom de l'hôte. Il faut alors séparer les dossiers (ou répertoires) par des barres obliques (/ = slash en anglais).

Les URLs les plus utilisés sont :

URLs Web : Les URLs les plus connus sont ceux désignant une page Web. Le préfixe «http://», indique l'emploi du protocole HTTP (acronyme de «HyperText Transfer Protocol»). Suit l'adresse nominale de l'hôte sur lequel est stocké le site, puis le dossier (répertoire) dans lequel se trouve ce site et enfin le nom du fichier correspondant à la page d'accueil (chemin d'accès du fichier = «path»). Dans l'exemple ci-dessus, l'hôte est «host.domain.org», le dossier est «repertoire» et la page d'accueil s'appelle «index.html».

URLs e-mail : Les URLs correspondant aux boîtes aux lettres des utilisateurs du courrier électronique sont préfixés par «mailto:». Le reste de l'adresse e-mail est composé de deux parties, séparées par le signe typographique @. Ce signe, appelé en anglais «at symbol» correspond à la préposition anglaise «at» (chez, à). On l'appelle en français «arobace».

La partie de l'adresse située après le @ représente le nom de l'hôte où est situé la boîte aux lettres (dans l'exemple ci-dessus, «menara.ma»). D'habitude, ce nom correspond au nom de domaine, soit il a un rapport avec la raison sociale de l'hôte.

La partie située avant le @ constitue le nom unique de l'utilisateur de la boîte aux lettres. Comme il s'agit d'une personne physique la plupart du temps, il est judicieux de conserver la structure du prénom et du nom pour cet identificateur.

URLs FTP : Les URLs des sites permettant le transfert de fichiers par FTP ont la même syntaxe que les URLs Web. Seule l'entête est différente, «ftp://» à la place de «http://».

Le chemin d'accès du fichier à télécharger est mis à la suite du nom de l'hôte, ici encore avec des barres obliques pour séparer les dossiers.

URLs News : Pour accéder aux messageries, on utilise des URLs formés de l'entête «news:». La suite de l'adresse est constituée du nom du forum de discussion choisi. Dans l'exemple ci-dessus, le forum s'appelle «comp.sys.mac.programmer.tools».

II. Les serveurs Web

1. Introduction

Il ne fait plus de doute pour personne, aujourd'hui, qu'une entreprise (ou un établissement d'enseignement, une association, etc.) doit être vue sur Internet, et donc posséder un site Web. La création d'un tel site, d'ailleurs, n'est pas très compliquée, si l'on est assez raisonnable pour commencer de manière simple, en se limitant à une taille modeste.
Le site Web étant créé à l'aide d'un éditeur adéquat, il faut le mettre en ligne sur un serveur spécialisé fonctionnant en permanence. Les organismes qui possèdent déjà un réseau local raccordé à Internet via une passerelle ou un routeur choisiront généralement d'installer leur propre serveur Web intra muros. Les entreprises qui ne possèdent pas de liaison permanente à Internet confieront généralement l'hébergement de leur site Web à un prestataire de service.
Quand elle le peut sans surcoût important, l'entreprise a intérêt à héberger elle-même son site Web, de manière à en garder la maîtrise, et à le gérer comme elle l'entend.

2. L'offre de logiciel serveur Web

2.1. Qu'est-ce qu'un serveur Web ?

Un serveur HTTP ou démon HTTP ou HTTPd (HTTP daemon) ou (moins précisément) serveur Web, est un logiciel servant des requêtes respectant le protocole de communication client serveur HTTP, qui a été développé pour le World Wide Web.
Un ordinateur sur lequel fonctionne un serveur HTTP est appelé serveur Web. Le terme « serveur Web » peut aussi désigner le serveur HTTP (le logiciel) lui-même. Les deux termes sont utilisés pour le logiciel car le protocole HTTP a été développé pour le Web et les pages Web sont en pratique toujours servies avec ce protocole. D'autres ressources du Web comme les fichiers à télécharger ou les flux audio ou vidéo sont en revanche fréquemment services avec d'autres protocoles.

2.2. Les principaux éditeurs

Les serveurs HTTP les plus utilisés sont :
• Apache HTTP Server de la Apache Software Foundation, successeur du NCSA httpd
• Internet Information Services de Microsoft (IIS)
• Sun ONE de Sun Microsystems (anciennement iPlanet de Netscape Communications Corporation)
• Le serveur Web Zeus de Zeus Technology
Le plus populaire est Apache HTTP Server qui sert environ 69% des sites Web en octobre 2005 selon Netcraft.

2.3. Apache

Les logiciels serveurs d'Apache font partie de l'open source, ce qui signifie en pratique que leur code source est disponible gratuitement. Les versions les plus utilisées fonctionnent sous Unix Il existe aussi des versions toutes prêtes pour Windows NT, mais elles n'ont pas très bonne réputation (étant peu utilisées, elles sont corrélativement mal déboguées). Apache est systématiquement utilisé pour les serveurs Web qui assurent un très gros trafic, et ceux qui hébergent un grand nombre de sites.

2.4. Internet Information Server

Internet Information Server (IIS) est le principal logiciel serveur Web de l'éditeur Microsoft. La version 2, assez rudimentaire, faisait partie de Windows NT4 Server, mis sur le marché en 1996. Une mise à jour vers la version 3 a été offerte gratuitement en 1997 avec un "Service Pack". La version 4 a été publiée en 1998 sous le titre "Option Pack". La version 5 est

intégrée à Windows 2000 Server, disponible depuis février 2000. Enfin Microsoft propose dans toutes les versions de Windows 2003 Server une nouvelle version des IIS, la version 6.0. Depuis la version 4, IIS est considéré comme un bon produit, possédant sur Apache l'avantage d'être prêt à l'emploi (pas de code à compiler), mais l'inconvénient d'être payant. Sa mise en oeuvre ne requiert pas la présence d'un informaticien professionnel.

3. Le choix du logiciel

Ce sont surtout des considérations de coût et de compétences qui guide les entreprises à choisir un serveur Web ou un autre. Le choix de la plate-forme, et celui du système d'exploitation, sont étroitement liés au choix du logiciel serveur Web. Ainsi, IIS ne fonctionne que sur Windows. Apache, pour sa part, est pratiquement toujours utilisé avec le système d'exploitation Unix.

III. Installer un serveur Web avec IIS sous XP

1. Présentation

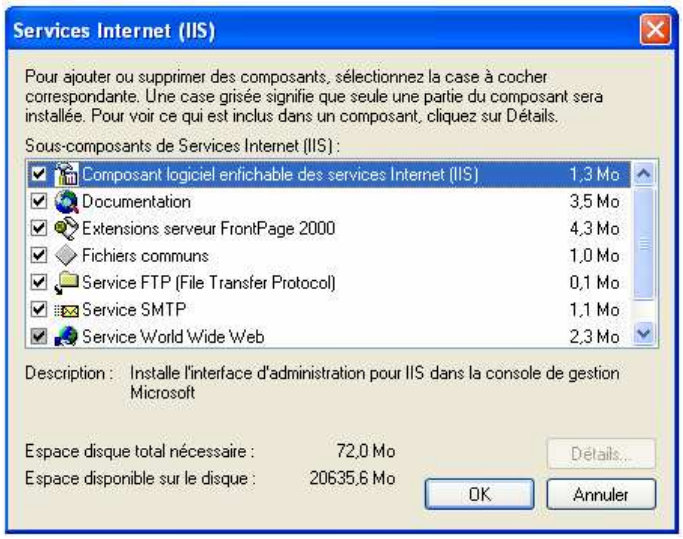
IIS est l'abréviation de Internet Information Server. Il s'agit d'un ensemble d'outils de communication qui regroupe un ensemble de serveurs :
Un serveur Web : HTTP
Un serveur de news : NNTP
Un serveur d'envoi de mails (ou de routage de mail) : SMTP
Un langage de programmation pour le serveur Web : ASP (Active Server Page).
Un générateur de certificats SSL (sites Web sécurisés)
Et enfin un serveur FTP.
C'est le premier et le dernier que nous allons mettre en œuvre dans ce cours.

2. Installation des composants de IIS

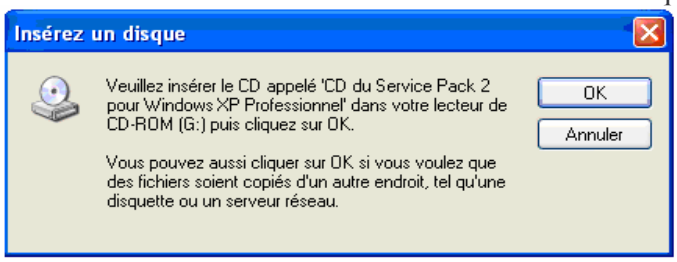
Vous devez tout d'abord installer le service IIS si vous ne l'avez pas déjà fait.
Pour cela rendez-vous dans le " **Panneau de configuration** ", puis " **Ajout/Suppression de programmes** ".

Puis cliquez sur " **Ajouter ou supprimer des composants Windows** ", vous obtenez alors la fenêtre ci-dessous :

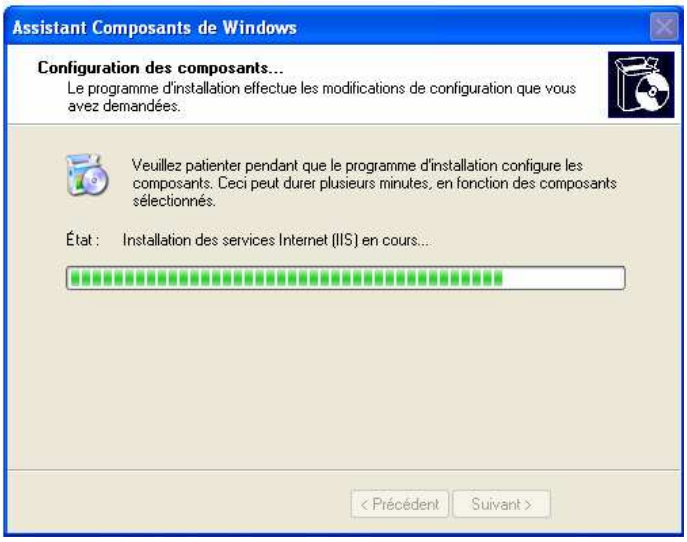
Cochez la case en face de " **Services Internet** " et cliquez sur le bouton " **Détails...** " pour vérifier que les bons composants sont sélectionnés.



L'installation de tous les composants n'est pas nécessaire, seuls les " **Composant logiciel enfichable des services Internet** " (obligatoire), " **Service World Wide Web** " et " **Service FTP** " nous intéressent.
N'oubliez pas de vous munir de votre CD d'installation de Windows et cliquez sur " **OK** ".



Insérez votre CD dans le lecteur afin que Windows récupère les fichiers nécessaires et cliquez sur " **OK** ".

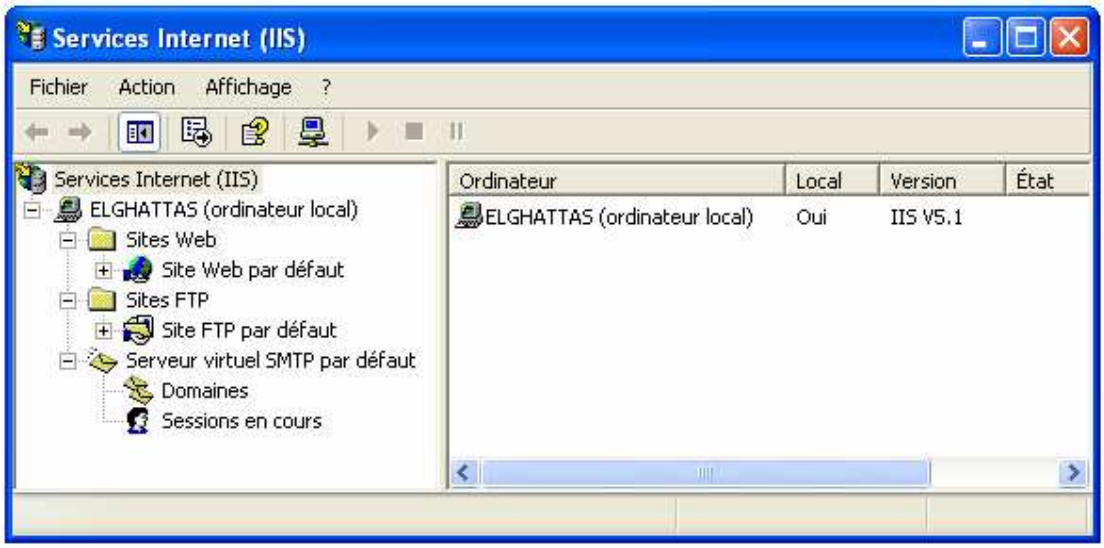


Le service s'installe...

Cliquez sur " **Terminer** ", le service est installé !

3. Configuration du serveur

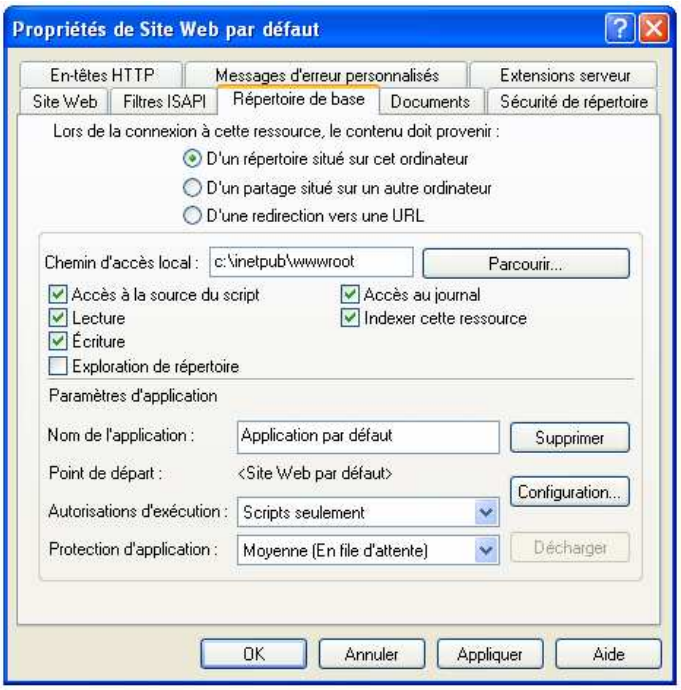
Pour configurer le serveur, car il ne suffit pas de l'installer, rendez-vous dans le " **Panneau de configuration** ", ouvrez les " **Outils d'administration** " et exécutez l'icône nommée " **Services Internet (IIS)** ".



Nous pouvons voir que dans la liste figure le nom de votre ordinateur, qui est maintenant un serveur HTTP, il n'est certes pas encore paramétré mais nous y arrivons...

Affichez les propriétés du " **Site Web par défaut** " par un clic droit dessus puis " **Propriétés** ".

3.1. Répertoire de base



L'onglet par lequel il vous faudra passer en premier est **Répertoire de base** où l'on peut modifier le répertoire ou le lecteur qui contient le site.

Chemin d'accès local

Par défaut le répertoire du serveur Web (c'est-à-dire le répertoire où vous placez les pages que vous voulez rendre disponibles par le serveur) est **C:\Inetpub\wwwroot** mais vous pouvez le modifier en choisissant n'importe quel autre répertoire. Trois possibilités sont offertes:

- Un répertoire local (chemin défini dans la zone "Chemin local", actuellement C:\Inetpub\wwwroot).
- Un répertoire partagé par un autre ordinateur (nom du partage défini dans la zone "Chemin local" sous la forme \\serveur\partage).
- Une redirection vers une URL (URL définie dans la zone "Chemin local" sous la forme http://adresseInternet). Le site Web redirige ainsi les requêtes qui lui sont adressées vers un autre site Web.

Si votre site Web contient des fichiers placés sur un lecteur autre que celui du répertoire de base ou sur un ordinateur autre que celui qui exécute les services Internet, vous devez créer des répertoires virtuels de manière à pouvoir inclure ces fichiers dans votre site Web. Pour utiliser un répertoire situé sur un autre ordinateur, vous devez spécifier le nom UNC (Universal Naming Convention) du répertoire et fournir un nom d'utilisateur et un mot de passe qui seront utilisés pour les autorisations d'accès.

Pour créer un répertoire virtuel

1. Dans le composant logiciel enfichable Services Internet (IIS), sélectionnez le site Web ou FTP auquel vous souhaitez ajouter un répertoire.
2. Cliquez sur le bouton **Action**, puis pointez sur **Nouveau** et sélectionnez **Répertoire virtuel.**
3. Utilisez l'Assistant **Création de répertoire virtuel** pour créer le répertoire.

Conseil : Si vous utilisez NTFS, vous pouvez également créer un répertoire virtuel comme suit : cliquez avec le bouton droit sur un répertoire dans l'Explorateur Windows, cliquez sur **Partage**, puis sélectionnez la feuille de propriétés **Partage Web**.

Pour supprimer un répertoire virtuel

1. Dans le composant logiciel enfichable Services Internet (IIS), sélectionnez le répertoire virtuel que vous souhaitez supprimer.
2. Cliquez sur le bouton **Action** et sélectionnez **Supprimer**. La suppression d'un répertoire virtuel n'entraîne pas celle du répertoire et des fichiers physiques correspondants.

Remarque : Dans IIS 3.0, tout répertoire virtuel non associé à une adresse IP spécifique était accessible à partir de tous les sites Web hébergés sur le serveur. Dans IIS 4.0 et 5.0, cette fonctionnalité a été modifiée afin que tout répertoire virtuel puisse être accessible à partir de plusieurs sites Web utilisant des adresses IP différentes. Pour rendre un répertoire virtuel accessible à partir de plusieurs sites Web utilisant des adresses IP différentes, vous devez maintenant ajouter le répertoire virtuel à chaque site.

Accès à la source du script

Les utilisateurs peuvent accéder aux fichiers source. Si l'autorisation **Lecture** est sélectionnée, le code source peut être lu. Si l'autorisation **Écriture** est sélectionnée, le code source peut être modifié. L'autorisation Accès à la source du script permet d'accéder au code source des fichiers, par exemple les scripts d'une application ASP. Cette option est disponible uniquement si l'autorisation **Lecture** ou **Écriture** est activée.

Lecture

En cochant cette case les utilisateurs peuvent visualiser le contenu et les propriétés des fichiers.

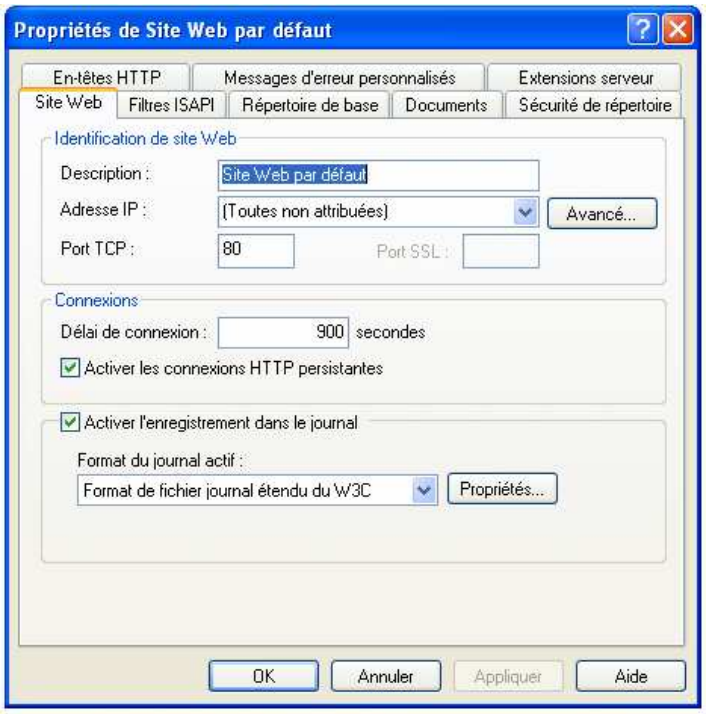
Écriture
En cochant cette case les utilisateurs peuvent modifier le contenu et les propriétés des fichiers. Si vous ne faites qu'afficher des pages (sans enregistrement), ne cochez pas la case **Écriture,** vous y gagnerez en sécurité.
Exploration de répertoire
En choisissant cette option les utilisateurs peuvent afficher une liste hypertexte des fichiers et sous répertoires de ce répertoire virtuel. Egalement par sécurité il est conseillé de décocher cette case car cela permettrait à n'importe quel visiteur de parcourir vos répertoires.
Accès au journal
Pour enregistrer les visites rendues à ce répertoire dans un fichier journal, sélectionner cette option. Les visites ne sont enregistrées que si l'enregistrement est activé pour ce site Web.
Indexer cette ressource
Sélectionner cette option permet au service d'indexation Microsoft d'inclure ce répertoire dans un index en texte intégral de votre site Web. L'indexation permet aux utilisateurs d'effectuer une recherche par mot clé afin de trouver des informations contenues dans la ressource.
Paramètres d'application
Une application IIS peut être définie comme tout fichier exécuté au sein d'un ensemble défini de répertoires dans votre site Web. Lorsque vous créez une application, vous utilisez le composant logiciel enfichable Services Internet (IIS) pour désigner le répertoire de point de départ de l'application (également appelé racine de l'application) dans votre site Web. Tous les fichiers et répertoires placés sous ce répertoire de point de départ dans votre site Web sont considérés comme faisant partie de l'application, jusqu'au prochain répertoire de point de départ rencontré. La portée d'une application est ainsi définie par les limites du répertoire.
Point de départ de l'application
Dans le composant logiciel enfichable Services Internet (IIS), le point de départ d'une application est représenté par une icône symbolisant un package. L'illustration suivante montre une application dont le répertoire de point de départ est nommé /SiteAdmin :

Les fichiers des répertoires \Login et \Order sont considérés comme faisant partie de l'application /SiteAdmin.
Un site Web peut comporter plusieurs applications. Le site Web par défaut créé lors de l'installation des services Internet (IIS) est le point de départ d'une application.
Les services Internet (IIS) prennent en charge les applications ASP, ISAPI, CGI, IDC et SSI. Une application peut partager des informations avec les fichiers de l'application. Par exemple, les applications ASP partagent le flux contextuel, l'état de session et les paramètres des variables avec les différentes pages de l'application.
Autorisations d'exécution
Permet de définir le niveau d'exécution du programme autorisé pour l'application. Il y a trois options :

- Aucune Seuls les fichiers statiques, tels que les fichiers .html ou .gif, sont accessibles.
- Scripts seulement Seuls les scripts, tels que les scripts ASP, peuvent être exécutés.
- Scripts et exécutables Tous les types de fichiers sont accessibles et peuvent être exécutés

Protection d'application :
IIS 5.0 propose trois niveaux de protection d'application. La protection d'application fait référence au processus dans lequel les applications sont exécutées. Dans IIS 4.0, il était possible de définir les applications de telle sorte qu'elles soient exécutées dans le même processus que les services Web (Inetinfo.exe) ou dans un processus distinct (DLLHost.exe). IIS 5.0 dispose d'une troisième possibilité : les applications peuvent être exécutées dans un processus mis en pool (autre instance de DLLHost.exe).
Ces différentes options fournissent des niveaux variables de protection pour les situations dans lesquelles une application présentant un dysfonctionnement peut échouer et faire que le processus dans lequel elle est exécutée cesse de répondre. Par défaut, les services Web (Inetinfo.exe) s'exécutent dans leur propre processus et les autres applications s'exécutent dans un processus mis en pool unique (DLLHost.exe). Vous pouvez ensuite définir l'exécution des applications à priorité élevée en tant que processus isolés (autre instance de DLLHost.exe). Pour des raisons de performances, il est déconseillé d'exécuter plus de 10 applications isolées.

3.2. Site Web



L'onglet **Site Web** permet de définir les paramètres d'identification de votre site Web.
Description
Tapez n'importe quel nom pour le nom du serveur. Ce nom apparaît dans l'arborescence du composant logiciel enfichable IIS.
Cliquez sur le bouton **Avancé** pour configurer l'adresse IP, le numéro de port TCP et le nom d'entête de l'hôte.
Adresse IP
Pour qu'une adresse apparaisse dans cette zone, son utilisation sur cet ordinateur doit déjà avoir été définie dans le Panneau de configuration. Si vous n'attribuez pas une adresse IP spécifique, le site répond à toutes les adresses IP attribuées à cet ordinateur et non attribuées aux autres sites, ce qui fait de celui-ci le site Web par défaut.

Port TCP
Détermine le port sur lequel le service fonctionne. Le port par défaut est 80. Vous pouvez remplacer cette valeur par tout numéro de port TCP unique. Cependant, les clients doivent savoir à l'avance qu'ils doivent demander ce numéro de port, sinon leurs requêtes pour se connecter à votre serveur échouent.
Ainsi si l'adresse de votre site est http://196.206.1.2, et que vous avez choisi comme port TCP le port 2006 il faudra utiliser la syntaxe suivante : http://196.206.1.2:2006 pour se connecter à votre site.
Port SSL
Pour spécifier le port utilisé pour le cryptage SSL (Secure Socket Layer), tapez le numéro de port dans cette zone. Vous pouvez remplacer le numéro de port par tout numéro de port unique. Cependant, les clients doivent savoir à l'avance qu'ils doivent demander ce numéro de port, sinon leurs requêtes pour se connecter à votre serveur échouent. Un numéro de port SSL n'est requis que si le cryptage SSL est utilisé.
Délai de connexion
Définit la durée en secondes avant que le serveur ne déconnecte un utilisateur inactif. Cette option garantit la fermeture de toutes les connexions dans le cas où le protocole http ne fermait pas une connexion.
Activer les connexions HTTP persistantes
Permet de maintenir la connexion ouverte pour exécuter plusieurs requêtes HTTP, par exemple lorsqu'un navigateur charge dans sa fenêtre une page qui comporte plusieurs éléments graphiques. Les connexions persistantes sont activées par défaut et il n'est, sauf à de très rares exceptions, pas judicieux de désactiver celles-ci.
Activer l'enregistrement dans le journal
Sélectionnez cette option pour activer les fonctionnalités d'enregistrement de votre site Web, lesquelles peuvent enregistrer des détails sur l'activité utilisateur et créez des journaux au format souhaité. Après avoir activé l'enregistrement dans le journal, sélectionnez un format dans la liste **Format de journal actif**.

Format de journal actif :

- Le format Microsoft IIS : il est non personnalisable et enregistre des informations spécifiques telles que le temps de chargement d'un élément, le nombre d'octets envoyés, … Il s'agit d'un format ASCII avec séparateur.
- Le format NSCA est un format fixe, non personnalisable. Son intérêt réside dans son standard et sa compatibilité avec d'autres logiciels serveurs Web.
- Le format étendu W3C. Il s'agit d'un format personnalisable et donc d'un emploi plus souple que les 2 précédents. Pour personnaliser celui-ci il convient d'accéder à la boite de dialogue Propriétés du journal étendu de la feuille de propriétés du site Web. Il est dès lors possible de sélectionner les champs qui apparaîtront ou non dans le journal.
- Journal ODBC (Disponible uniquement avec les Windows Server) Format fixe enregistré dans une base de données.

Il est possible de préciser à IIS la façon dont il doit créer de nouveaux journaux plutôt que d'ajouter des enregistrements à ceux existants. Il existe 3 critères principaux :

- La période : tous les jours, toutes les semaines ou tous les mois.
- La taille : une fois la taille atteinte, un nouveau journal est créé.
- L'unicité : 1 seul journal est créé, les données sont alors toujours ajoutées à ce dernier. Ce fichier n'est accessible qu'après arrêt du site.

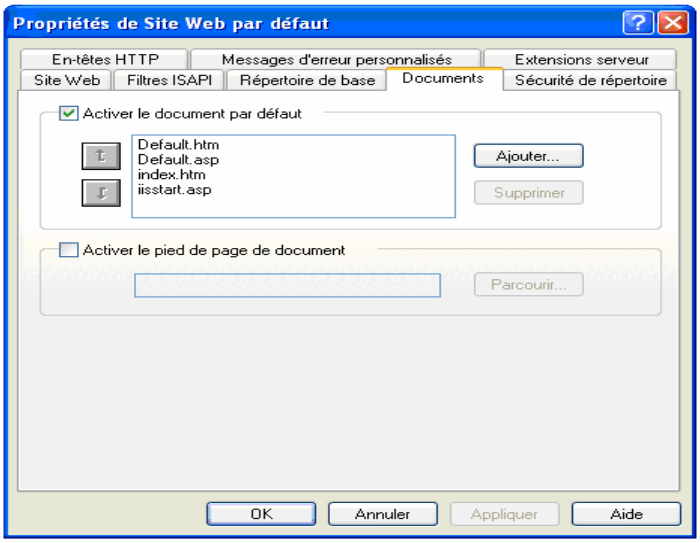
Le nom du journal a trait à son type et au mode d'enregistrement choisit, ainsi :

- Un fichier Microsoft IIS a pour préfixe **in** pour un enregistrement sur une période ou inetsv pour un enregistrement selon la taille.
- Un fichier NCSA a pour préfixe **nc** pour un enregistrement sur une période ou **ncsa** pour un enregistrement selon la taille.
- Un fichier W3C étendu a pour préfixe **ex** pour un enregistrement sur une période ou **extend** pour un enregistrement selon la taille.
- Un fichier dont l'enregistrement porte sur la journée aura un suffixe de type **aammjj**.
- Un fichier dont l'enregistrement porte sur la semaine aura un suffixe de type **aammss** ou **ss** est le N° de la semaine.
- Un fichier dont l'enregistrement porte sur le mois aura un suffixe de type **aamm**.
- Un fichier dont l'enregistrement est fonction de la taille aura comme suffixe un N° d'ordre **nn** séquentiel.

Ce qui donne en final des exemples de ce type :

- inetsv03.log IIS / mode fonction de la taille.
- NC991231 NCSA / mode enregistrement quotidien.

3.3. Documents



Dans cet onglet-ci, vous pouvez spécifier le nom des pages lues par défaut.

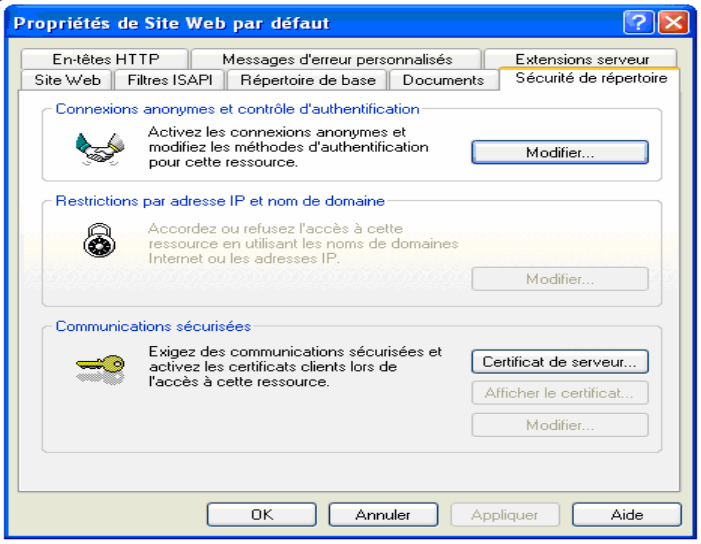
Activer le document par défaut

Pour prendre en charge un document par défaut chaque fois qu'une demande de navigateur ne spécifie pas le nom de document, activer cette case à cocher. Les documents par défaut peuvent être la page d'accueil d'un répertoire ou une page d'index contenant une liste des répertoires de documents du site.

- Pour ajouter un nouveau document par défaut, cliquez sur **Ajouter**. Vous pouvez utiliser cette fonctionnalité pour spécifier plusieurs documents par défaut. Les documents par défaut sont pris en charge dans l'ordre d'apparition des noms dans la liste. Le serveur renvoie le premier document trouvé.
- Pour modifier l'ordre de recherche, sélectionnez un document et cliquer sur les fichiers.
- Pour supprimer un document par défaut de la liste, cliquez sur **Supprimer**.

Activer le pied de page de document
Pour ajouter automatiquement un pied de page au format HTML à chaque document envoyé par votre serveur Web, sélectionner cette option. Le fichier de pied de page ne doit pas être un document HTML complet. Il doit contenir uniquement les balises HTML nécessaires à la mise en forme de l'apparence et de la fonction du contenu du pied de page.
Pour spécifier le chemin d'accès complet et le nom de votre fichier de pied de page cliquez sur **Parcourir**.

4. Sécurité de répertoire



L'onglet **Sécurité de répertoire** permet de définir les fonctionnalités de sécurité de votre serveur Web.
Connexions anonymes et contrôle d'authentification
Cette fonctionnalité présente la méthode de contrôle d'accès aux sites Web la plus courante. Elle permet à tout le monde de visiter les zones publiques de vos sites Web, tout en empêchant les utilisateurs non autorisés d'accéder aux fonctionnalités d'administration et aux informations personnelles sensibles de votre serveur Web.
Lorsque vous configurez un accès anonyme sur votre serveur Web, vous pouvez appliquer des autorisations NTFS afin d'empêcher les utilisateurs ordinaires d'accéder aux fichiers et aux répertoires confidentiels. On rappelle que les différents niveaux d'autorisation NTFS sont les suivants :

- **Contrôle total** Les utilisateurs peuvent modifier, ajouter, déplacer ou supprimer des fichiers (ainsi que leurs propriétés) ou des répertoires. En outre, ils peuvent modifier les paramètres d'autorisation pour tous les fichiers et sous répertoires.
- **Modifier** Les utilisateurs peuvent visualiser et modifier les fichiers et les propriétés des fichiers. Ils peuvent par exemple supprimer ou ajouter des fichiers dans un répertoire ou des propriétés de fichier dans un fichier.
- **Lecture et exécutables** Les utilisateurs peuvent exécuter des fichiers exécutables, par exemple des scripts.
- **Afficher le contenu des dossiers** Les utilisateurs peuvent afficher une liste du contenu d'un dossier.
- **Lecture** Les utilisateurs peuvent visualiser les fichiers et les propriétés des fichiers.
- **Écriture** Les utilisateurs peuvent écrire dans un fichier.

Par défaut, votre serveur Web connecte tous les utilisateurs à l'aide du compte anonyme. Au cours de l'installation, votre serveur crée un compte d'utilisateur anonyme particulier appelé IUSR_nomordinateur. Les sites Web de votre serveur peuvent utiliser le même compte d'utilisateur d'ouverture de session anonyme, ou bien des comptes différents. Grâce à l'utilitaire Utilisateurs et groupes locaux, vous pouvez créer un nouveau compte d'utilisateur « d'ouverture de session anonyme ».

Restrictions par adresse IP et nom de domaine

Cette fonctionnalité, disponible uniquement pour les installations Windows Server, permet de configurer votre serveur Web de manière à empêcher des ordinateurs, des groupes d'ordinateurs ou des réseaux entiers d'accéder au contenu de votre serveur Web. Lorsqu'un utilisateur essaie d'accéder pour la première fois au contenu de votre serveur Web, le serveur confronte l'adresse IP de l'ordinateur de l'utilisateur avec les paramètres de restriction relatifs aux adresses IP du serveur.

Communications sécurisées

Pour créer une demande de certificat de serveur à l'aide du nouvel Assistant Certificat, cliquez sur **Certificat de serveur….**Vous ne pouvez utiliser les fonctionnalités de communications sécurisées de votre serveur Web avant d'avoir installé un certificat de serveur valide.

Rappel

Les certificats : ce sont des documents d'identification numériques qui permettent aux serveurs et aux clients de s'authentifier mutuellement. Ils sont exigés par le navigateur du client et du serveur pour établir une connexion SSL permettant de transmettre des informations cryptées. Dans IIS, les fonctionnalités SSL basées sur des certificats comprennent un certificat serveur, un certificat client et plusieurs clés numériques. Vous pouvez créer ces certificats à l'aide des services de certificats Microsoft ou vous les procurer auprès d'une organisation tierce de confiance appelée autorité de certification.

Certificats serveurs : Les certificats serveurs permettent aux utilisateurs de confirmer l'identité de votre site Web. Un certificat serveur contient des informations d'identification détaillées, telles que le nom de l'organisation affiliée au contenu du serveur, le nom de l'organisation ayant émis le certificat et une clé publique permettant d'établir une connexion cryptée. Ces informations permettent de garantir aux utilisateurs l'authenticité du contenu du serveur Web, ainsi que l'intégrité de la connexion HTTP sécurisée.

Certificats clients : Avec SSL, votre serveur Web a également la possibilité d'authentifier les utilisateurs en vérifiant le contenu de leur certificat client. Généralement, un certificat client contient des informations d'identification détaillées sur un utilisateur et sur l'organisation ayant émis le certificat, ainsi qu'une clé publique. Vous pouvez associer l'authentification par certificat client avec le cryptage SSL pour implémenter une méthode de vérification de l'identité des utilisateurs très sécurisée.

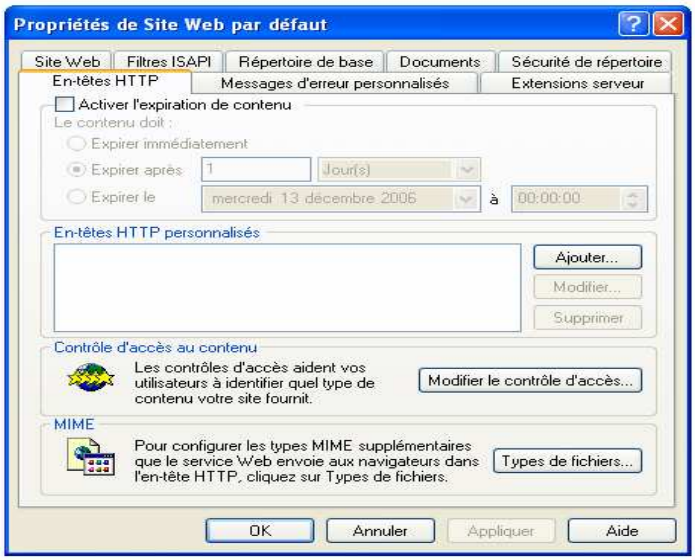
Cryptage : Vous pouvez permettre aux utilisateurs d'échanger des informations personnelles avec votre serveur (par exemple, des numéros de carte de crédit ou des numéros de téléphone) de manière sécurisée en utilisant le cryptage. Le cryptage consiste à « brouiller » les informations avant de les envoyer, et le décryptage à déchiffrer ces informations après les avoir reçues. La base du cryptage dans IIS est le protocole SSL 3.0, qui fournit une méthode sécurisée pour établir une communication cryptée avec les utilisateurs. SSL garantit l'authenticité du contenu de votre site Web et, si vous le souhaitez, vérifie l'identité des utilisateurs qui accèdent aux sites Web à accès limité.

Les certificats comprennent des clés permettant d'établir une connexion SSL sécurisée. Une clé est une valeur unique utilisée pour authentifier le serveur et le client lors de l'établissement

d'une connexion SSL. La clé publique et la clé privée forment une paire de clés SSL. Votre serveur Web utilise cette paire de clés pour négocier une connexion sécurisée avec le navigateur Web de l'utilisateur, pour déterminer le niveau de cryptage nécessaire pour garantir la sécurité des communications.
Pour ce type de connexion, votre serveur Web et le navigateur de l'utilisateur doivent utiliser des utilitaires de cryptage et de décryptage compatibles. Lors de l'échange, une clé de cryptage, ou de session, est créée. Votre serveur et le navigateur Web utilisent cette clé de session pour crypter et décrypter les informations transmises. Le degré, ou niveau, de cryptage de la clé de session est mesuré en bits. Plus le nombre de bits composant la clé de session est élevé, plus le niveau de cryptage et de sécurité est élevé. Bien qu'un niveau élevé de cryptage de la clé garantisse davantage de sécurité, il nécessite également davantage de ressources serveur. En règle générale, la clé de session d'un serveur Web comporte 40 bits. Mais elle peut atteindre 128 bits, en fonction du niveau de sécurité souhaité.
Pour configurer les fonctionnalités de communications sécurisées SSL de votre serveur Web, cliquez sur **Modifier**. Vous pouvez effectuer l'une des opérations suivantes :

- Obliger l'utilisateur à établir une liaison sécurisée (cryptée) pour se connecter à votre répertoire ou fichier ;
- Configurer les fonctionnalités de mappage et d'authentification des certificats clients de votre serveur Web ;
- Créer et configurer des listes de certificats de confiance (CTL).

5. En-têtes HTTP



Cet onglet permet d'envoyer les valeurs renvoyées au navigateur dans l'en-tête de la page HTML.

Activer l'expiration de contenu

Activer cette case à cocher pour inclure les informations d'expiration. Inclure une date dans des documents à caractère provisoire, tels que des offres spéciales ou l'annonce d'évènements. Le navigateur compare la date actuelle à la date d'expiration afin de déterminer si une page mise en mémoire cache doit être affichée ou si une page mise à jour doit être demandée au serveur.

En-têtes HTTP personnalisés

Utiliser cette propriété pour envoyer un en-tête HTTP personnalisé à partir du serveur Web vers le navigateur client. Les en-têtes personnalisés peuvent être utilisés pour envoyer des instructions qui ne sont pas encore prises en charge dans la spécification HTML en cours, telles que des balises HTML plus récentes qu'IIS ne prend peut-être pas en charge au moment du lancement du produit. Par exemple, vous pouvez utilise un en-tête HTTP personnalisé pour permettre au navigateur client de mettre la page en mémoire cache tout en évitant que les serveurs proxy ne le fassent.

Pour modifier un en-tête personnalisé existant, sélectionnez le, puis cliquez sur **Modifier.**

Pour interrompre l'envoi d'un en-tête personnalisé, sélectionnez le, puis cliquez sur **Supprimer**.

Contrôle d'accès au contenu

Utiliser des contrôles d'accès au contenu afin d'incorporer des étiquettes descriptives dans les en-têtes HTTP de vos pages Web. Certains navigateurs, tels que Microsoft Internet Explorer version 3.0 ou ultérieure, peuvent détecter les contrôles d'accès au contenu pour aider les utilisateurs à identifier les éventuelles informations choquantes sur le Web.

Pour définir des contrôles d'accès au contenu d'un site Web, répertoire ou fichier, cliquez sur **Modifier le contrôle d'accès…**

MIME (Multipurpose Internet Mail Extensions)

Qu'est ce que MIME ?

Un navigateur sait traiter les fichiers de texte (ASCII), les fichiers HTML, les images GIF et JPEG. Lorsqu'il rencontre un fichier d'un autre type, il fait appel à un module externe (plug-in) ou à une application présente sur la machine cliente (ex : Word pour un fichier ".doc"). Sur la plate-forme PC, le navigateur peut se fier à l'extension du fichier, mais sur la plate-forme Apple, il doit utiliser une autre moyen. Le type MIME a été créé pour caractériser le type d'un fichier indépendamment de la plate-forme à laquelle appartient l'ordinateur client. A l'origine, le type MIME était utilisé uniquement pour les fichiers attachés du courrier électronique, mais par la suite son usage fut étendu au Web.

Si l'on fait appel, dans une page HTML, à un fichier dont le type MIME n'est pas déclaré sur le serveur Web utilisé, toutes sortes de choses désagréables peuvent se produire. Le serveur Web peut refuser de servir la page en question, le navigateur peut l'afficher n'importe comment, à moins qu'il ne se plante systématiquement chaque fois que la page est demandée, ou qu'il ignore superbement le fichier en question.

L'organisme qui gère son propre site Web doit donc apprendre à déclarer le type MIME d'un nouveau type de fichier.

Configuration MIME

Cliquer sur le bouton **Types de fichier…** pour configurer les mappages MIME. Les types de fichiers enregistrés qui sont installés par défaut dans Windows sont affichés dans la boîte de dialogue **Types de fichiers…** . Les extensions de types de fichiers et les mappages MIME sont affichés pour les types de fichiers sélectionnés dans la zone **Informations sur les types de fichiers**.

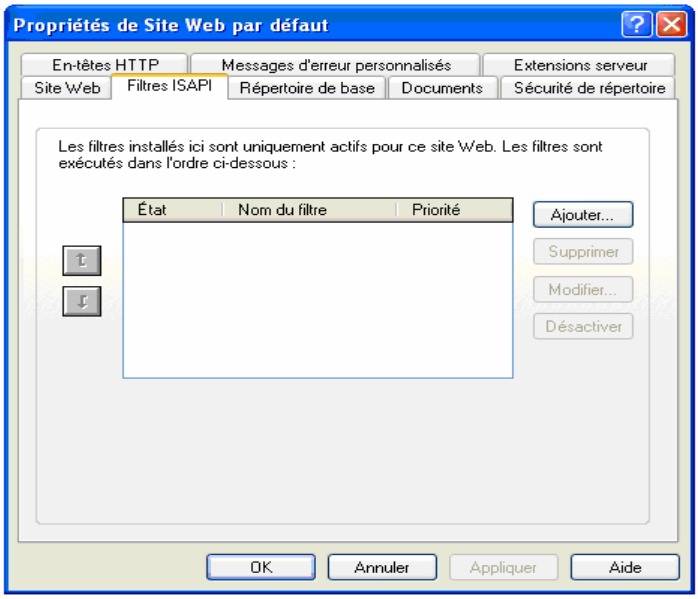
Pour configurer des mappages MIME supplémentaires, cliquez sur le bouton **Nouveau type…** dans la boîte de dialogue **Types de fichiers…** , puis dans la boîte de dialogue **Types de fichiers…,** tapez l'extension associée au fichier dans la zone **Extension associée** (par exemple .**swf** l'extension des animations Flash), Ensuite dans la zone **Type de contenu (MIME)**, entrez le type MIME suivi de l'extension de nom de fichier en utilisant le format type MIME/extension de nom de fichier (par exemple **application/x-shockwave-flash** le type MIME des animations flash).

Pour supprimer les mappages MIME, sélectionnez le type de fichier dans la zone **Types de fichiers enregistrés** et cliquez sur **Supprimer**.
Pour modifier des mappages MIME existants, sélectionnez le type de fichier dans la zone **Types de fichiers enregistrés**, cliquez sur le bouton **Modifier** et modifiez le contenu des zones **Extension associé** et **Type de contenu (MIME)** si nécessaire.
Si vous définissez des mappages MIME dans les feuilles de propriétés principales de votre ordinateur, les sites Web et les répertoires de votre ordinateur utilisent les mêmes mappages. Vous pouvez modifier les mappages MIME d'un site Web ou d'un répertoire. Si vous réappliquez ensuite les propriétés principales, celles-ci remplacent toutefois complètement les propriétés modifiées du site Web ou du répertoire. Autrement dit, les propriétés ne sont pas fusionnées.

Liste des MIME populaires

Extensions	**Type MIME**
.pdf	application/pdf
.swf	application/x-shockwave-flash
.xml	application/xhtml+xml
.mid / .midi	audio/midi
.mp3	audio/mp3
.wav	audio/wav
.gif	image/gif
.jpg / .jpeg	image/jpg
.png	image/png
.tif / .tiff	image/tif
.ico / .cur	image/x-icon
.css	text/css
.htm / .html	text/html
.js	text/javascript
.avi	video/avi
.mpg / .mpeg	video/mpeg
.txt	text/plain

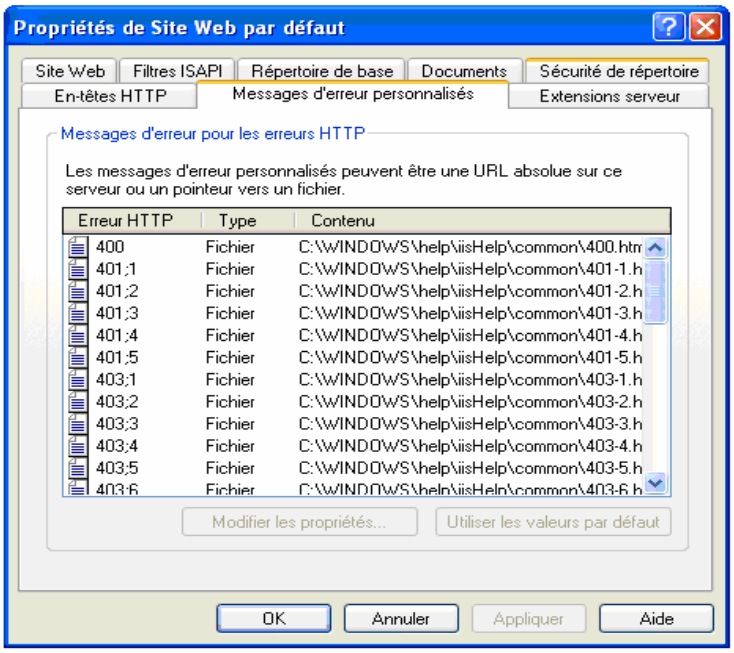
6. Filtres ISAPI



Cet onglet permet de définir les options des filtres ISAPI.
Un filtre ISAPI (Internet Services Application Programming Interface) est une DLL qui s'exécute dans le processus inetinfo.exe afin de filtrer les données qui circulent vers et depuis le serveur. Le filtre enregistre la notification des événements. Lorsque les événements sélectionnés se produisent, le filtre prend le contrôle et il est alors possible d'analyser les données et de les modifier (pendant leur transfert du serveur au client ou inversement). Les filtres ISAPI optimisent la journalisation des requêtes HTTP (par exemple, ils permettent de savoir qui se connecte à votre serveur), facilitent la personnalisation des procédures de cryptage ou de compression et offrent des méthodes supplémentaires d'authentification. Lorsque ces filtres sont mis en oeuvre, toutes les requêtes et les réponses doivent transiter par eux, ce qui peut avoir des répercussions non négligeables sur les performances du site.
Un exemple de filtre ISAPI est php5isapi.dll qui permet à IIS de supporter le langage PHP dans sa version 5. Un autre exemple est celui de URLScan : ce filtre ISAPI applique des règles aux URLs avant même qu'elles soient interprétées par IIS afin d'interdire par exemple les URLs comportant des caractères interdits.

- Pour ajouter (supprimer) un filtre ISAPI, cliquez sur le bouton **Ajouter** (**Supprimer**).
- Pour modifier les propriétés d'un filtre ISAPI, sélectionnez le et cliquez sur le bouton **Modifier**.
- Pour activer (désactiver) un filtre ISAPI, sélectionnez le et cliquez sur le bouton **Activer** (**Désactiver**).
- Pour modifier l'ordre d'exécution d'un filtre ISAPI, sélectionnez le et cliquez sur la flèche orientée vers le bas ou celle orientée vers le haut. Vous pouvez uniquement modifier l'ordre de chargement de filtres dont la priorité est identique.

7. Messages d'erreur personnalisés



L'onglet **Messages d'erreur personnalisés** permet de configurer IIS pour envoyer des messages d'erreur personnalisés à la place des messages d'erreur HTTP 1.1 par défaut. Ces messages d'erreur personnalisés peuvent être mappés sur un nom de fichier ou sur une URL.

Rappel

Messages d'erreur HTTP 1.1 : Lorsqu'un utilisateur tente de se connecter à un site Web et qu'une erreur HTTP se produit, un message générique est renvoyé au navigateur du client avec une brève description des événements survenus lors de la tentative de connexion. Par exemple, si un utilisateur tente de se connecter à un site Web qui a atteint ses capacités maximales de connexion, une erreur HTTP sera renvoyée sous la forme d'une page HTML, contenant le message « Too many users ».

Messages d'erreur personnalisés : Les messages d'erreur HTTP suivants peuvent être personnalisés avec IIS :

Code d'erreur	Message d'erreur
400	Bad request
401.1	Logon failed
401.2	Logon failed due to server configuration
401.3	Unauthorized due to ACL on resource
401.4	Authorization failed by filter
401.5	Authorization failed by ISAPI/CGI application
403.1	Execute access forbidden
403.2	Read access forbidden

403.3	Write access forbidden
403.4	SSL required
403.5	SSL 128 required
403.6	IP address rejected
403.7	Client certificate required
403.8	Site access denied
403.9	Too many users
403.10	Invalid configuration
403.11	Password change
403.12	Mapper denied access
403.13	Client certificate revoked
403.14	Directory listing denied
403.15	Client Access Licenses exceeded
403.16	Client certificate untrusted or invalid
403.17	Client certificate has expired or is not yet valid
404	Not found
404.1	Site not found
405	Method not allowed
406	Not acceptable
407	Proxy authentication required
412	Precondition Failed
414	Request-URI too long
500	Internal server error
500.12	Application restarting
500.13	Server too busy
500.15	Requests for Global.asa not allowed
500-100.asp	ASP error
501	Not implemented
502	Bad gateway

Pour modifier les propriétés des messages d'erreur personnalisés, cliquez sur le bouton **Modifier les propriétés…**. Si le type de sortie est une URL, cette URL doit se trouver sur un serveur local.
Pour configurer une erreur personnalisée de manière à utiliser le code de retour d'erreur HTTP 1.1 par défaut, sélectionnez l'erreur, puis cliquez sur le bouton **Utiliser les valeurs par défaut**.

8. Serveur HTTP configuré et prêt à fonctionner

Pour tester le serveur Web, créez une page HTML simple intitulée test.html, puis enregistrer-la dans le dossier Inetpub\wwwroot de l'ordinateur exécutant le serveur Web. Cette page HTML peut comporter une seule ligne, par exemple : Mon serveur fonctionne.
Ouvrez ensuite une page test dans un navigateur Web avec une requête HTTP. Si IIS est exécuté sur votre ordinateur local, entrer l'URL suivante dans votre navigateur Web :
http://localhost/test.html
Si IIS est exécuté sur un ordinateur en réseau, utiliser le nom de l'ordinateur en réseau comme nom de domaine. Par exemple, si le nom de l'ordinateur qui exécute IIS est Formateur, entrez l'URL suivante dans votre navigateur:
http://Formateur/monFichierTest.html
Ou bien
http://Adresse-IP-Formateur/test.html
Pour vous simplifiez la tâche, car vous ne disposez certainement pas d'une IP fixe, il existe des services gratuits sur Internet (www.no-ip.com, www.DynDNS.org, www.Dns2Go.com, …) qui permettent d'avoir une URL fixe qui redirige automatiquement l'utilisateur vers votre ordinateur, de façon à avoir une adresse du type :
http://ce-que-vous-voulez.no-ip.com

IV. Installation et configuration du serveur Apache sous Windows

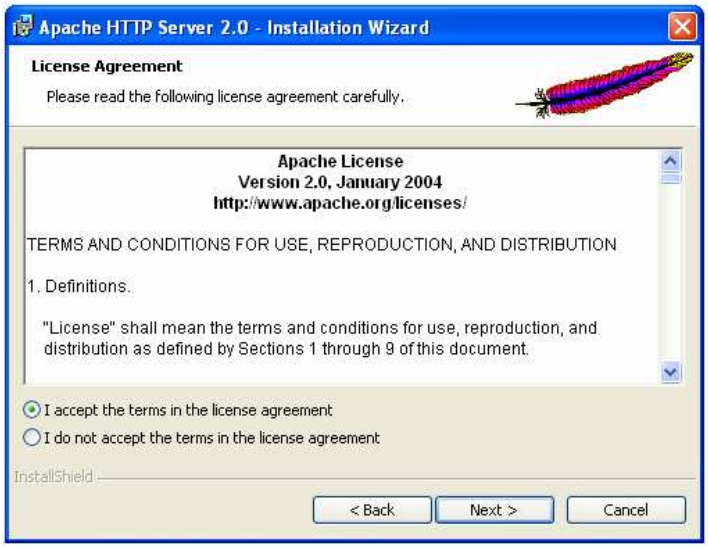
1. Introduction

Cette partie décrit comment installer et configurer un serveur **Apache 2.0.58** sur Windows pour un environnement de test.
La plupart des développeurs utilisent leur PC personnel pour développer leurs scripts ou leurs sites Web personnels et souhaitent pouvoir tester ces derniers en local avant publication.
La mise en place d'un serveur Web Apache est la première brique de cet environnement de développement.
Cette partie décrit l'installation d'un Apache 2.0.58 sur un PC équipé d'un Windows XP. Il est à noter que l'installation d'un Apache du même train logiciel (2.0.x) sera certainement semblable. De même une installation sur Windows 2000/2003 Server ne devrait pas apporter de grandes différences.

2. Installation

Il faut tout d'abord télécharger la version Apache pour Windows. Celle-ci se trouve sur **http://httpd.apache.org/**, le fichier s'appelle "**apache_2.0.58-win32-x86-no_ssl.msi**".
Un double-clic lancera le programme d'installation... On clique sur **Next**.

Vous devez tout d'abord accepter la licence d'utilisation de Apache.

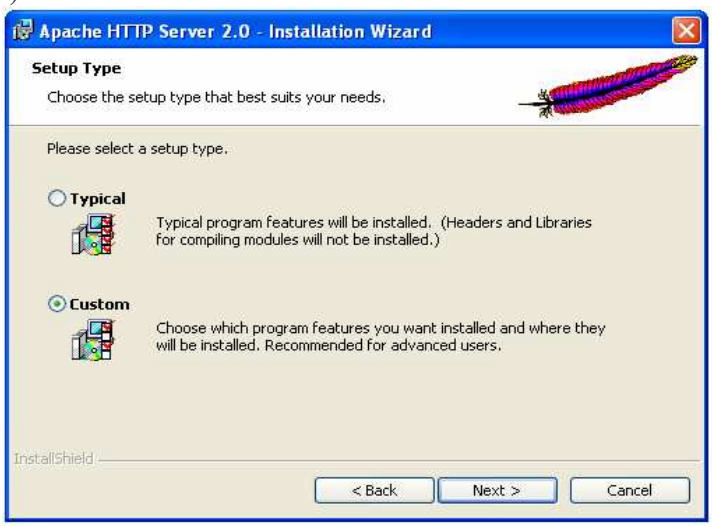


Cochez **I accept the terms in the licence agreement** puis cliquez sur **Next**.
Ceci étant si vous n'acceptez pas les termes de la licence, l'installation s'achèvera là...
Une fenêtre contenant une petite explication de ce qu'est Apache apparaît par la suite. Cliquez sur **Next**.

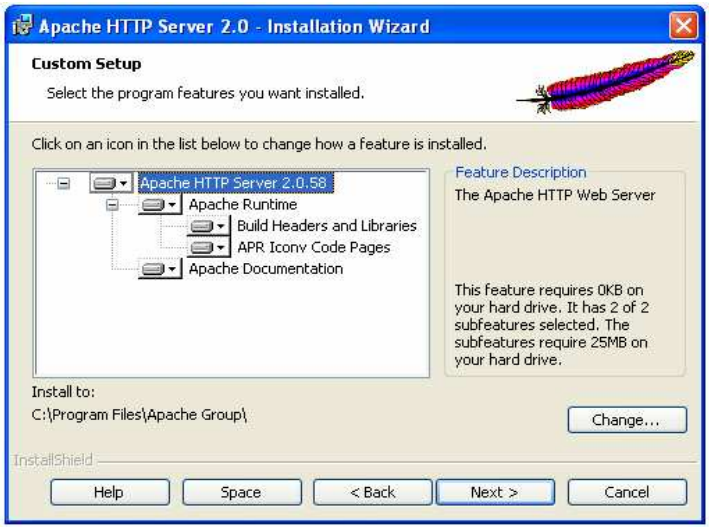
A cet écran, vous allez configurer le nom de domaine, le nom du serveur ainsi que l'adresse e-mail de l'administrateur du serveur.

Network Domain : Nom de domaine du serveur, Localhost correspondant à l'hôte local dans le cas présent.
Server Name : Nom du serveur, ici, nous allons mettre 127.0.0.1 qui correspond à l'IP interne de la machine.
Administrator's Email Address : l'adresse e-mail de l'administrateur en l'occurrence vous.
For All Users, on Port 80, as Service : cette option permet d'installer apache pour **tout les comptes utilisateurs** en utilisant le **port 80** (port utilisé par défaut pour un serveur web) **en tant que service** (le service est utilisé par Windows XP ou 2000).
only for the Current User, on Port 8080, when started Manually : cette option permet d'installer apache pour **l'utilisateur courant** (qui procède à l'installation) en utilisant le **port 8080** et avec un **démarrage manuel**. Cette dernière est recommandée si vous ne souhaitez pas mettre en production votre serveur web, mais que vous l'utilisez dans un objectif de développement web.

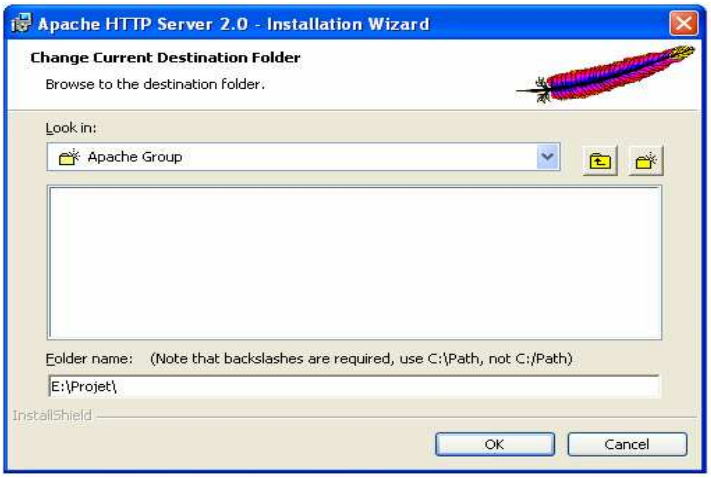
Dans le cas présent, on procède à une installation de type « tout utilisateurs, sur le port 80 en tant que service ».
Cliquez sur **Next** pour continuer l'installation...
Choisissez le type d'installation pour votre serveur web :
• **Typical** : Installation typique (va installer les principales éléments pour l'utilisation du serveur) – recommandé si vous n'avez pas trop d'idée des composants dont vous avez besoin.
• **Custom** : Installation personnalisée (on défini les composants que l'on souhaite installer pour notre serveur)



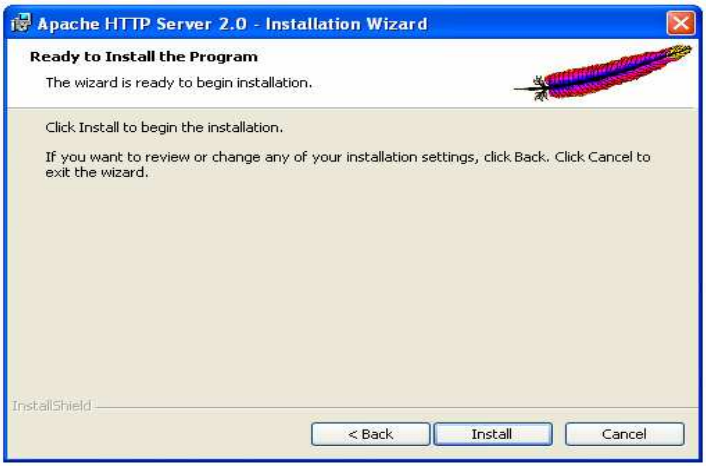
Dans, le cas présent, on choisit une installation de type **Custom**, et on clique sur **Next**.
Nous avons (ci-dessous) les principaux composants pour notre serveur web, à noter que tous ne sont pas utiles si l'on pense utiliser notre serveur de manière standard.



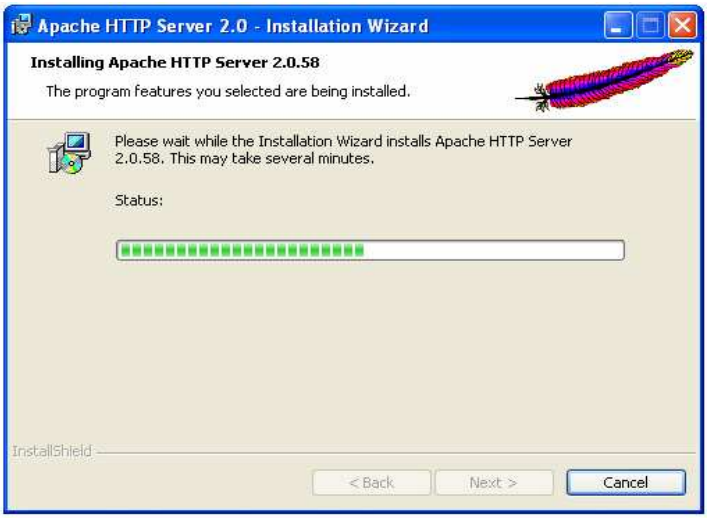
Apache s'installe par défaut dans : « **C:\Program Files\Apache Group** ».
Si vous souhaitez procéder à l'installation dans un autre répertoire, cliquez sur le bouton **Change**... et entrez le nouvel emplacement E:\Projet\ par exemple.



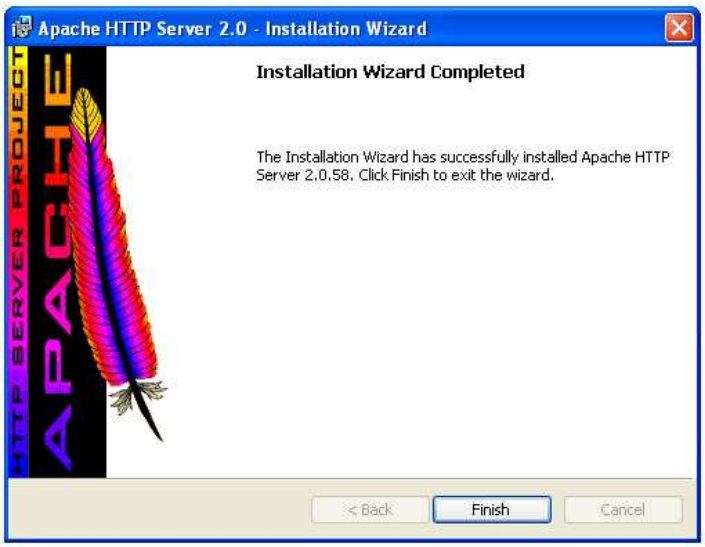
Cliquez sur le bouton **OK** pour valider puis sur le bouton **Next** pour continuer notre installation.



Cliquez sur le bouton **Install** pour procéder à l'installation.

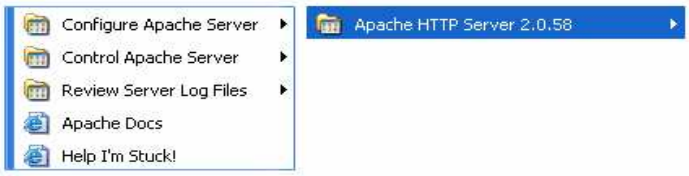


Une fois l'installation terminée, nous avons l'écran ci-dessous qui s'affiche.



Cliquez sur le bouton **Finish**.

A présent, notre serveur est opérationnel, d'ailleurs, si l'installation était standard, les services sont déjà en action.
Par ailleurs, si vous regardez dans le menu **Démarrer / Tous les programmes**, vous devriez avoir le menu suivant :



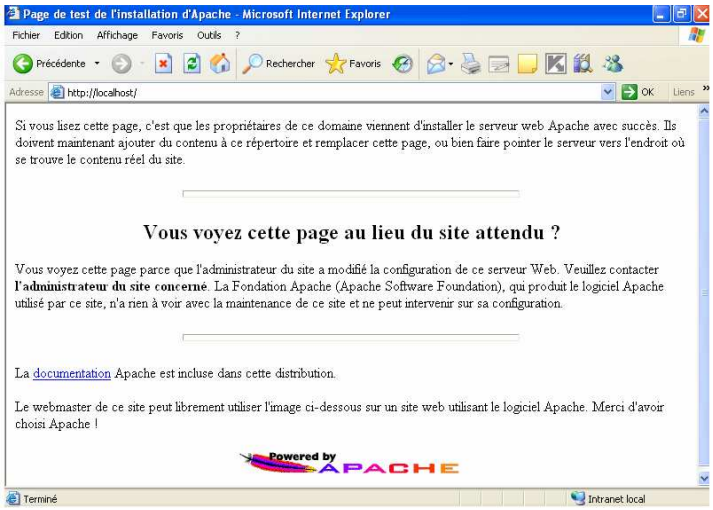
Vous aurez pu aussi remarquer la présence de **Apache Service Monitor** dans votre systray (à côté l'heure) qui est représenté par l'icône ci-dessous :

Cet utilitaire vous permet de démarrer / arrêter /redémarrer le service Apache2. Pour accéder à Apache monitor, un clic droit sur vous affichera le menu **Open Apache Monitor**. Ce dernier vous permettant de lancer ou non votre Apache.

Note: Si vous souhaitez lancer votre service apache sans pour cela passer par **Apache Service Monitor**. Il vous suffit de faire un **clique droit sur Poste de Travail / Gérer** ensuite, aller dans la rubrique **Services et applications / Services**. Là, on trouve le service **Apache2** sur lequel on va faire un clique droit, puis **démarrer** ou **arrêter** selon le cas.

Une astuce toute simple est d'ouvrir une invite de commande, pour cela, **Démarrer / Exécuter** puis taper **cmd**. La fenêtre ouverte, on tape :
net start apache2 (pour démarrer le service)
net stop apache2 (pour arrêter le service)
Voilà, votre service sera lancé ou arrêté selon le cas.

Ma première visite !
Pour cela, ouvrez notre navigateur, puis tapez dans la barre d'adresse :
http://localhost ou **http://127.0.0.1**
Si lors de l'installation vous avez choisi l'option « **only for the Current User, on Port 8080, when started Manually** », vous devez ajouter **:8080** à la fin de l'url comme ceci : **http://localhost:8080** ou
http://127.0.0.1:8080
Ceci n'étant valide que dans le cas où vous avez entré les mêmes informations indiquées lors de l'installation.
Si vous avez rentré une IP de votre réseau local en lieu et place de **127.0.0.1**. Votre serveur est visible à l'url suivante depuis n'importe quel poste de votre réseau LAN : **http://192.168.0.1** (par exemple)
Si tout a été bien installé et fonctionne, vous devriez avoir un écran similaire à celui-ci.



Votre serveur web est à présent online.

En cas de problème :
Si pour une raison ou une autre, vous n'arrivez pas à accéder à la page par défaut de apache (ci-dessus), il vous faut vérifier les points suivants :
Vérifier que le service apache2 est bien démarré, pour cela utiliser le **Gestionnaire de l'ordinateur** rubrique **Services et applications / Services** dans lequel vous aurez l'état actuel du service en question**.**
Vérifier le fichier log de apache, ce dernier se nomme **error.log** et se trouve dans le sous répertoire **logs** de votre Apache. Celui-ci inscrivant les erreurs qui peuvent être intervenu lors du lancement du service ainsi que pendant son fonctionnement.

3. Configuration de apache
3.1. Administrateur & développeur
Rappelons la distinction entre serveur et site. Le site est un ensemble de documents HTML et de scripts ; c'est un contenu d'informations à disposition des clients. Il est développé par des personnes qui récoltent l'information propre au site, l'organisent, la stockent et la formatent.

Le serveur est un programme qui écoute les demandes adressées au site et s'efforce de livrer au client les informations de ce site. Le serveur peut soutenir l'activité d'un site ou de plusieurs sites.
Votre rôle d'administrateur est de piloter ce programme. Vous le faites, pour l'essentiel, à partir d'un seul document : le fichier de configuration. C'est votre centre de commandement. En Windows, c'est le document intitulé **httpd.conf** situé en **…/Apache2/conf/.** Votre rôle est d'en ajouter, d'en modifier, de les paramétrer. Il sera aussi de vérifier dans les journaux d'exploitation si vos interventions en httpd.conf ont été pertinentes !
Situons, dans la structure, les répertoires majeurs (Que vous trouvez dans le répertoire Apache2) :
bin : le programme exécutable, Apache.exe
conf : le fichier de configuration, httpd.conf
htdocs: le(s) site(s)
Mais aussi :
modules : les modules appelés de manière dynamique
manual : la documentation

3.2. Configuration

La configuration de Apache se fait de manière simple et ce via un seul et unique fichier de configuration. Le fichier de configuration du serveur web se nomme **httpd.conf** (un fichier texte qui sera édité avec le bloc-notes) et est situé dans le sous répertoire **conf** d'Apache et que vous pouvez ouvrir à partir du menu de démarrage : **Apache HTTP Server 2.0.xx -> Configure Apache Server -> Edit the httpd.conf configure file**.
Ce fichier contient les principaux éléments pour faire en sorte que votre serveur web tourne sans encombre. Une modification dans ce fichier peut rendre indisponible Apache.
Le fichier httpd.conf est « divisé » en 3 sections.
• « **Global environment** », présentant les directives qui contrôlent les activités d'Apache dans leur ensemble.
• «**Main Server configuration** », présentant les directives du serveur principal, ou en l'absence d'hôtes virtuels, du serveur unique.
• « **Virtuals hosts** », section susceptible de recevoir un ou plusieurs cadres (containers) comportant chacun les directives pour des sites distincts.
Les deux dernières font référence à la formule des hôtes virtuels pour la gestion de sites différents.
Vérifions : toute la troisième section est en commentaire. Une installation « par défaut » ne comporte pas d'hôtes virtuels. Repérons cependant en passant en quoi des hôtes virtuels pourraient se singulariser : par un nom d'administrateur, surtout par un nom de serveur et une racine de site particuliers, et enfin par des fichiers de maintenances propres.

a. section 1 : environnement global

Les directives dans cette section affectent le comportement global d'Apache, comme le nombre maximum de requêtes concurrentes auquel il peut répondre ou où il peut trouver ses fichiers de configuration.
ServerRoot : racine du répertoire contenant la configuration du serveur, les fichiers log d'erreurs et les fichiers log de connexions.
Par exemple : **ServerRoot "C:/Program Files/Apache Group/Apache2"**

ScoreBoardFile: fichier utilisé pour stocker les informations sur les processus internes au serveur. Toutes les architectures ne nécessitent pas ceci. Mais si la votre le nécessite (vous le saurez parce que ce fichier sera créé lors du lancement d'Apache) alors vous devez vous assurer que deux instances d'Apache ne partagent pas le même fichier "**scoreboard**".
Par défaut : **ScoreBoardFile logs/apache_runtime_status**

PidFile: fichier dans lequel le serveur stocke les numéros d'identification des processus (process identification, PID), lorsqu'il démarre.
Par défaut : **PidFile logs/httpd.pid**

Timeout: nombre de secondes avant lequel le serveur reçoit et envoie un time out (échec de requête).
Par défaut : **Timeout 300**

KeepAlive: permet ou non d'autoriser les connexions persistantes (plus d'une requête par connexion). Mettre la valeur à "Off" si vous voulez désactiver cette option.
Par défaut : **KeepAlive On**

MaxKeepAliveRequests: nombre maximum de requêtes permises lors de connexion persistantes. Mettre la valeur à 0 afin de permettre un nombre illimité de requêtes. Nous recommandons de laisser cette valeur relativement haute afin d'améliorer les performances.
Par défaut : **MaxKeepAliveRequests 100**

KeepAliveTimeout: nombre de secondes d'attente entre deux requêtes d'un même client pour la même connexion.
Par défaut : **KeepAliveTimeout 15**

Sous les systèmes Win32 Apache crée toujours un processus fils (child process) afin de gérer les requêtes. Si ce processus n'est plus valide, il est automatiquement recréé. Le processus fils permet de multiplier les tâches gérant les requêtes. Les deux directives suivantes permettent de contrôler le comportement des tâches et processus.

MaxRequestsPerChild: nombre de requêtes que chaque processus fils a la possibilité de gérer avant que le processus ne soit plus valide. Le processus fils se terminera afin d'éviter tous problème après un usage prolongé de la mémoire et des autres ressources par Apache (et peut-être des librairies qu'il utilise). Sur la plupart des systèmes d'exploitation, ceci n'est pas réellement indispensable, mais certains (comme les systèmes Solaris) disposent de lacunes certaines au niveau des librairies. Pour un système Win32, mettez cette valeur à zéro (illimité), sauf avis contraire.
Note: Cette valeur ne comptabilise pas les keepalive requests après la requête initiale par connexion. Par exemple, si un processus fils gère une requête initiale et 10 sous-jacentes requêtes "keepalive", il ne comptabilisera qu'une seule requête.
Par défaut : **MaxRequestsPerChild 0**

ThreadsPerChild : nombre de tâches concurrentes (par exemple des requêtes) que le serveur autorise simultanément. Ajustez cette valeur en fonction du temps de réponse de votre serveur (plus ce nombre est élevé, plus les requêtes concurrentes seront lentes) ainsi qu'en fonction des ressources que le serveur est autorisé à utiliser.
Par défaut : **ThreadsPerChild 250**

Listen: Indique les adresses et ports que le serveur doit « écouter ». Si vous voulez que votre serveur accepte toutes les adresses, mais sur les deux seuls ports 80 et 8000. Alors :
Listen 80
Listen 8000
Ou si vous ne permettez l'accès qu'à deux couples d'adresses ports, alors :
Listen 192.168.0.1 :80
Listen 192.168.0.2 :8000

Une option très utile dans la configuration est l'utilisation des modules. Leur nom comprend obligatoirement l'extension **so** et étend les fonctionnalités du serveur, qui, dans sa configuration de base, ne peut pas faire grande chose. Cette modularité des fonctionnalités permet de gérer très souplement le fonctionnement d'un serveur. La liste des modules disponibles s'agrandit à chaque nouvelle version. Nous nous limiterons à indiquer ci-dessous les plus basiques. A chaque module correspondent des instructions spécifiques qui, ajoutées dans le fichier de configuration d'Apache, configurent le fonctionnement du module correspondant.

Module	**Description**
mod_access	Permet de contrôler quelles machines peuvent accéder à un répertoire du site
mod_actions	Contrôle l'exécution de scripts CGI
mod_alias	Permet de rediriger les clients vers un autre fichier, répertoire ou un autre serveur
mod_auth	Permet de contrôler l'authentification des utilisateurs et l'usage des ressources
mod_dir	Sans ce module d'employer des noms de fichiers par défaut comme index.htm, index.html….
mod_cgi	Exécution des scripts CGI, y compris la gestion des variables d'environnement DOCUMENT_ROOT, REMOTE_HOST, REMOTE_IDENT, REMOTE_USER
mod_imap	Pour pouvoir employer les images interactives
mod_log_agent	Autorise le recueil d'informations relatives aux clients utilisateurs
mod_mime	Pour l'organisation des différents types MIME
mod_rewrite	Autorise, sous contrôle de règles, la réécriture des URL fournis par les clients
mod_setenvif	Permet de définir les variables d'environnement en fonction du navigateur.
mod_so	Facilite le chargement des bibliothèques dynamiques
mod_userdir	Convertit un nom d'utilisateur en un répertoire particulier et un nom de fichier par défaut. Par défaut cela correspond au répertoire de nom public_html rangé dans le répertoire de démarrage de l'utilisateur.

Pour ajouter un module, le module status par exemple qui permet d'obtenir des informations en quasi temps réel sur l'état du serveur, aller dans le fichier de configuration et rechercher la ligne suivante :
 # LoadModule status_module modules/mod_status.so
Puis décommenter la :
LoadModule status_module modules/mod_status.so

b. section 2: configuration du serveur 'principal'
Les directives dans cette section permettent de configurer les valeurs servant pour le serveur Web principal, qui répondra à toutes les requêtes qui ne sont pas prises en compte par la définition d'un hôte virtuel (VirtualHost). Ces valeurs permettent aussi de définir des valeurs par défaut pour tous les containers <VirtualHost> que vous pourriez définir plus loin dans ce fichier.
Toutes ces directives peuvent apparaître à l'intérieur des containers <VirtualHost>, cas dans lequel, ces valeurs par défaut ne seront pas prises en compte pour l'hôte virtuel en question.

Port: port par lequel les requêtes devront être adressés au serveur autonome. Certains firewalls doivent être configurés afin qu'Apache soit apte à recevoir des requêtes de ports spécifiques. Les autres serveurs
httpd lancés interfèreront aussi avec ce port. Désactivez tous firewalls, paramètres de sécurité et autres services, si vous rencontrez des problèmes. Afin de vous aider à résoudre les problèmes, utilisez la commande Windows NT: netstat –a.
Par exemple : **Port 80**

ServerAdmin: l'adresse email à laquelle les problèmes devraient être envoyés. Cette adresse apparaît sur certaines pages auto générées par le serveur comme les documents d'erreur.
Par exemple : **ServerAdmin webmaster@nomdedomaine.ext**

ServerName : vous permet de définir un nom d'hôte qui sera retourné aux clients si celui-ci est différent du nom d'hôte de la requête. (Par exemple, utilisez "www" en lieu et place du véritable nom d'hôte).
Note: Vous ne pouvez pas simplement inventer des noms d'hôtes et espérer que ceux-ci fonctionneront. Le nom définit ici doit être un nom DNS valide pour votre hôte.
Si votre hôte ne dispose pas d'un nom DNS enregistré, il vous faut entrer ici son adresse IP.
Ainsi, vous devrez accéder au serveur via son adresse IP (par exemple, http://196.206.1.2/).
L'adresse IP 127.0.0.1 est l'adresse de bouclage local TCP/IP (loop-back address), souvent nommé localhost. Votre machine se reconnaît toujours par cette adresse. Si vous n'utilisez Apache uniquement pour des tests locaux, vous pouvez utiliser 127.0.0.1 en temps que nom de server.
Par exemple : **ServerName 127.0.0.1**

UseCanonicalName: lorsque cette option est sur "On", quand le fonctionnement d'Apache nécessite d'utiliser une URL pointant sur lui-même, il utilisera les valeurs ServerName et Port afin de créer un nom "canonique". Avec cette option à "Off", Apache utilisera le nom d'hôte:port que lui fournit le client, lorsque cela est possible.
Par défaut : **UseCanonicalName On**

DocumentRoot: Répertoire contenant les documents à afficher par le serveur Web. Par défaut, toutes les requêtes sont effectuées depuis ce répertoire, mais les liens symboliques et les alias peuvent être utilisés afin de pointer vers des localisations différentes.
Par exemple: **DocumentRoot "C:/Program Files/Apache Group/Apache2/htdocs "**

Chaque répertoire auquel Apache à accès, peut être configuré en fonction des services et fonctionnalités qui lui sont alloués et / ou désactivés dans ce répertoire (et sous répertoire). Il y a pour tout dossier (et ses sous-dossiers) une directive <Directory "....."></Directory> décrivant ces propriétés.

En premier lieu, il nous faut configurer l'option par défaut afin d'appliquer la politique la plus restrictive en la matière. Par exemple :

<Directory />
Options FollowSymLinks ExecCGI
AllowOverride None
</Directory>

Notez qu'à partir de ce point, il va vous falloir spécifier que les fonctionnalités spéciales soient activées ainsi si quelque chose ne fonctionne pas comme désiré, soyez sûr de l'avoir activée ci-dessous.

La valeur ci-dessous devrait coïncider avec la valeur se trouvant sous DocumentRoot. Elle sert à définir les droits concernant ce répertoire.

<Directory "C:/Program Files/Apache Group/Apache2/htdocs">

Par la suite on doit spécifier les options de ce répertoire, les valeurs possibles pour Options sont "None", "All", ou toutes autres combinaisons de "Indexes", "Includes", "FollowSymLinks", "ExecCGI", ou "MultiViews".

None	Désactive toutes les options.
All	Active toutes les options SAUF Multiviews.
Indexes	Permet aux utilisateurs d'avoir des indexes générés par le serveur. C'est à dire si l'index du répertoire (index.htm le + souvent) est manquant, cela autorise le serveur à lister le contenu du répertoire (dangereux suivant les fichiers contenus dans ce répertoire).
FollowSymLinks	Autorise à suivre les liens symboliques.
ExecCGI	Autorise à exécuter des scripts CGI à partir de ce répertoire.
Includes	Autorise des fichiers include pour le serveur.
IncludesNOEXEC	Permet les includes mais empêche la commande EXEC (qui permet d'exécuter du code).
Multiviews	Autorise les vues multiples suivant un contexte. Cela permet par exemple d'afficher les pages dans un langage suivant la configuration du langage du client.
SymLinksIfOwnerMatch	Autorise à suivre les liens seulement si le user ID du fichier (ou répertoire) sur lequel le lien pointe est le même que celui du lien

Par exemple : **Options Indexes FollowSymLinks MultiViews**

Vous pouvez aussi spécifier l'option AllowOverride qui permet de contrôler les directives à placer dans les fichiers .htaccess . Il peut prendre les valeurs "All", "None", ou toute combinaison des mots-clefs: Options FileInfo AuthConfig Limit.

All	Gère tout ce qui est dans .htaccess
AuthConfig	Active les directives d'autorisations AuthDBMGroupFile, AuthDBMUserFile, AuthGroupFile, AuthName, AuthType, AuthUserFile, require
FileInfo	Active les directives d'autorisations AddEncoding, AddLanguage, AddType, DefaultType, ErrorDocument, LanguagePriority

Limit	Active la directive d'autorisation Limit
None	Ne lit pas le fichier .htaccess et laisse les droits "Linux" de ce répertoire.
Options	Active la directive Option

Par défaut: **AllowOverride None**

Enfin Vous pouvez gérer la sécurité des requêtes sur le serveur en utilisant **Order allow,deny** et **Allow from all** définit par défaut.

Order : Donne l'ordre d'application des règles Allow Deny:

deny,allow	Applique les règles deny puis allow
allow,deny	Applique les règles allow puis deny

Allow (ou **deny**) :

Nom d'hôte	Autorise les hôtes spécifié, les adresses IP, le nom de domaine, etc..(ou les refuse si la règle est deny)
All	Autorise tout le monde (ou refuse si la règle est deny)

</Directory> : Indique la fin des règles pour ce répertoire.
A vous de placer vos règles suivant le contenu de vos répertoire accessibles par le Web. Il existe les mêmes règles pour les fichiers (**<Files> </Files>**) et les locations (**<Location> </Location>**).

UserDir: nom du répertoire qui sera utilisé comme répertoire d'accueil en cas de requêtes nominales.
Avec les systèmes Win32, la détermination du répertoire d'accueil au login Windows n'est pas faite, ainsi le formatage comme ci-dessous doit être effectué. Lisez la documentation à propos de UserDir en cas de problème.
Par exemple : **UserDir "Mes documents/Mes sites Web"**

DirectoryIndex: nom du fichier ou des fichiers à utiliser en tant qu'index de répertoire. Séparez les entrées multiples par des espaces.
Par exemple : **DirectoryIndex index.html index.htm index.php**

AccessFileName: nom du fichier dans lequel Apache trouvera les informations d'accès aux fichiers / répertoires dans chaque répertoire.
Par défaut: **AccessFileName .htaccess**

CacheNegotiatedDocs: par défaut, Apache envoie "Pragma: no-cache" pour chaque document négocié sur la base du contenu du document. Ainsi, le serveur proxy ne devrait pas mettre le document en cache. Activer la ligne suivante désactive cette fonction, donnant ainsi la possibilité au proxy de mettre vos documents en cache.
Par exemple : **CacheNegotiatedDocs On**

TypesConfig décrit où trouver le fichier mime.types (ou son équivalent).
Par défaut : **TypesConfig conf/mime.types**

DefaultType permet de définir quel sera le type MIME utilisé par défaut si le serveur ne peut pas déterminer son type à l'aide de son extension. Si votre serveur publie principalement des fichiers texte ou des documents HTML, "text/plain" est une bonne valeur. Si la plupart de vos fichiers sont des fichiers binaires, comme des applications ou des images, vous aurez peut-être envie d'utiliser "application/octet-stream" afin que les navigateurs n'affichent pas vos fichiers binaires en mode texte.
Par exemple : **DefaultType text/plain**

HostnameLookups: permet d'archiver les noms d'hôtes des clients ou simplement leurs adresse IP. Par exemple, www.apache.org (on) ou 204.62.129.132 (off). Par défaut, cette option est mise sur Off car il serait beaucoup mieux pour le net si ce genre d'options étaient désactivées sciemment, l'activation oblige chaque client à effectuer au MINIMUM un lookup à son serveur de noms (DNS).
Par défaut : **HostnameLookups Off**

EnableMMAP: permet de controller si le mapping de mémore est utilise pour délivrer les fichiers. (En supposant que cette fonctionnalité est prise en compte par votre système d'exploitation). Pour plus de détails voir http://localhost/manual/mod/core.html#enablemmap.
Par défaut: **EnableMMAP On**
EnableSendfile: permet de contrôler cette fois ci si les fichiers sont délivrés par le noyau du système d'exploitation. Pour plus de détails voir
http://localhost/manual/mod/core.html#enablesendfile
Par défaut : **EnableSendfile On**

ErrorLog: emplacement du fichier 'log'. Si vous ne spécifiez pas de directive ErrorLog dans un container
<VirtualHost>, les messages d'erreur en rapport à cet hôte virtuel seront archivés à cet endroit. Si vous définissez un chemin pour le fichier 'log' de l'hôte virtuel, l'archivage des erreurs se fera à cet endroit et non ici.
Par exemple : **ErrorLog logs/error.log**

LogLevel: permet de contrôler la nature des messages fichier error.log, et donc leur nombre. Les valeurs possibles sont: debug, info, notice, warn, error, crit, alert, emerg.

emerg	Enregistre seulement les erreurs qui rendent le serveur inutilisable
Alert	"emerg" + erreurs nécessitant une intervention.
Crit	"emerg" + "Alert" + erreurs critiques (accès réseau impossible par exemple)
error	"ermerg" + "Alert" + "Crit" + erreurs dans les pages, les scripts
warn	"ermerg" + "Alert" + "Crit" + "error" + erreurs non bloquantes (pages mal codées, scripts comportant des erreurs non bloquantes...)
info	"ermerg" + "Alert" + "Crit" + "error" + "Warn" + toutes les informations générées
debug	Enregistre TOUT ce qui peut se passer sur le serveur (un client demande une page: on enregistre)

Par défaut : **LogLevel warn**

CustomLog: permet de définir l'emplacement et formatage du fichier 'log' concernant les accès (utilise le format standard des fichiers 'log'). Si vous ne définissez aucun fichier 'log' dans les containers <VirtualHost>, ils seront archivés à cet endroit. Par contre, si vous définissez un fichier 'log' pour les accès par <VirtualHost>, les transactions seront archivées à l'endroit spécifié et non dans ce fichier.
Par exemple: **CustomLog logs/access.log common**
Si vous désirez archiver les agents ainsi que les referrers des clients, enlever le # des lignes suivantes afin qu'elles ne soient plus en commentaire.
#CustomLog logs/referer.log referer
#CustomLog logs/agent.log agent
Si vous préférez avoir recours à un fichier 'log' unique, contenant les informations sur les accès, agents et referrers (format de fichier 'log' combiné), vous pouvez utiliser la directive suivante :
CustomLog logs/access.log combined

ServerTokens : Pour faire en sorte que le visiteur ait un minimum d'information concernant votre serveur lorsque une page d'erreur type 404 s'affiche, nous pouvons modifier la valeur du paramètre ServerTokens en lui donnant la valeur Prod cela permet de ne fournir que le nom du serveur, soit dans le cas présent Apache, il n'y aura aucune information concernant la version utilisée ni d'autres informations qui pourraient renseigner une personne mal intentionnée. D'autres valeurs possibles sont : Full | OS | Minor | Minimal | Major | Prod. Ainsi,
Avec **ServerTokens Prod[uctOnly]** le serveur envoie (par exemple) : Server: Apache
Avec **ServerTokens Major** le serveur envoie (par exemple) : Server: Apache/2
Avec **ServerTokens Minor** le serveur envoie (par exemple) : Server: Apache/2.0
Avec **ServerTokens Min[imal]** le serveur envoie (par exemple) : Server: Apache/2.0.41
Avec **ServerTokens OS** le serveur envoie (par exemple) : Server: Apache/2.0.41 (Unix)
Avec **ServerTokens Full (or not specified)** le serveur envoie (par exemple) : Server: Apache/2.0.41 (Unix) PHP/4.2.2 MyMod/1.2
Par défaut on a : **ServerTokens Full**

ServerSignature : il est possible de manière optionnelle d'ajouter une ligne contenant la version du serveur et le nom de l'hôte virtuel aux pages générées par le serveur (pages d'erreurs, listings des répertoires FTP, …etc., mais pas des documents générés par des CGI). Avec "EMail" comme valeur, ces documents contiennent alors aussi un lien mailto: pointant sur la valeur ServerAdmin. Les valeurs possibles sont: On | Off | EMail
Par défaut : **ServerSignature Off**

Aliases: Ajoutez ici autant d'alias qu'il vous faut (aucune limite n'est fixée). Le format à respecter est :
Alias pseudonyme vrai_nom
Par exemple : **Alias /icons/ "C:/Program Files/Apache Group/Apache/icons/"**
Notez que si vous incluez un / en queue du pseudonyme, il vous faudra le spécifier au serveur afin que le serveur reconnaisse l'alias. Ainsi, "/icons" n'est pas en alias dans l'exemple. Seul "/icons/" est en alias.
Si le pseudonyme est terminé par un slash, alors le vrai_nom doit aussi se terminer par un slash. De plus, si le pseudonyme ne comporte pas de slash, il faut que le vrai_nom n'en comporte pas.

ScriptAlias: contrôle quel répertoire contient les scripts du serveur. Les ScriptAlias fontionne pratiquement de la même manière que les Aliases, à l'exception que les fichiers se trouvant à cet endroit sont traités en tant qu'applications et exécutés par le serveur lorsqu'ils sont demandé, alors que les documents sont envoyés directement au client.
Les règles se rapportant aux slashs de queue sont les même que pour la directive Alias.
Par exemple :
ScriptAlias /cgi-bin/ "C:/Program Files/Apache Group/Apache/cgi-bin/"
ScriptAlias /php/ "c:/php/"
AddType application/x-httpd-php .php
Action application/x-httpd-php "/php/php.exe"

Redirect : cette directive vous permet d'envoyer à un client des documents n'existant plus à l'endroit spécifié, mais ayant été déplacé. Cette option vous permet de définir aux clients où trouver les documents en question.
Format: **Redirect ancienne-URI nouvelle-URL**

Les directives qui suivent permettent de contrôler l'affichage des listings auto générés par le serveur.

FancyIndexing : vous permet de définir si vous désirez avoir un listing de type graphique ou standard.
Note: n'ajoutez l'option TrackModified au listing IndexOptions par défaut uniquement si tous les répertoires indexés se trouvent sur des volumes NTFS. Une fois cette option ajoutée, TrackModified rapportera la date de la dernière modification afin d'assister les caches et proxies afin de traquer les changements dans chaque répertoire, mais ceci ne fonctionne pas sur les volume en FAT.
Par exemple : **IndexOptions FancyIndexing**

AddIcon*: Ces directives permettent au serveur de définir quelle icône affiché suivant le type de fichier ou son type d'extension. Ces icônes ne sont affichés qu'à condition d'activer FancyIndex.
Par exemple :
AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip

AddIconByType (TXT,/icons/text.gif) text/*
AddIconByType (IMG,/icons/image2.gif) image/*
AddIconByType (SND,/icons/sound2.gif) audio/*
AddIconByType (VID,/icons/movie.gif) video/*
AddIcon /icons/binary.gif .bin .exe
AddIcon /icons/binhex.gif .hqx
AddIcon /icons/tar.gif .tar
AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
AddIcon /icons/a.gif .ps .ai .eps
AddIcon /icons/layout.gif .html .shtml .htm .pdf
AddIcon /icons/text.gif .txt
AddIcon /icons/c.gif .c
AddIcon /icons/p.gif .pl .py
AddIcon /icons/f.gif .for

AddIcon /icons/dvi.gif .dvi
AddIcon /icons/uuencoded.gif .uu
AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
AddIcon /icons/tex.gif .tex
AddIcon /icons/bomb.gif core
AddIcon /icons/back.gif ..
AddIcon /icons/hand.right.gif README
AddIcon /icons/folder.gif ^^DIRECTORY^^
AddIcon /icons/blank.gif ^^BLANKICON^^

DefaultIcon: vous permet de définir quel icône affiché lorsque le type de fichier n'est pas défini explicitement.
Par exemple : **DefaultIcon /icons/unknown.gif**

AddDescription: vous permet de placer une courte description après un fichier dans les index générés par le serveur. Ces descriptions ne seront affichées que pour les répertoires où FancyIndex est activée.
Format: **AddDescription "description" nom_du_fichier**
Par exemple : **AddDescription "tar archive" .tar**

ReadmeName: définit le nom du fichier README que le serveur doit chercher par défaut, et le lier aux listings de répertoires.
HeaderName: définit le nom du fichier permettant de définir un entête aux index auto-générés par le serveur.
Si MultiViews fait partie des Options activées, le serveur cherchera en premier lieu name.html et l'incluera s'il le trouve. Si name.html n'existe pas, le serveur cherchera ensuite name.txt et l'incluera en temps que fichier plain text s'il le trouve.
Par exemple:
ReadmeName README
HeaderName HEADER

IndexIgnore: permet de créer une liste de noms de fichier qui seront ignorés lors de la création automatique du listing de fichiers. L'utilisation des wildcards est autorisée.
Par exemple : **IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t**

Les directives qui suivent permettent de définir le type des documents.

AddEncoding : vous permet d'activer la décompression à la volée de certains documents par les navigateurs qui le supporte (Mosaic/X 2.1+).
Note: Tous les navigateurs ne supportent pas cette option.
En dépit des apparences similaires, les directives Add* qui suivent n'ont rien à voir avec les directives de paramétrage de FancyIndexing citées plus haut.
Par exemple : AddEncoding **x-compress Z**

AddLanguage : vous permet de définir le langage d'un document. Il vous est alors possible d'effectuer une transaction avec le client afin de lui fournir le fichier idéal.
Note 1: Le suffixe n'a pas besoin d'être le même que le mot clé pour le langage --- les polonais, par exemple, (dont le standard Internet est le code pl) pourrait avoir envie d'utiliser "AddLanguage pl .po" afin d'éviter toutes confusions avec l'extension standard des scripts perl.
Note 2: L'exemple ci-dessous illustre bien que les deux caractères du code de langage ne sont pas toujours identiques aux deux se rapportant à l'abréviation du code du pays.
Exemple : 'Danmark/dk' contre 'Danish/da'.
Note 3: Dans le cas de 'ltz', en utilisant 3 caractères, la norme RFC est violée. Mais une modification est en cours afin de régler ce problème et de suivre la référence du rfc1766.
Voici quelques codes :
Danemark (da) – Pays-Bas (nl) – Royaume-Uni (en) - Estonie (ee) - France (fr) – Allemagne (de) – Grèce (el) - Italie (it) - Corée (kr) - Norvège (no) - Norvège Nynorsk (nn) - Portugal (pt) - Luxembourg*(ltz) - Espagne (es) - Suède (sv) - Catalogne (ca) – Tchequie (cz) - Pologne (pl) - Brézil (pt-br) - Japon (ja) - Russie (ru).
Exemple de addlanguage :
AddLanguage da .dk
AddLanguage nl .nl
AddLanguage en .en
AddLanguage et .ee
AddLanguage fr .fr
AddLanguage de .de
AddLanguage el .el
AddLanguage he .he
AddCharset ISO-8859-8 .iso8859-8
AddLanguage it .it
AddLanguage ja .ja

LanguagePriority : vous permet d'assigner une priorité à certains langages en cas d'égalité lors d'une négociation. Listez simplement les langages dans l'ordre décroissant des préférences. Ici, les langues sont plus ou moins classés alphabétiquement. Vous voudrez probablement modifier cet ordre.
Par exemple : **LanguagePriority en da nl et fr de el it ja kr no pl pt pt-br ru ltz ca es sv tw**

AddType : vous permet de paramétrer le fichier mime.types sans pour autant l'éditer ou de définir certains fichiers comme étant d'autres types déjà déclarés.
Par exemple, le module PHP 3.x (ne fait pas partie intégrante de la distribution d'Apache - voir http://www.php.net) utilisera normalement:
AddType application/x-httpd-php3 .php3
AddType application/x-httpd-php3-source .phps
Et pour PHP 4.x:
AddType application/x-httpd-php .php
AddType application/x-httpd-php-source .phps

AddHandler : vous permet de définir certaines actions pour certains types d'extensions, actions sans rapport avec le type de fichier. Celles-ci peuvent être intégrées au serveur ou ajouter par la suite à la commande 'Action' (voir plus bas).
Si vous voulez utiliser des composants 'server side includes' (SSI), ou des scripts CGI en dehors des répertoires spécifiés sous ScriptAlias, supprimez le commentaire des lignes suivantes :
Pour utiliser les scripts CGI:
#AddHandler cgi-script .cgi
#AddHandler cgi-script .pl
Pour utiliser des fichiers HTML traités par le serveur:
AddType text/html .shtml
AddHandler server-parsed .shtml
Supprimez le commentaire de la ligne suivante afin d'activer l'option Apache 'send-asis' permettant d'envoyer des fichiers via le protocole HTTP.
#AddHandler send-as-is asis
Si vous désirez utiliser des image-maps traités par le serveur, activez cette ligne :
#AddHandler imap-file map
Afin d'activer l'utilisation des fichiers de type 'type-map', activez la ligne qu suit :
#AddHandler type-map var
Fin des directives définissant le type des documents.

Action : vous permet de définir les types de média qui exécuteront un script lorsqu'un fichier correspondant est demandé. Ceci élimine le besoin de répéter les chemin d'accès sous forme d'URL pour les CGI qui manipule beaucoup les fichiers.
Format: **Action media/type /cgi-script/localisation**
Format: **Action handler-nom /cgi-script/localisation**

MetaDir: spécifie le nom du répertoire dans lequel Apache pourra trouver les fichiers contenant les meta-informations. Ces fichiers contiennent des entêtes HTTP additionnels afin de les inclure lors de l'envoi du document.
Par exemple : **MetaDir .web**

MetaSuffix: spécifie l'extension des fichiers contenant les meta-informations.
Par exemple : **MetaSuffix .meta**

ErrorDocument : permet la paramétrisation des messages d'erreur (style Apache). Trois méthodes différentes existent
1) Messages de type 'plain text'
ErrorDocument 500 "Le serveur a effectué une erreur
Note : l'ouverture des guillemets (") permet de définir le message comme étant un texte simple, il ne faut pas les fermer.
2) Redirections locales
ErrorDocument 404 /missing.html afin de rediriger le client vers un document local /missing.html
Note: vous pouvez rediriger le client vers un script ou un document utilisant le server-side-include (SSI).
3) Redirections distantes
ErrorDocument 402 http://un.autre_serveur.com/subscription_info.html

Note: beaucoup de variables d'environnement associées à la requête originale ne seront "plus" disponible à un tel script.

Les directives suivantes modifient le comportement des réponses HTTP standards. La première directive désactive l'option keepalive pour Netscape 2.x et les navigateurs qui ne le supportent pas. Il est connu que des problèmes subsistent avec l'implémentation de ces navigateurs. La seconde directive est utilisé pour Microsoft Internet Explorer 4.0b2 dont l'implémentation d'HTTP/1.1 n'est pas correct et ne supporte pas correctement l'option keepalive quand celle-ci est utilisé pour les réponses de type 301 ou 302 (redirection).

```
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
```

La directive suivante désactive les réponses HTTP/1.1 pour les navigateurs ne répondant pas aux spécifications énoncées pour HTTP/1.0 en étant incapable de manier correctement une réponse basique 1.1.

```
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0
```

Pour générer un rapport sur le statut du serveur, accessible via l'URL http://nom_du_serveur/server-status, on écrit :

```
<Location /server-status>
   SetHandler server-status
   Order deny,allow
   Deny from all
   Allow from serveur.test
</Location>
```

Pour générer un rapport sur la configuration du serveur, accessible via l'URL http://servername/server-info (nécessite que mod_info.c soit chargé), on écrit :

```
<Location /server-info>
   SetHandler server-info
   Order deny,allow
   Deny from all
   Allow from serveur.test
</Location>
```

Note : Changez "serveur.test" afin que cette valeur coïncide avec le domaine depuis lequel vous voudrez voir ces informations.

c. section 3: hôtes virtuels (Virtual Hosts)

Les virtualhosts permettent de mettre plus d'un site web par IP, en les appelant par nom de domaine ou par IP. Ce qui permet d'avoir des centaines de sites sur un serveur n'ayant qu'une seule IP (c'est comme cela que font tous les hébergeurs, ils ne prennent pas une nouvelle IP pour chaque nouveau client hébergé).

Par exemple, votre serveur web héberge deux sites web d'url: www.domaine1.com et www.domaine2.com, et a comme adresse IP: 80.10.20.30, voici comment définir les deux VirtualHost:

NameVirtualHost 80.10.20.30
<VirtualHost 80.10.20.30>
ServerAdmin webmaster@domain1.com
DocumentRoot "C:/Program Files/Apache Group/Apache2/htdocs/domaine1"
ServerName www.domain1.com
ErrorLog logs/domain1-error.log
CustomLog logs/domain1-access.log combined
ServerAlias domain1.com
</Virtualhost>

<VirtualHost 80.10.20.30>
ServerAdmin webmaster@domain2.com
DocumentRoot "C:/Program Files/Apache Group/Apache2/htdocs/domaine2"
ServerName www.domain2.com
ErrorLog logs/domain2-error.log
CustomLog logs/domain2-access.log combined
ServerAlias domain2.com
</Virtualhost>

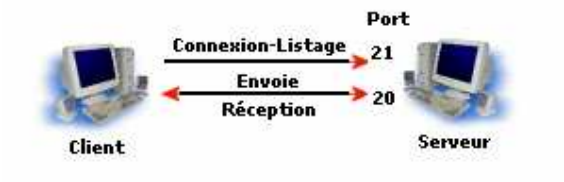
NameServer permet de définir sur quelle IP les virtualhosts sont définis. **<VirtualHost>** permet de définir un nouvel hôte virtuel apache, avec son adresse IP associée. En combinaison avec la directive ServerName il définit aussi le nom avec lequel le serveur doit être appelé. Cela signifie que si le serveur reçoit une requête sur son IP 80.10.20.30 avec le nom "www.domain1.com", le serveur va donc fournir les pages webs contenues dans C:/Program Files/Apache Group/Apache2/htdocs/domaine1 (grâce à la directive DocumentRoot).
De la même façon, il va fournir les pages de C:/Program Files/Apache Group/Apache2/htdocs/domaine2 si on appelle celle-ci avec l'url www.domain2.com.
Pour que cela fonctionne, il faut bien sur qu'un serveur DNS soit configuré pour faire pointer www.domain1.com et www.domain2.com sur l'IP 80.10.20.30.
Les directives ErrorLog et Customlog permettent de définir les fichier logs de chaque hôte virtuel (autrement les logs s'ajouteront aux logs principaux du serveur défini dans les directives en dehors de la directive <VirtualHost>.
ServerAlias permet d'indiquer sous quel autre nom l'hôte virtuel peut être appelé (ici domainX.com en plus de www.domainX.com), bien sur là aussi le serveur DNS doit être configuré pour faire pointer domainX.com sur 80.10.20.30
Une autre façon de faire des hôtes virtuels, si on n'a pas plusieurs noms de domaine, est de la faire par IP ou par IP et Port.
Par IP, il suffit de faire des **<VirtualHost ip1>** et **<VirtualHost ip2>** etc... , et par port il suffit de faire des **<VirtualHost ip:port1> <VirtualHost ip:port2>**
Il faut aussi des directives de Bind et Listen sur chaque IP et port supplémentaire (voir les directives Listen et Bind plus haut dans ce document).
Dans chaque virtualhost, vous pouvez aussi ajouter d'autres directives, comme les directives de ScriptAlias (pour l'exécution de cgi), de Directory (option des répertoires du site), ... En gros, toutes les directives peuvent être redéfinies dans chaque VirtualHost pour configurer le site web virtuel. Voir pour cela la documentation officielle d'apache. Pour chaque directive, il est spécifié si elle peut être utilisé dans un contexte de VirtualHost ou pas.

Voilà donc pour les principales directives utilisées dans **httpd.conf**. D'autre directives existent (voir la doc officielle), et les modules chargés par apache ajoutent eux aussi des directives spécifiques (voir la documentation du module ajouté).

V. Installer un serveur FTP avec IIS sous XP

1. Rappel

Le FTP est un protocole de transfert de fichiers.
Il s'agit du protocole optimal pour l'échange de fichiers entre utilisateurs.
Comme tout protocole d'échange il est constitué de 2 parties : le serveur et le client.
Le serveur écoute sur un port TCP donné (par défaut le port 21 appelé FTP Control) et attend que des clients s'y connectent. Une fois connecté, le client peut envoyer ou recevoir des données que le serveur met à sa disposition par le port TCP 20 par défaut appelé FTP Data.



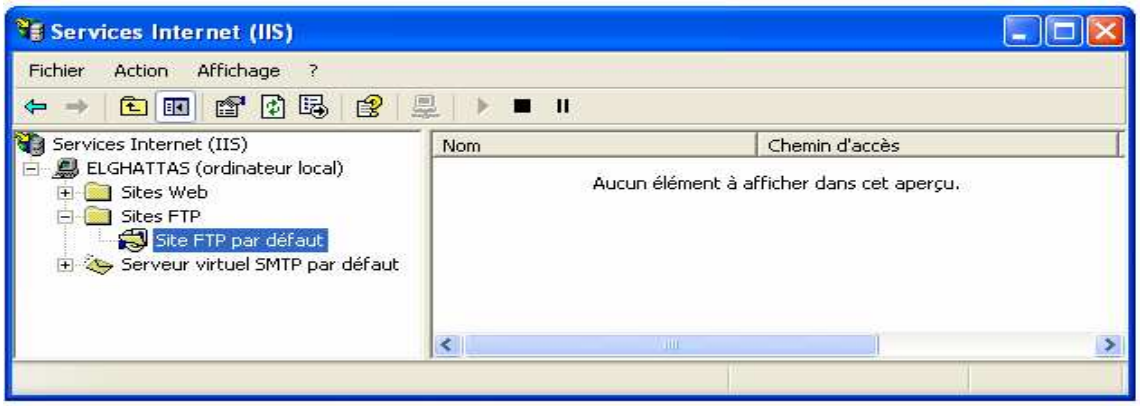
2. Installation de IIS

Vous devez tout d'abord installer le service IIS si vous ne l'avez pas déjà fait. (Voir II.2 Installation des composants IIS page 4)

3. Administration du serveur et configuration

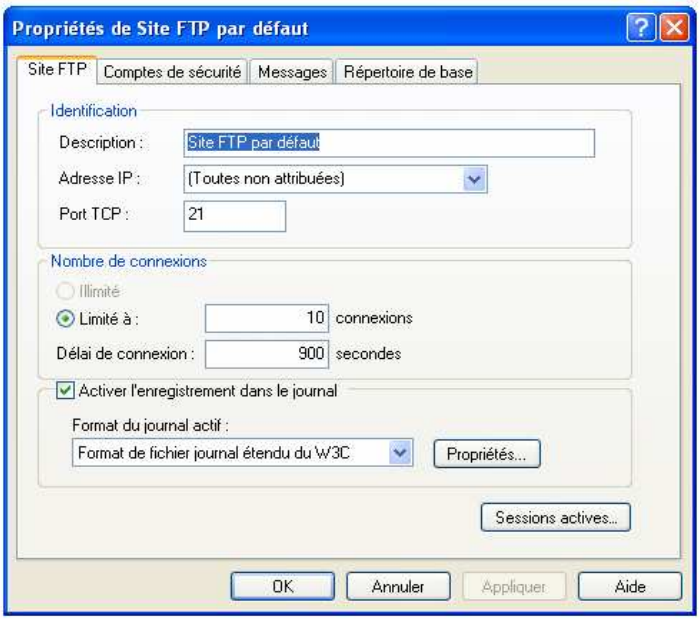
Pour cela, rendez vous dans le "**Panneau de configuration**", "**Outils d'administration**" et exécuter celui nommé "**Services Internet (IIS)**".

La fenêtre devrait ressembler à celle-ci :



Faites une clique droit sur **Site FTP par défaut** et choisissez **Propriétés**. Une nouvelle boîte de dialogue apparaît avec 4 onglets. Vous pouvez maintenant personnaliser votre serveur, nous allons étudier les différents onglets proposés.

3.1. Site FTP



Le premier onglet permet de définir les paramètres élémentaires du serveur.

Description

Fournit le 'nom' du site FTP. Il sert surtout pour l'organisation.

Adresse IP

Permet de restreindre le FTP à une IP particulière, par exemple quand le serveur a plusieurs IP (Intranet et Internet) pour ne le faire fonctionner que sur Internet. Par défaut, on le laissera à **(Toutes non attribuées)**

Port TCP

Port sur lequel écoute le serveur (21 est la valeur par défaut).

Nombre de connexions

La section nombre de connexion permet de restreindre le nombre de connexions simultanées que pourra supporter le serveur. Pour Windows XP et Windows 2000 Professionnel, ce nombre est limité à 10. Pour les versions Server des Windows, ce nombre peut-être illimité.

Délai de connexion

C'est le nombre de secondes d'inactivité au bout duquel un utilisateur est déconnecté. Cela permet de ne pas encombrer le serveur avec des connexions qui ne servent plus et à palier une défaillance du protocole FTP.

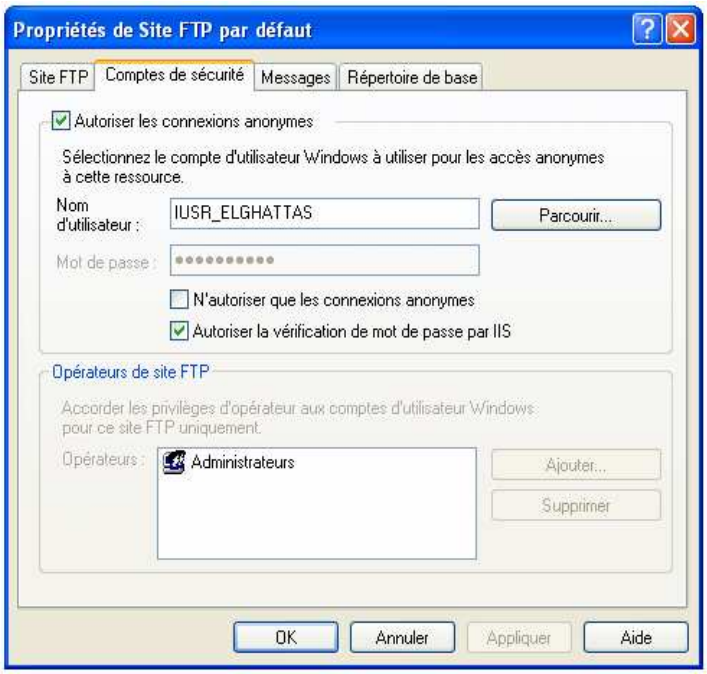
Activer l'enregistrement dans le journal

Cela permet d'avoir une trace de tout ce qui se passe sur le serveur FTP. Par défaut le format est celui du W3C. Il est possible d'enregistrer ce journal dans une base de données, mais uniquement avec les versions Servers de Windows.

Sessions actives

Cette fonction permet de connaître en temps réel les utilisateurs connectés au serveur FTP. Elle permet de les déconnecter si nécessaire.

3.2. Comptes de sécurité



Cet onglet permet de définir le niveau de sécurité au niveau du serveur FTP.

Autoriser les connexions anonymes

Permet à un utilisateur d'accéder au contenu du serveur FTP sans pour autant avoir un login et un mot de passe

Nom d'utilisateur

C'est le compte Windows utilisé pour les accès anonymes au FTP, il est de la forme IUSR_nomOrdinateur

Mot de passe

Entrez le mot de passe que vous voulez utiliser pour le compte des utilisateurs anonymes

N'autoriser que les connexions anonymes

Comme son nom l'indique, cette option n'autorise que les connexions anonymes. Si un utilisateur essaie de se connecter avec son login et son mot de passe, il échouera.

Autoriser la vérification du mot de passe par IIS

Elle permet une vérification des mots de passe directement par rapport aux comptes Windows. Quand elle est activée, il n'est plus possible de spécifier le mot de passe utilisé pour les connexions anonymes.

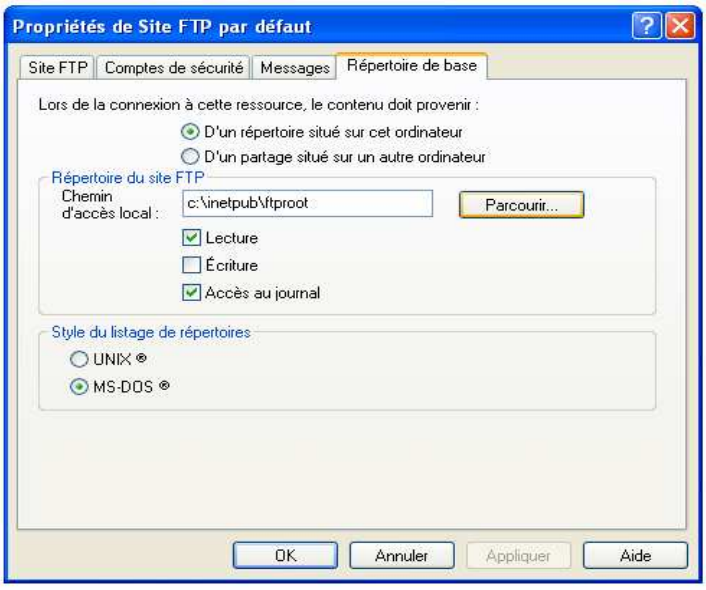
Opérateurs de site FTP

Il s'agit d'un groupe d'utilisateur avec des droits particuliers. Il ne peuvent modifier que les informations qui touchent au site FTP dont ils ont la responsabilité, pas au reste (IIS en lui même, le Windows qui héberge le IIS, ...)

3.3. Messages

C'est dans cet onglet que vous entrerez les messages que verront vos utilisateurs.
Bannière
Affiche un message au client lorsque le client FTP établit une connexion avec le serveur.
Bienvenue
Affiche un message au client lors de la première connexion au serveur.
Quitter
Affiche un message au client lorsque celui-ci se déconnecte du serveur.
Nombre maximal de connexions
Affiche un message apparaissant en retour de l'erreur 421 du protocole FTP, c'est à dire si un utilisateur essaye de se loger mais que le nombre maximal de connexions est déjà atteint.

3.4. Répertoire de base



L'onglet **Répertoire de base** est l'onglet où l'on configure le répertoire racine du FTP, c'est le répertoire que le visiteur verra en premier une fois connecté à votre serveur.

Origine du contenu

Répertoire situé sur cet ordinateur. Dans ce cas, il répertoire que sert à stocker les fichiers gérés par le serveur FTP sont situé cet ordinateur. Il est conseillé dans ce cas d'allouer une partition au serveur FTP pour diverses raisons (sécurité, mise en oeuvre)

Partage situé sur un autre ordinateur. Ici, le répertoire de stockage est situé sur un ordinateur du réseau. Pour spécifier le dossier ciblé, il faut utiliser UNC (Universal Naming Convention). Par exemple : \\serveurWeb\dossierftp

Chemin d'accès local

Entrer le nom du dossier cible en correspondance avec le choix fait dans **Origine du contenu**

Lecture

Permet de lire et/ou de télécharger le contenu du dossier

Ecriture

Permet d'écrire des fichiers dans le répertoire de stockage du serveur. Nous reviendrons plus en détail sur cette option plus tard.

Accès au journal

Indique au serveur qu'il doit inscrire tous les évènements relatifs à ce dossier dans le fichier journal.

Style du listage de répertoires

Cette option concerne principalement l'affichage des dates.

Dans les FTP, deux modes de listage existent : le mode Unix et le mode MS-DOS comme vous pouvez le voir.

- Exemple de listage d'un répertoire à la façon MS-DOS :
  11-29-06 03:35PM 7275 cours.doc
  11-26-06 01:42PM ftptest
- Exemple de listage d'un répertoire à la façon Unix :
  -rwxrwxrwx 1 owner group 7275 Nov 29 15:35 cours.doc
  drwxrwxrwx 1 owner group 0 Nov 26 13:42 ftptest

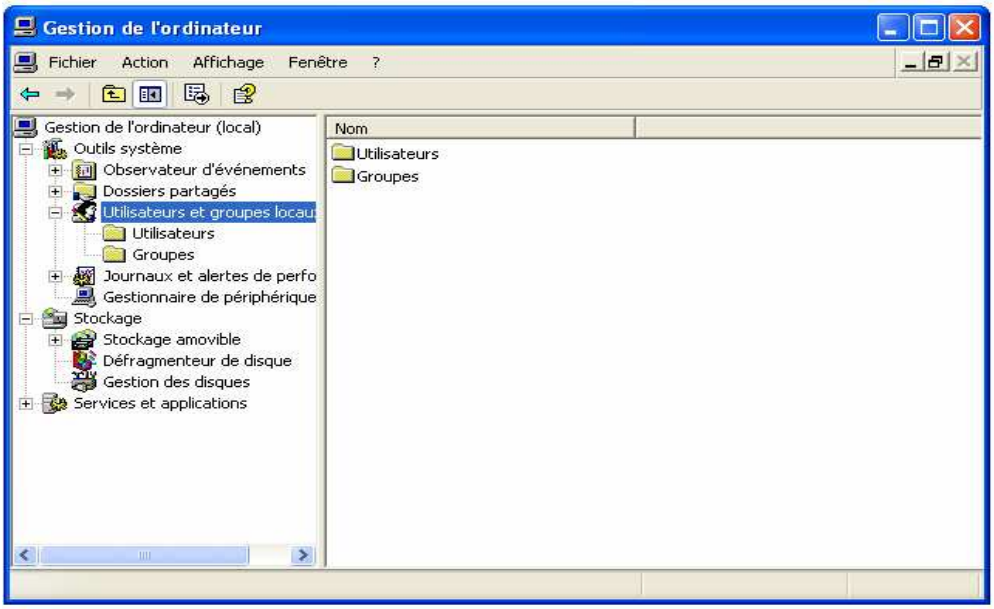
4. Création d'un serveur avec droits d'accès

Dans cet exemple, on créera des espaces réservés. C'est à dire que seulement certains utilisateurs auront accès à ces répertoires, en accès complet, c'est-à-dire lecture et écriture.

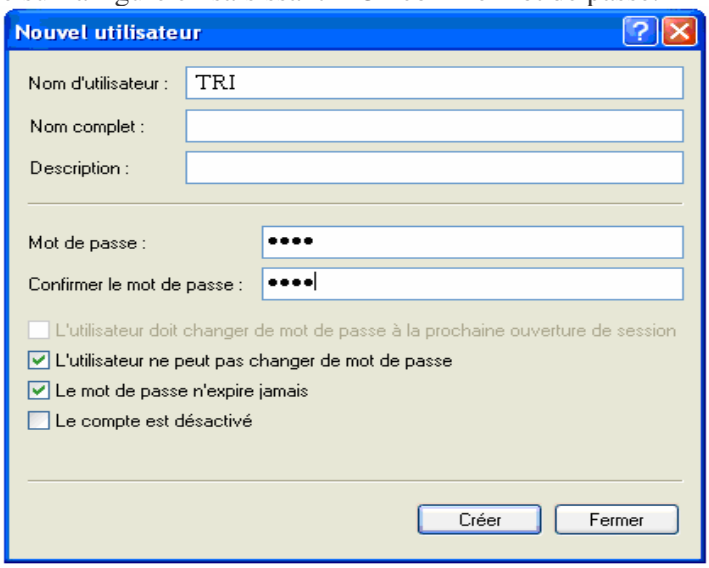
4.1. Préparatifs

Pour commencer, il y a une opération à effectuer avant toute chose : désactiver le partage simple en vigueur par défaut sous Windows XP. Pour cela aller dans le **Panneau de configuration -> Options des dossiers -> Affichage** et décocher l'option **Utiliser le partage des fichiers simple (recommandé)**.

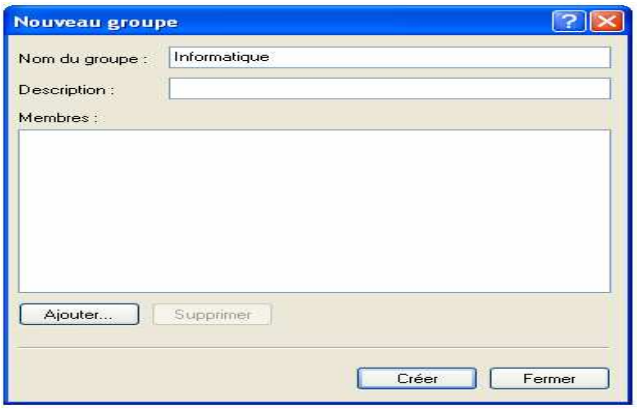
Ensuite, on va créer des comptes et un groupe d'utilisateurs pour notre exemple. Aller dans **Démarrer -> Panneau de configuration -> Outils d'administration -> Gestion de l'ordinateur**. Développez ensuite l'arboresence **Gestion de l'ordinateur (local) -> Outils système -> Utilisateurs et groupes locaux**.



On va maintenant créer un utilisateur **TRI**. Pour cela, faites un clic droit sur **Utilisateurs** et choisissez **Nouvel utilisateur ...** Une fenêtre qui ressemble à la suivante s'ouvre. Remplissez la comme indiquée sur la figure en saisissant **1234** comme mot de passe.

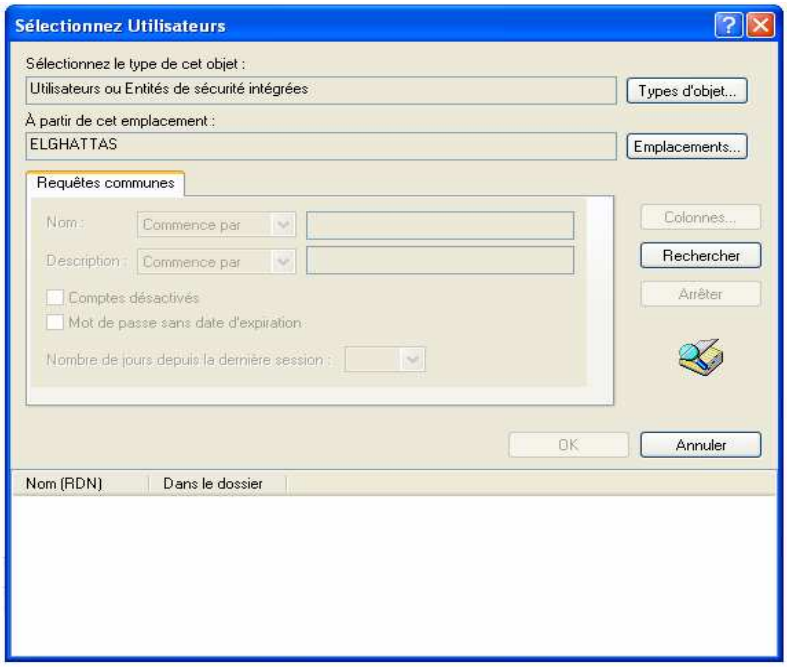


Validez en cliquant sur **Créer** puis fermez cette fenêtre. Cliquez sur **Utilisateurs** et vous pouvez voir **TRI** qui apparaît dans la liste des utilisateurs à droite.
De la même manière créer 2 autres utilisateurs que vous appellerez **TDI** et **TSB**.
Passons maintenant à la création du groupe d'utilisateurs. Comme pour ajouter un utilisateur, ouvrez le menu contextuel du **Groupes** et choisissez **Nouveau groupe ...** Une fenêtre qui ressemble à la suivante s'ouvre. Remplissez la de la même façon que la figure suivante :



Il faut maintenant ajouter TDI et TSB, les 2 utilisateurs qui feront parti du groupe d'utilisateurs **Informatique**. Pour cela, cliquer sur **Ajouter ...** et une nouvelle fenêtre s'ouvre.

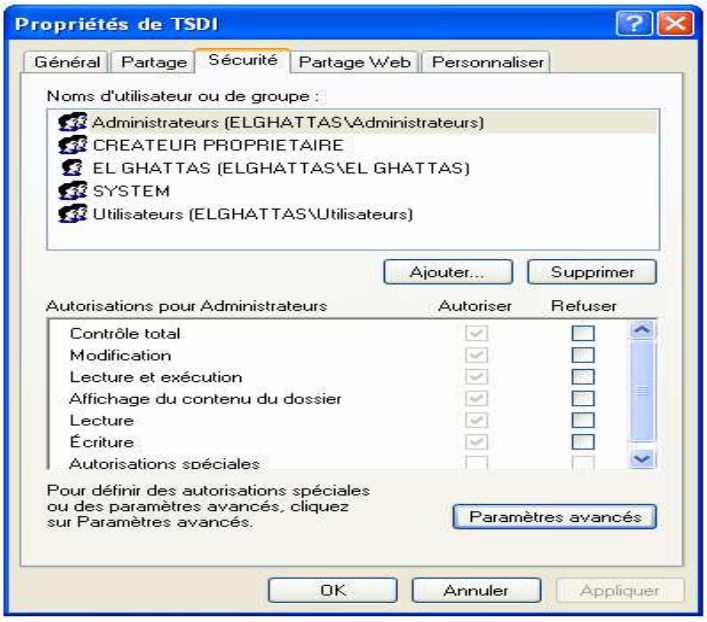
2 possibilités s'offrent à vous pour ajouter TDI et TSB. La première est de saisir directement les noms d'utilisateurs dans la case **Entrez les noms des objets à sélectionner** en les séparant par des ; sinon, choisissez l'option **Avancé ...** et une nouvelle fenêtre s'ouvre.



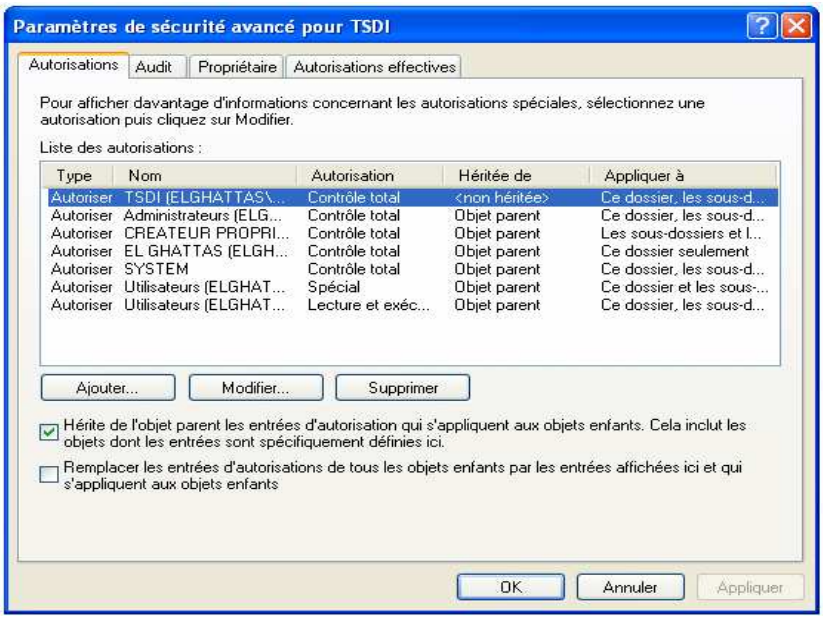
Cliquez sur **Rechercher** pour obtenir la liste de tous les utilisateurs et groupes d'utilisateurs présents sur cet ordinateur. Choisissez dans la liste TDI et TSB et cliquez sur **OK**. Cliquez une deuxième fois sur **OK** dans la boîte de dialogue de la figure précédente.
Cliquez maintenant sur **Créer** puis sur **Fermer** dans la boîte de dialogue **Nouveau groupe**. Votre groupe d'utilisateurs Informatique est crée et TDI et TSB en font parti.
On va maintenant créez un dossier TRI (C:\Inetupb\ftproot\TRI) et un dossier Informatique (c:\Inetupb\ftproot\Informatique).

4.2. Paramétrage du répertoire réservé à TRI

Allez maintenant dans les propriétés du dossier TRI (C:\Inetpub\ftproot\TRI) et dans la section Sécurité. Vous devriez obtenir ceci :



Cliquez sur maintenant sur **Ajouter ...** dans la fenêtre juste en haut. Vous obtenez le même genre de fenêtre que celle pour ajouter des utilisateurs ou groupes. Ajoutez TRI et validez. TRI apparaît maintenant dans la liste **Noms d'utilisateur ou de groupe**. Sélectionnez TRI et cochez la case Contrôle total dans la colonne **Autoriser**. Toutes les cases à cocher du dessous deviennent cochées.
Allez maintenant dans **Paramètres avancés**. Vous obtenez la fenêtre suivante :



Sélectionner maintenant Tout le monde et décocher la case **Hérite de l'objet parent les entrées ...** Une boite de dialogue s'ouvre, cliquez sur **Supprimer**.
Allez ensuite dans l'onglet **Propriétaire** et cliquez sur **Administrateurs**. Cochez la case **Remplacer le propriétaire des sous-conteneurs et des objets**. Cliquez sur **OK**. Une boite de dialogue s'ouvre vous indiquant que vous n'avez pas les autorisations de lire dans ce répertoire. Cliquez sur **Oui**.
Validez la boîte de dialogue précédente en cliquant sur **OK**.
TRI est maintenant le seul à avoir accès à ce dossier depuis le FTP, avec les utilisateurs appartenant au groupe administrateurs.

4.3. Paramétrage du répertoire réservé aux invités spéciaux

Cette opération est exactement la même que pour le répertoire réservé à l'utilisateur TRI, mais au lieu d'utiliser l'utilisateur TRI, on utilisera le groupe de travail Informatique, et au lieu du répertoire C:\Inetupb\ftproot\TRI, on prendra le répertoire C:\Inetupb\ftproot\Informatique.
Et Voici notre configuration du serveur FTP fini. S'il lui arrive un jour de planter, exécuter la commande **iisreset**. Elle fera redémarrer tout le serveur IIS, c'est à dire le serveur FTP, mais aussi tous ceux qui dépendent de IIS.

VI. Création d'un serveur FTP avec BulletProof FTP Server

Dans cette partie nous allons mettre en place un serveur FTP avec le logiciel BulletProof FTP Server, vous pouvez utiliser un autre logiciel de serveur FTP (FileZila Server,…), le principe est en gros le même.

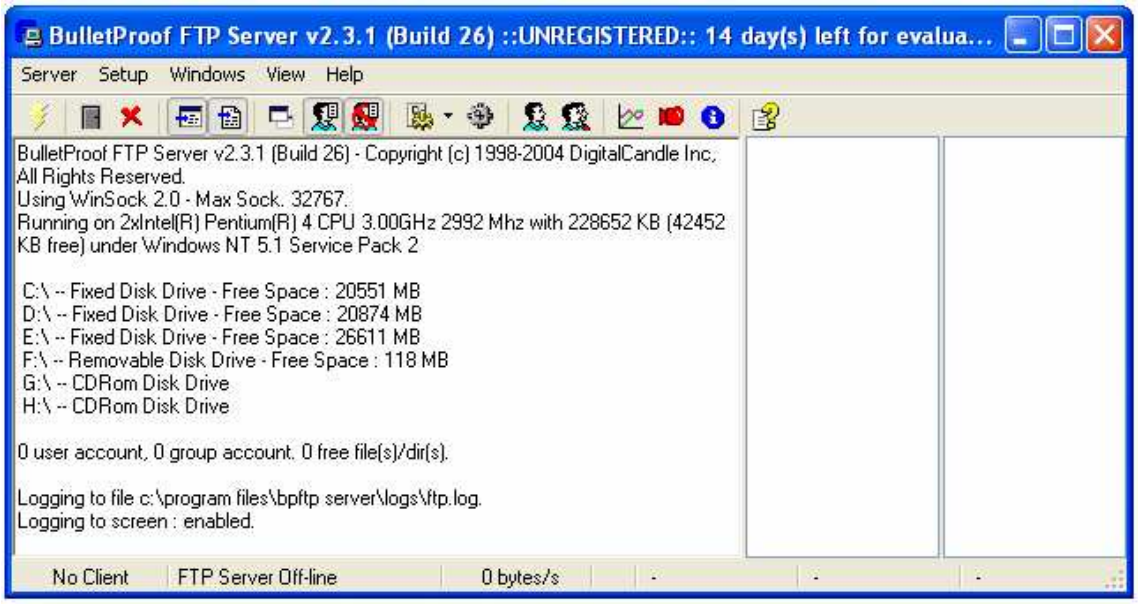
1. Introduction à BulletProof FTP Server

BulletProof FTP Server est le successeur du logiciel serveur FTP: "G6 FTP server". Il permet à n'importe quel utilisateur sous Windows de créer et configurer son propre serveur FTP et cela assez facilement. Ce logiciel est d'une simplicité pour tous ceux qui souhaitent monter un petit serveur privé chez eux ou échanger des données.
Vous pouvez le trouver là : http://www.bpftpserver.com/

BulletProof FTP Server vous permet de mettre un serveur en ligne. Il permet à des personnes qui veulent faire des échanges avec vous d'accéder à une partie de votre PC que vous aurez définie auparavant.

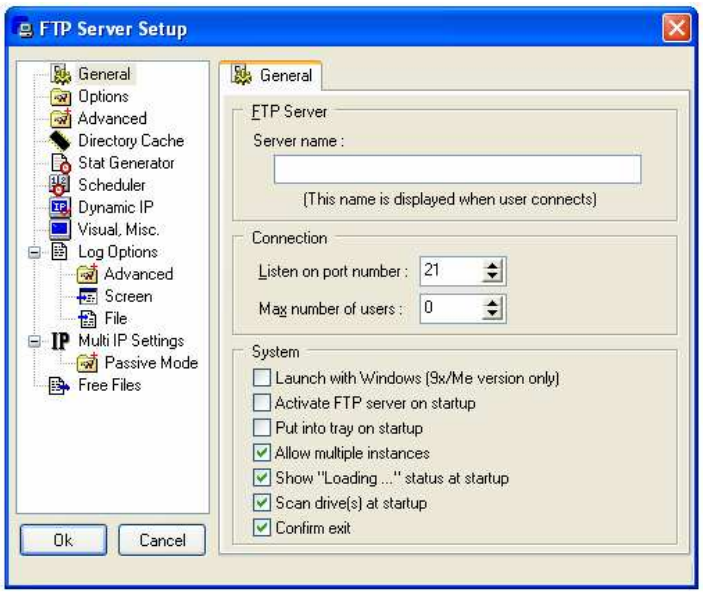
2. Configuration

Après avoir téléchargé sur le site officiel "bpftpserver_install.exe", Installez "BulletProof FTP Server v2.3.1 (Build 26)", une fois installé vous aurez l'interface suivante :



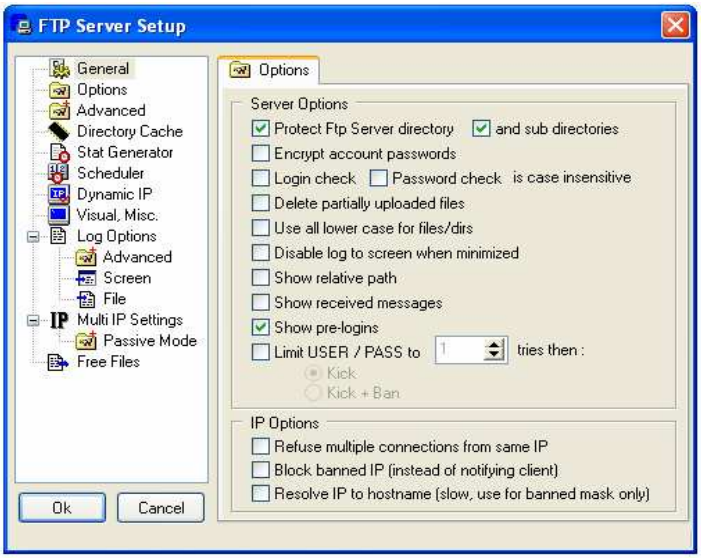
a. Configuration générale

Pour configurer votre serveur nous allons voir comment cela se paramètre afin de vous permettre de le mettre en route, on se limitera à la configuration des principaux éléments.
Faites "**Ctrl+m**" ou allez dans "**Setup**" puis "**Main**" et ensuite "**General**", vous arriverez dans ces trois cas sur cette fenêtre :



Server name
Comme son nom l'indique entrez ici le nom que portera votre serveur FTP.
Listen on port number
Indique au serveur le port TCP sur lequel il va travailler. Par défaut le port du FTP est le 21, ce que nous ne vous conseillons pas, d'une part pour éviter les tentatives de piratage, et de plus certains FAI ne le permettent pas dans le contrat. Le port 27015 est souvent utilisé par certains jeux en réseau, il est donc normal que du trafic soit présent sur ce port. Par contre, l'avantage du 21, c'est que c'est le port par défaut d'un service FTP dans tous les clients FTP, si vous changez le port, pensez à indiquer à vos utilisateurs le numéro de port à utiliser.
Max number of users
Définit le nombre maximum d'utilisateurs simultanés qui peuvent se connecter en même temps. Attention à votre bande passante !! Si vous avez l'ADSL 512, le débit montant est de 128 Kbits/s. Il faudra donc diviser ce débit par le nombre d'utilisateurs simultanés pour connaître leur débit de téléchargement. Ainsi 2 utilisateurs simultanés pourront télécharger à 64 Kbits/s chacun (en moyenne). Si vous voulez un nombre illimité d'utilisateurs laisse ce champ à 0.
Launch with Windows (9x/Me version only)
Cette option active le chargement du FTP dès le démarrage de Windows (uniquement pour Windows 95, 98 et Me).
Activate FTP server on startup
Cochez cette option si vous souhaitez que le serveur FTP se mette de lui-même "online" dès le démarrage de BulletProof FTP Server.
Put into tray on startup
Cochez cette case si vous souhaitez que BulletProof FTP se mette à son démarrage dans la barre de notification de Windows près de l'horloge de Windows.

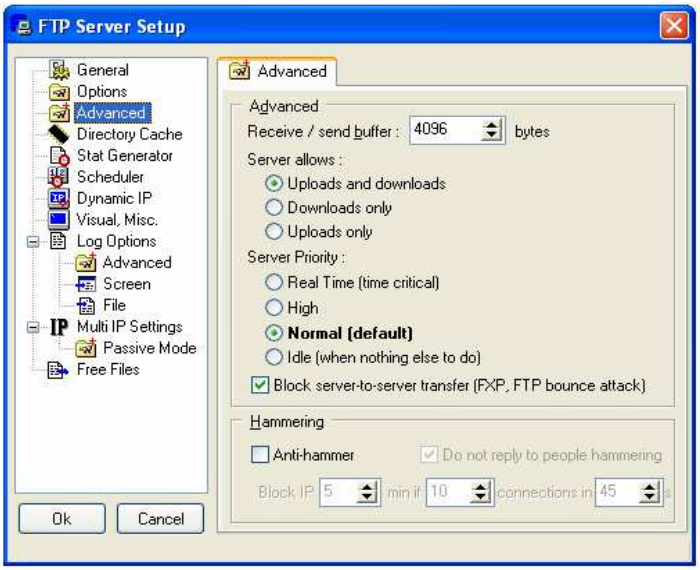
b. Configuration des options
Cliquez sur **Setup->Main->Options**.



Protect FTP Server directory and sub directories
Permet de protéger les répertoires d'installation de BulletProof FTP Server en empêchant toute activité FTP dans ces répertoires.

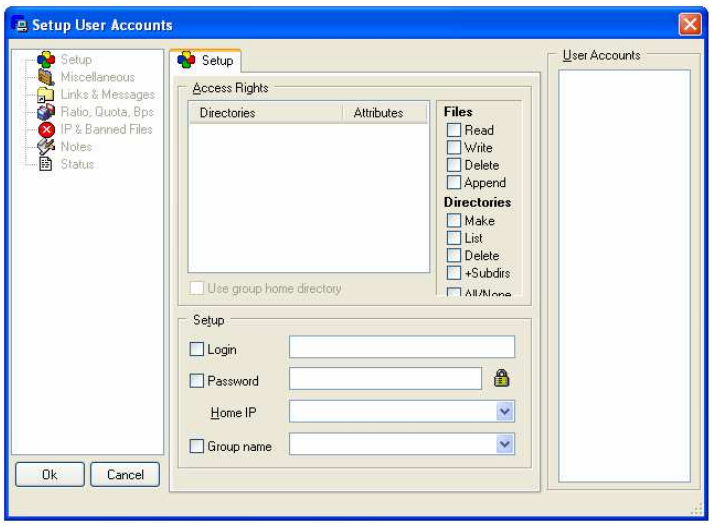
Login check et Password check is case insensitive
Permet de différencier les minuscules des majuscules dans les logins et / ou mot de passe.
Show relative path
Pour ne pas présenter l'arborescence réelle de votre disque dur.
Refuse multiple connections from same IP
Empêche les utilisateurs de se connecter plusieurs fois simultanément et donc de prendre la place de tout le monde et utiliser toute la bande passante.

c. Configuration des options avancées
Cliquez sur **Setup->Main->Advanced**

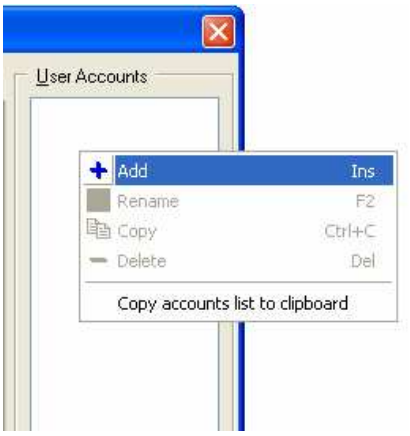


C'est la dernière boîte de dialogue de configuration utile directement, puisque c'est ici que vous pouvez gérer le hammering. Une personne n'ayant pas d'accréditation pour rentrer sur votre serveur peut en effet régler son client FTP pour qu'il refasse une requête à chaque seconde, ce qui peut s'avérer très gênant, surtout si vous êtes un peu limite en ressources système. Parce qu'une requête est reçue par le serveur, traitée puis refusée, il y a un risque de plantage du service et / ou du système à la clef. Cochez donc la case **anti-hammer** puis affinez le réglage par défaut (bloque l'IP 5 minutes s'il y a 10 tentatives en moins de 45 secondes).
Block server-to-server transfer (FXP, FTP bounce attack)
Cochez cette case pour empêcher le transfert de votre serveur FTP à un autre Serveur FTP (et vice versa). Voilà, le reste vous le découvrirez par vous-même si le besoin s'en fait sentir. Passons maintenant à l'ouverture de comptes utilisateurs : en bref les autorisations pour savoir qui est autorisé ou non à accéder aux parties que avez décidé de votre disque dur.

d. Création des comptes utilisateurs
Pour que votre serveur soit accessible aux utilisateurs, il faut leur créer un compte. Pour cela retournez dans le menu **Setup**, puis cliquez sur **User Accounts**. La boîte de dialogue suivante s'ouvre alors.



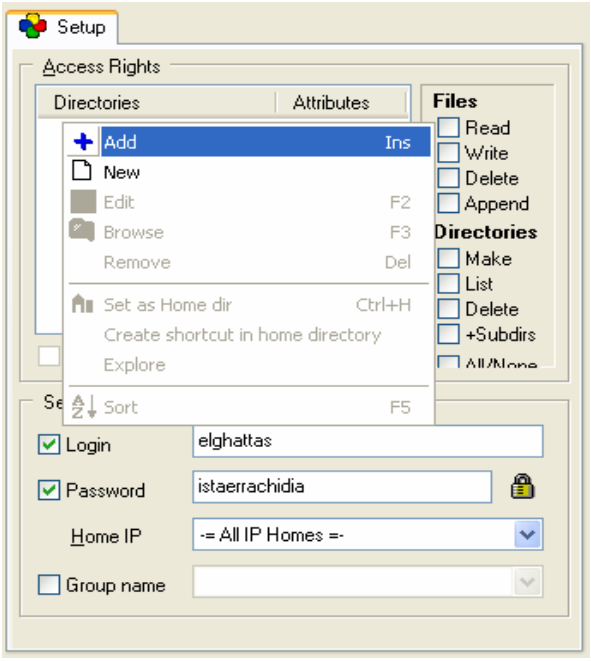
Dans la colonne intitulée **User Accounts,** cliquez avec le bouton droit de la souris, puis choisissez l'option **Add**.



Donnez ensuite le nom que vous souhaitez au compte, **elghattas** par exemple.

Par défaut, BulletProof FTP assigne un nom d'utilisateur (login) et un mot de passe (password) aléatoires à chaque nouveau compte utilisateur. Vous devrez transmettre ces informations aux personnes à qui vous souhaitez donner accès à votre serveur FTP.
Pour les modifier, changer la valeur des champs **Login** et **Password**.
Bien entendu, rien ne vous empêche d'autoriser les connexions anonymes, c'est à vous de voir ce que vous souhaitez faire de votre serveur FTP. Pour cela, il vous suffit de décocher les cases Login et Password.

A présent nous allons donner à l'utilisateur, la partie qu'il verra quand il se connectera sur le serveur FTP. Il vous suffit pour cela de cliquer droit dans la partie "**Access Rights**" et de faire "**Add**".



Vous aurez cette fenêtre :

Vous devrez alors choisir le dossier auquel aura accès les utilisateurs qui se connecteront à votre serveur FTP.
Vous pouvez définir les droits des utilisateurs à l'aide des cases à cocher de la rubrique **Access Rights**. Sélectionnez votre dossier dans la liste pour configurer les droits des utilisateurs.
Files
Read : Autoriser les utilisateurs à télécharger les fichiers qui se trouvent dans le dossier de FTP.
Write : Autoriser les utilisateurs à envoyer (upload) des fichiers dans votre dossier.
Delete : Autoriser les utilisateurs à supprimer un fichier.
Append : Autoriser la reprise des téléchargements et envois interrompus (resume).
Directories
Make : Autoriser les utilisateurs à créer des dossiers sur votre serveur.
List : Autoriser les utilisateurs à voir les dossiers de votre serveur.
Delete : Autoriser les utilisateurs à supprimer un dossier
+Subdirs : Autoriser les utilisateurs à parcourir l'arborescence de votre serveur, en entrant dans les sous-dossiers.

Cliquez ensuite sur la rubrique **Miscellaneous.**
La première chose à effectuer, c'est de mettre une limite aux nombres d'utilisateurs qui peuvent se connecter avec un compte unique.
Pour cela, cochez la case **Max no. of user** puis saisissez le nombre d'utilisateurs maximums que sous souhaitez autoriser.
Pour déconnecter les personnes du serveur FTP qui ne sont pas actives au bout d'un certain laps de temps, cochez la case **Enable time-out** puis définissez le temps en secondes avant de les déconnecter. Cela vous permettra ainsi de laisser la place aux utilisateurs qui attendent pour se connecter à votre serveur FTP.

3. Mise en ligne
Maintenant que tout est configuré, il ne vous reste plus qu'à mettre en ligne votre serveur FTP, c'est à dire le rendre accessible aux autres utilisateurs.
Pour cela, rien de plus simple, cliquez sur le menu **Server** puis sur **Go On-line**. Une icône vient se loger dans la barre de notification à côté de l'horloge. Cette icône est jaune pour indiquer que le serveur est en ligne, et rouge s'il est déconnecté.
Pour tester votre serveur FTP en local, ouvrez votre client FTP ou votre navigateur Web puis connectez vous à l'adresse IP : 127.0.0.1 en indiquant le nom d'utilisateur et le mot de passe de connexion que vous avez définis auparavant. Vous êtes sur votre serveur FTP !
Vous n'avez alors plus qu'à indiquer à vos correspondants votre adresse IP et leurs comptes (pas 127.0.0.1 qui correspond au localhost) pour qu'ils puissent accéder à votre serveur FTP par un client FTP ou par un navigateur.

A. EL GHATTAS
Errachidia, Le 19/10/2008