

Travaux pratiques 8.1.3 Sécurisation des données locales et des données transmises

Objectifs

- Utiliser le système d'autorisations NTFS (New Technology Files System) de Windows pour sécuriser les données locales sur un ordinateur exécutant Windows XP Professionnel
- Utiliser Internet Explorer 7 pour accéder à des sites Web sécurisés

Contexte / Préparation

Ces travaux pratiques se divisent en deux parties qui peuvent être réalisées ensemble ou séparément.

Partie 1 : sécurisation des données locales

Dans la première partie, vous allez sécuriser des données stockées sur un ordinateur utilisant le système de fichiers NTFS.

Scénario : dans une petite entreprise, deux utilisateurs partagent la même station de travail. Des données confidentielles sont stockées localement sur le disque dur de cet ordinateur. Il vous est demandé d'aider les utilisateurs à protéger et à sécuriser les données de manière à ce qu'elles ne soient accessibles que par un seul d'entre eux localement. Vous allez les sécuriser à l'aide des autorisations NTFS.

Les deux utilisateurs sont Bob et Joe. Bob a besoin d'un accès de type Modifier au dossier appelé « Documents de Bob » situé dans un autre dossier appelé « Données locales » sur le lecteur C. Joe ne doit pas pouvoir accéder au dossier « Documents de Bob ».

Partie 2 : identification d'un canal de communication sécurisé pour la transmission de données sur Internet

Dans la deuxième partie, vous allez utiliser Internet Explorer pour identifier les sites Web sécurisés et non sécurisés.

Scénario : vous êtes chargé de former les utilisateurs finaux d'une petite entreprise pour qu'ils puissent accéder aux sites Web de manière sécurisée. Vous allez leur enseigner comment distinguer un site Web légitime et sécurisé d'un site Web illégitime et non sécurisé.

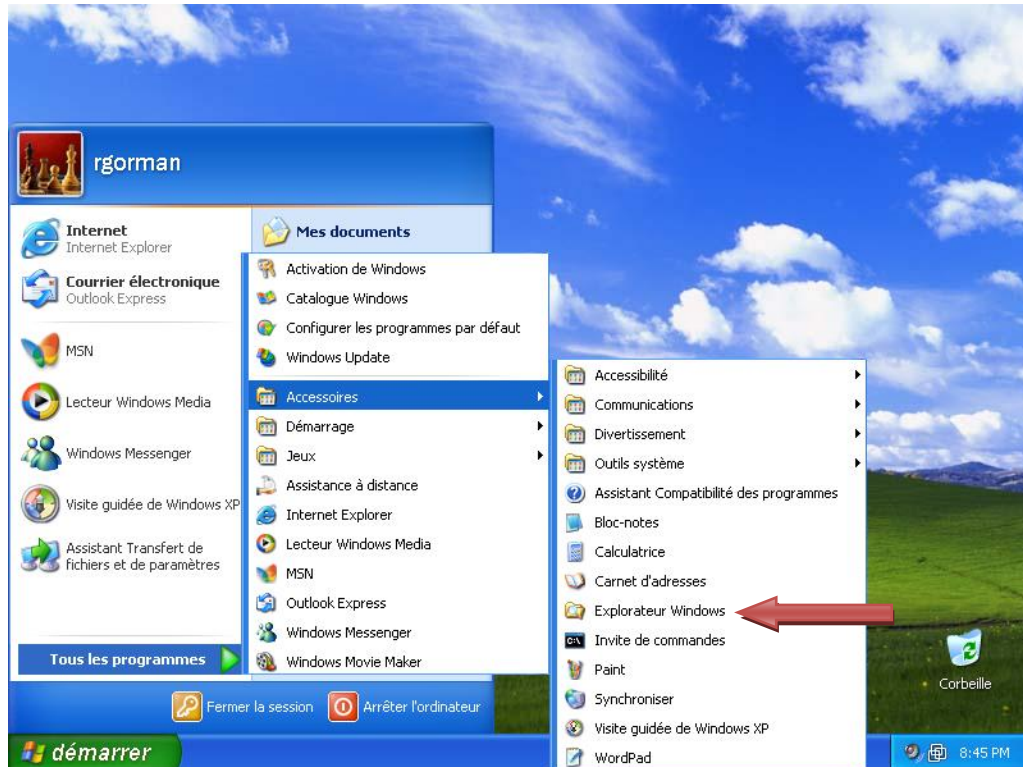
Ressources nécessaires :

- un ordinateur exécutant Windows XP Professionnel avec droits d'accès en tant qu'administrateur ;
- cet ordinateur doit utiliser le système de fichiers NTFS où le partage de fichiers est désactivé (sous les options des dossiers de l'Explorateur Windows) ;
- des comptes utilisateur préconfigurés pour les utilisateurs Bob et Joe ;
- une connectivité Internet.

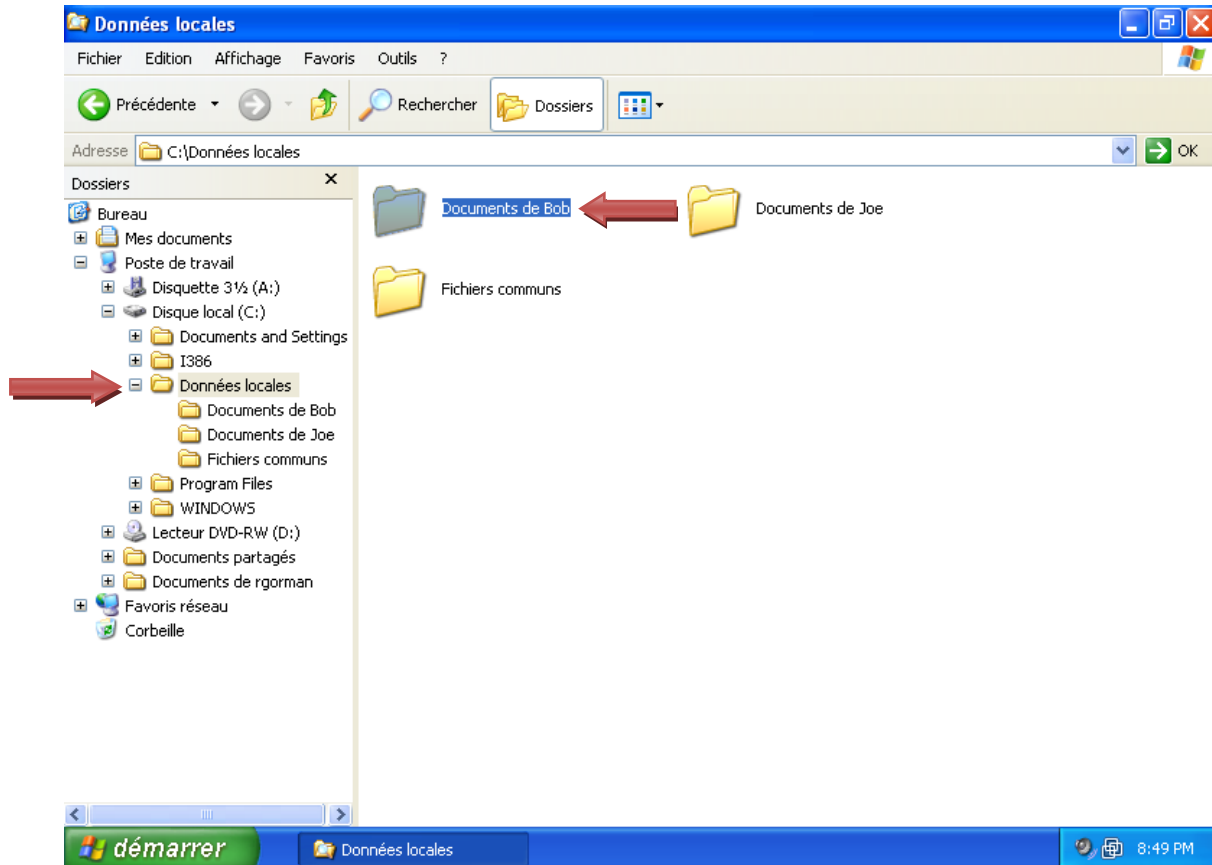
Partie 1 : sécurisation des données locales

Étape 1 : sécurisation du dossier Documents de Bob

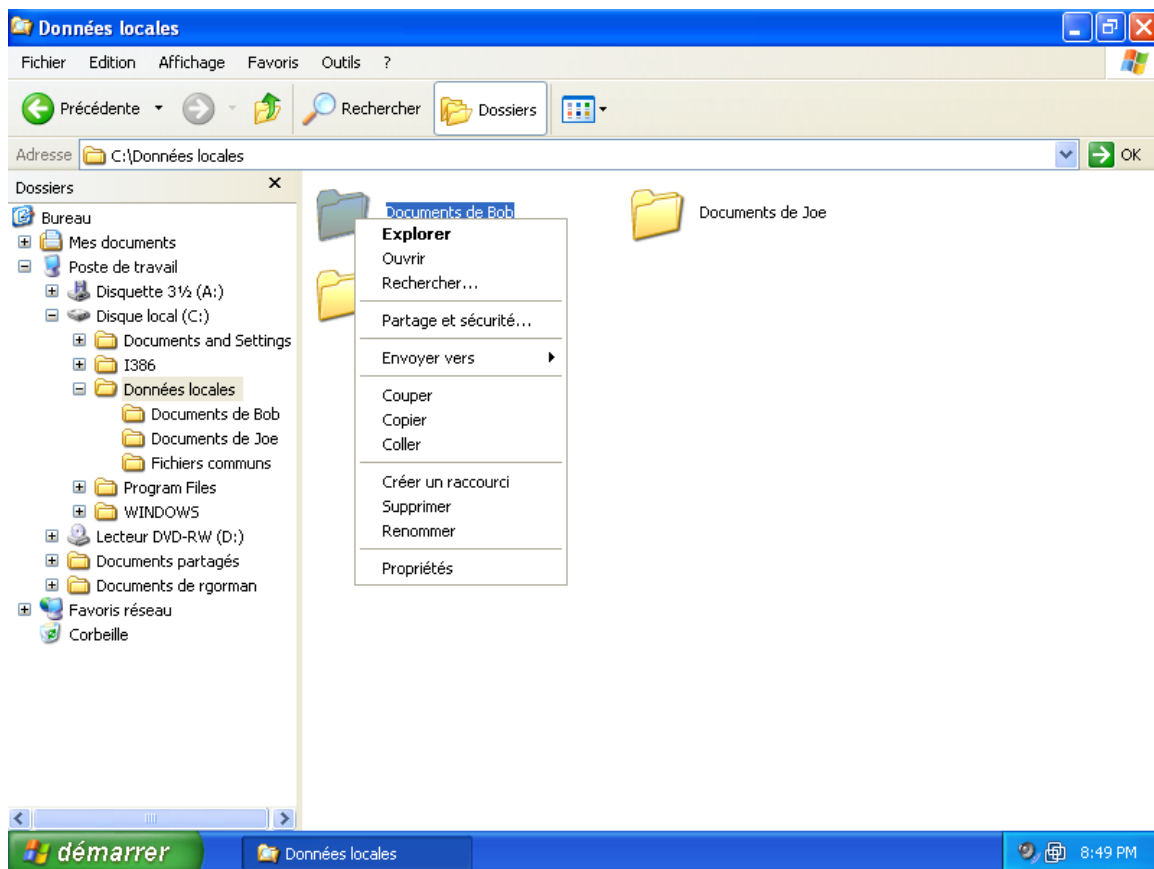
- Ouvrez une session en tant qu'administrateur sur l'ordinateur exécutant Windows XP.
- À partir du menu **Accessoires**, lancez l'Explorateur Windows.



- c. Utilisez l'Explorateur Windows pour créer le dossier **Données locales** sur le disque local (C:). Dans le menu **Fichier**, cliquez sur **Nouveau**, puis sur **Dossier**.
- d. Cliquez sur le dossier **Données locales**, puis cliquez avec le bouton droit de la souris dans la zone ouverte sur la partie droite de l'écran. Cliquez sur **Nouveau**, puis sur **Dossier** pour créer le dossier **Documents de Bob**. Répétez ce processus pour créer les dossiers **Fichiers communs** et **Documents de Joe**.
- e. Accédez au dossier **Données locales**, dans lequel vous pouvez voir le dossier **Documents de Bob**.

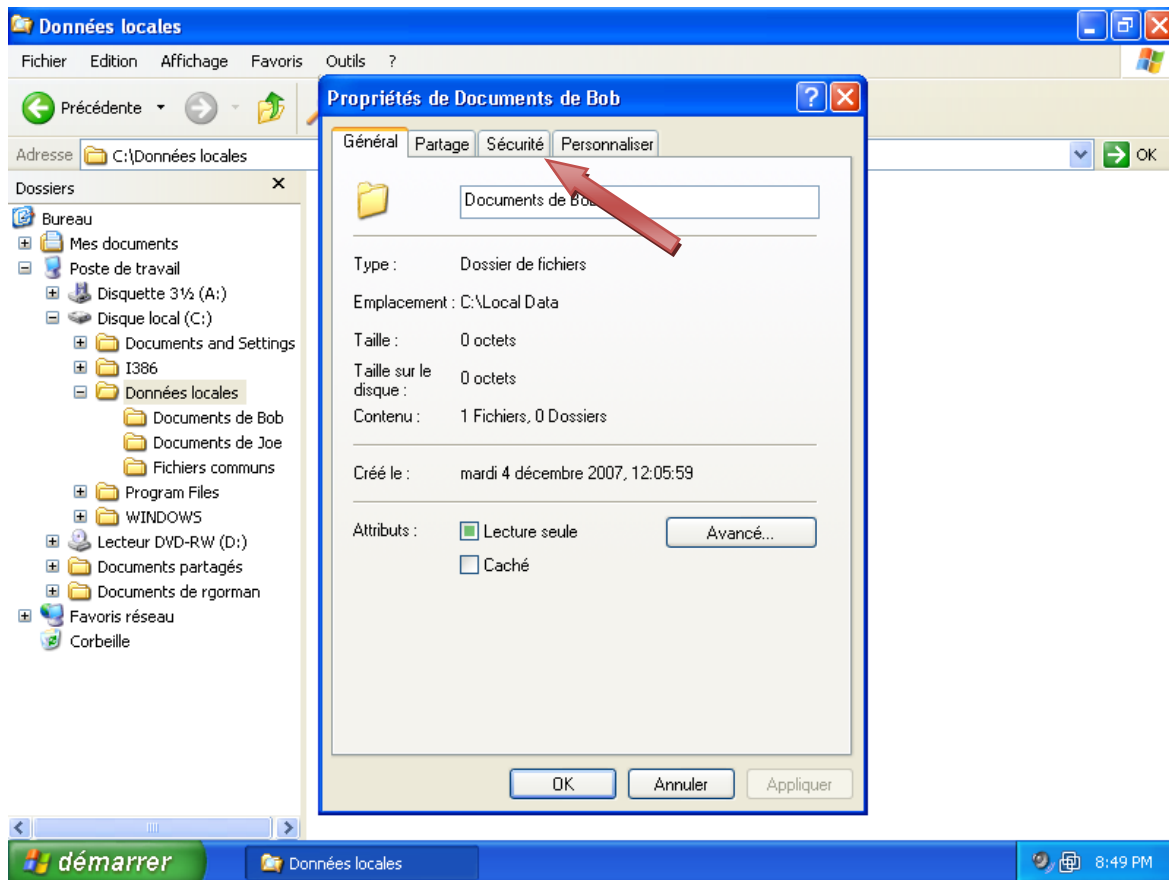


- f. Cliquez avec le bouton droit de la souris sur le dossier **Documents de Bob** et choisissez **Propriétés**.

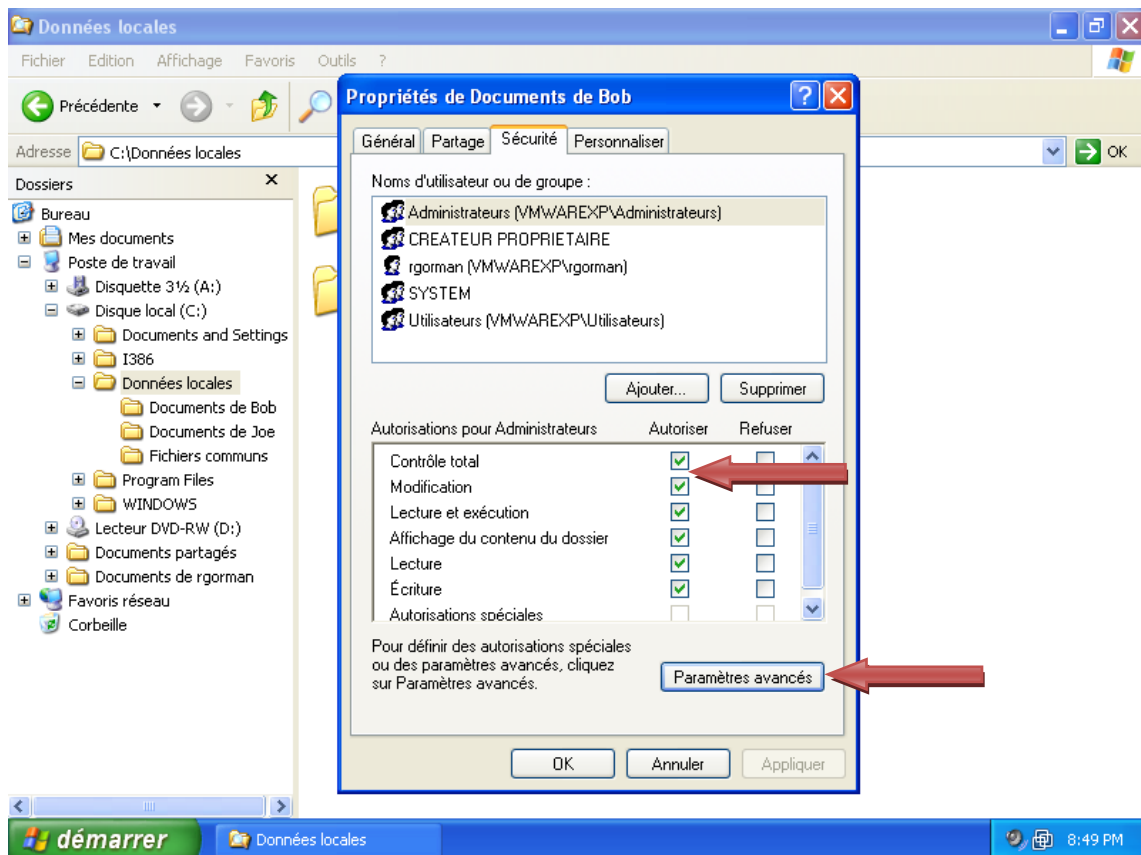


- g. Dans la boîte de dialogue **Propriétés de Documents de Bob**, cliquez sur l'onglet **Sécurité**.

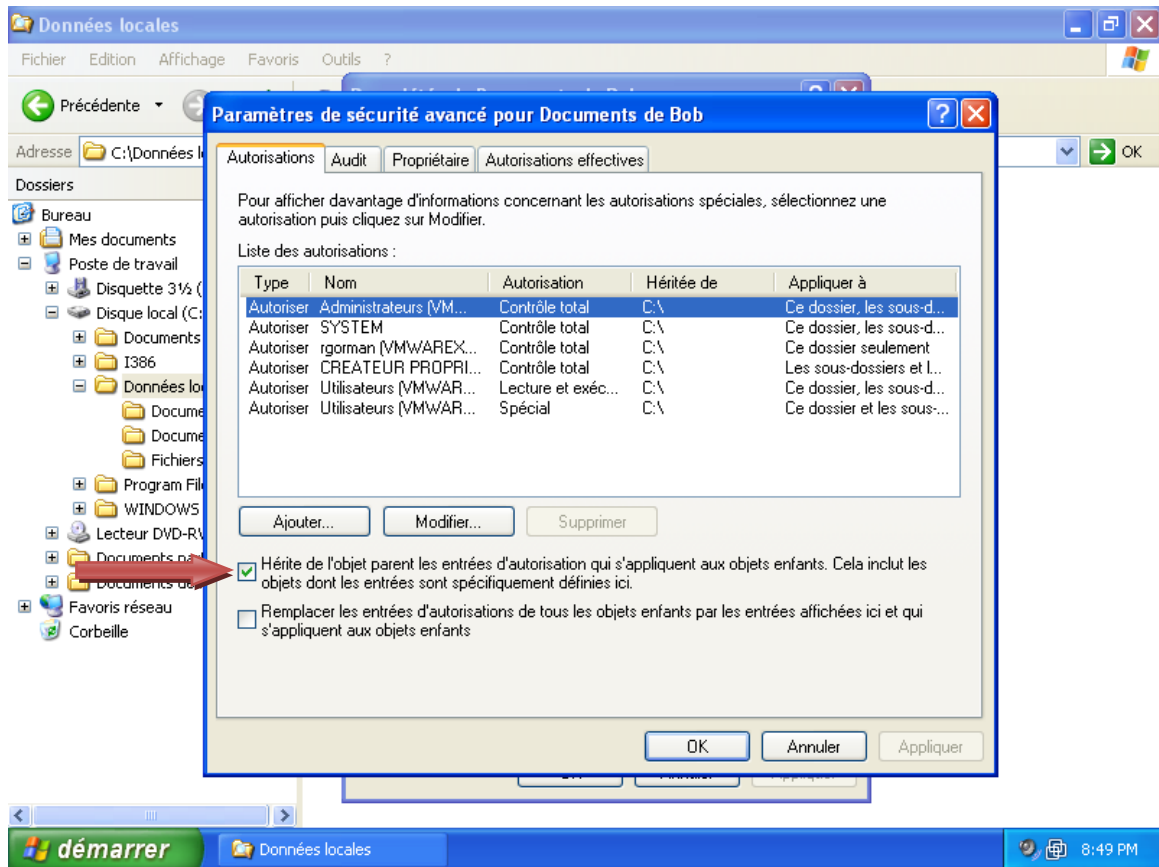
REMARQUE : le système de fichiers NTFS doit être installé sur le lecteur sur lequel vous travaillez, sinon l'onglet **Sécurité** ne s'affiche pas.



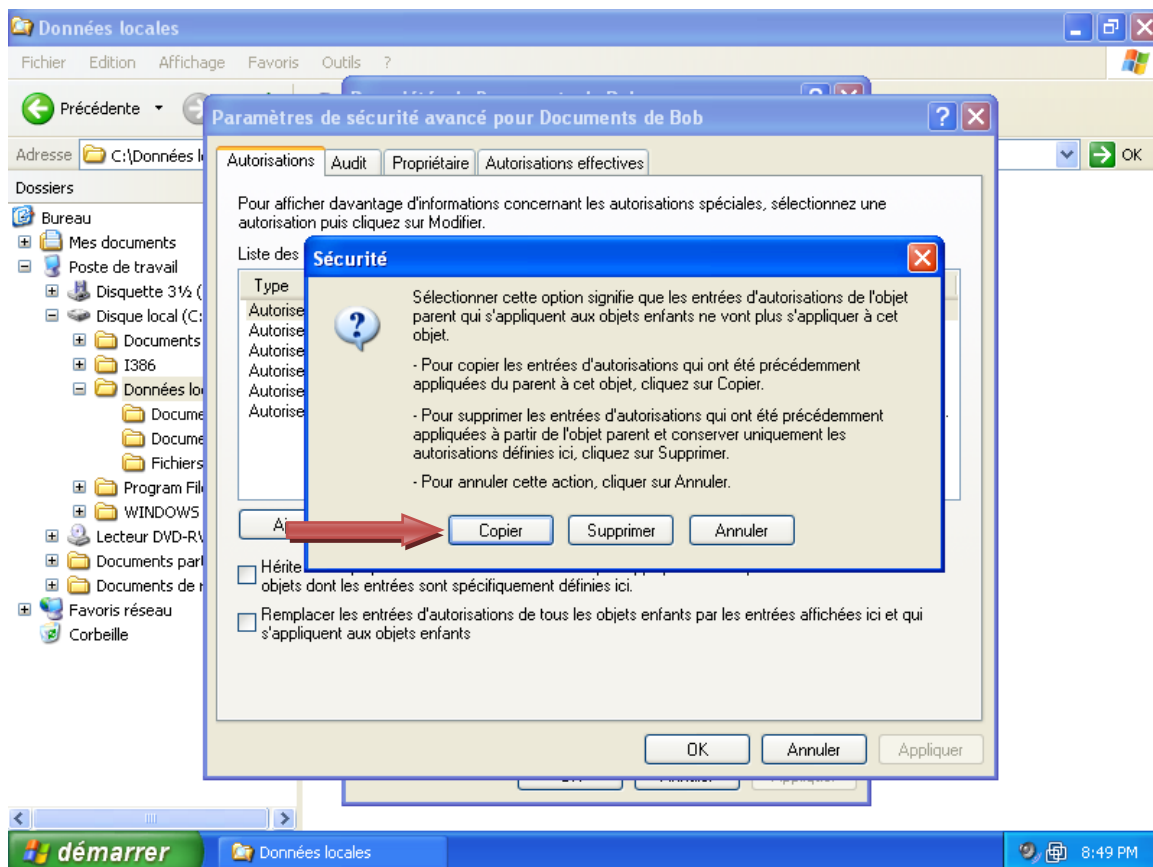
- h. Remarquez que les autorisations sont grisées et ne peuvent pas être modifiées. Cette restriction est imposée par les autorisations héritées d'un dossier parent. Pour sécuriser le dossier, vous devez désactiver les autorisations héritées. Dans l'onglet **Sécurité**, cliquez sur le bouton **Avancé**.



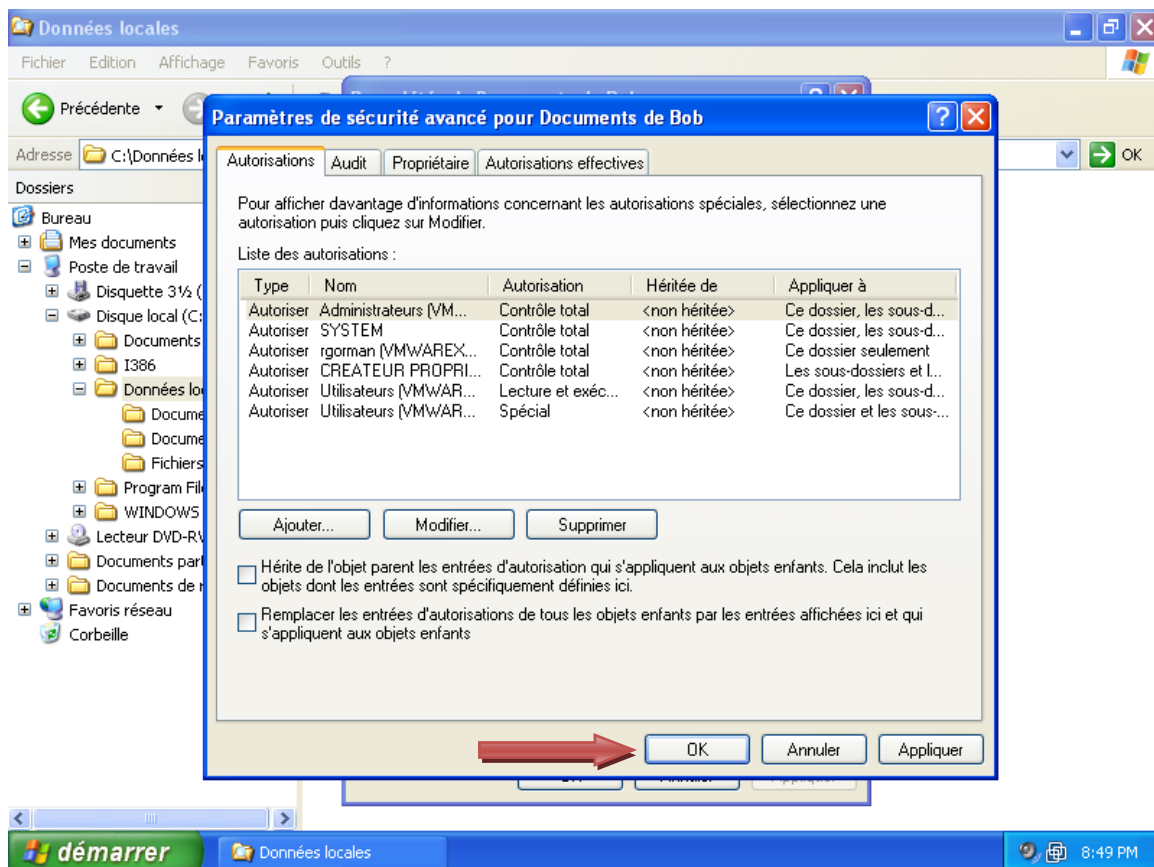
- i. Désactivez la case à cocher en regard de **Hérite de l'objet parent les entrées d'autorisation qui s'appliquent aux objets enfants**.



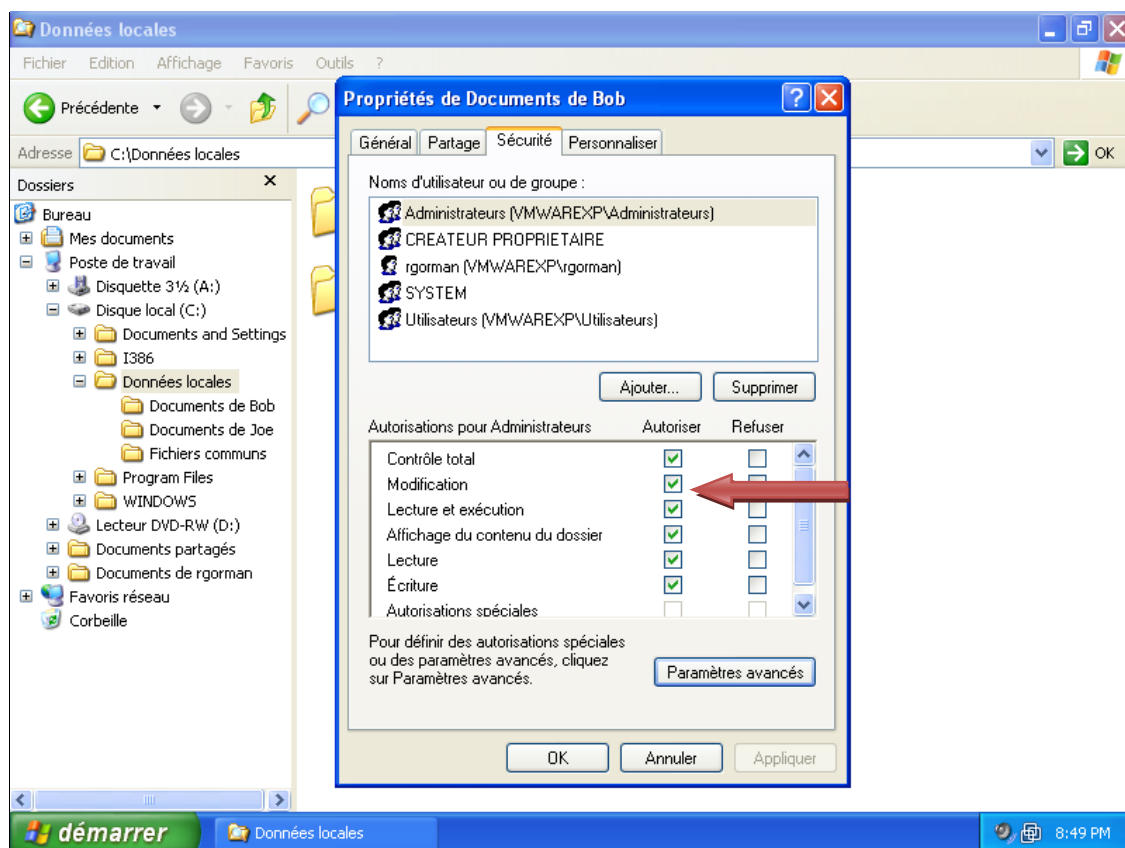
- j. Cliquez sur **Copier** pour conserver les autorisations existantes.



k. Cliquez sur **OK**.

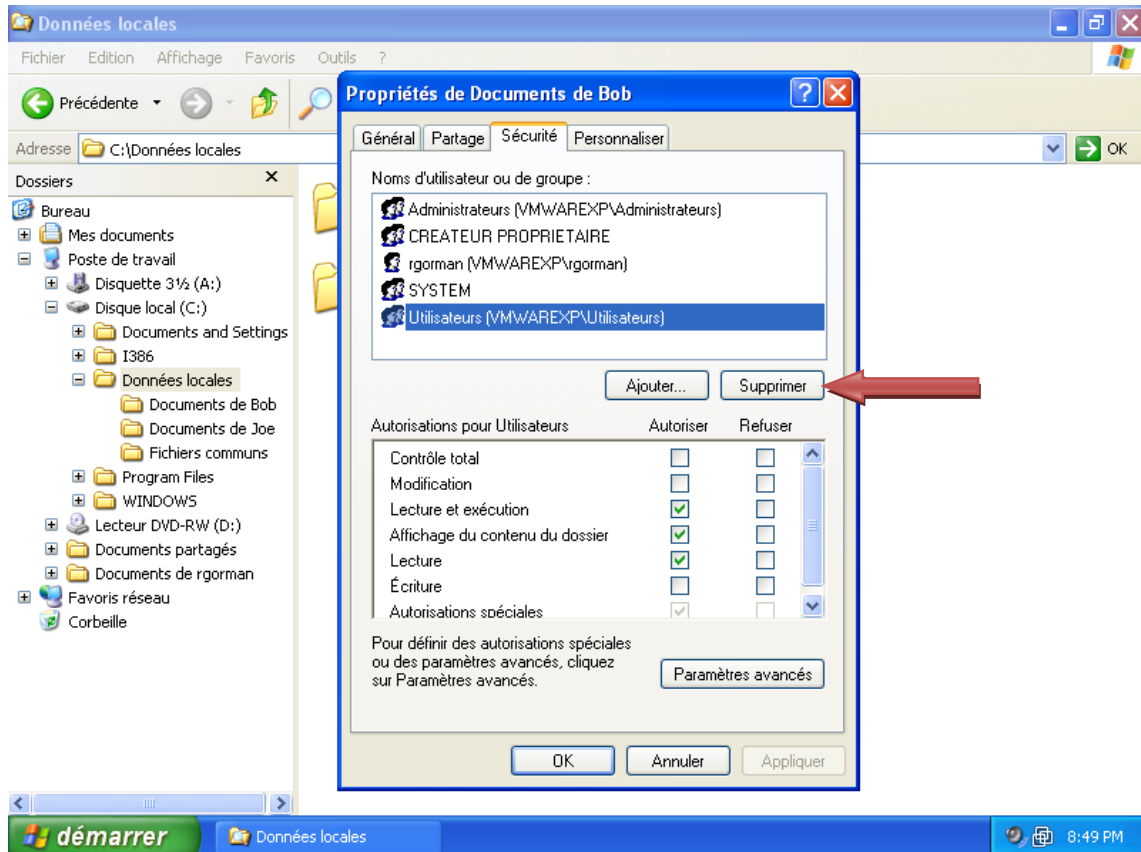


Une fois que la fonction d'héritage est désactivée, vous pouvez modifier les autorisations.

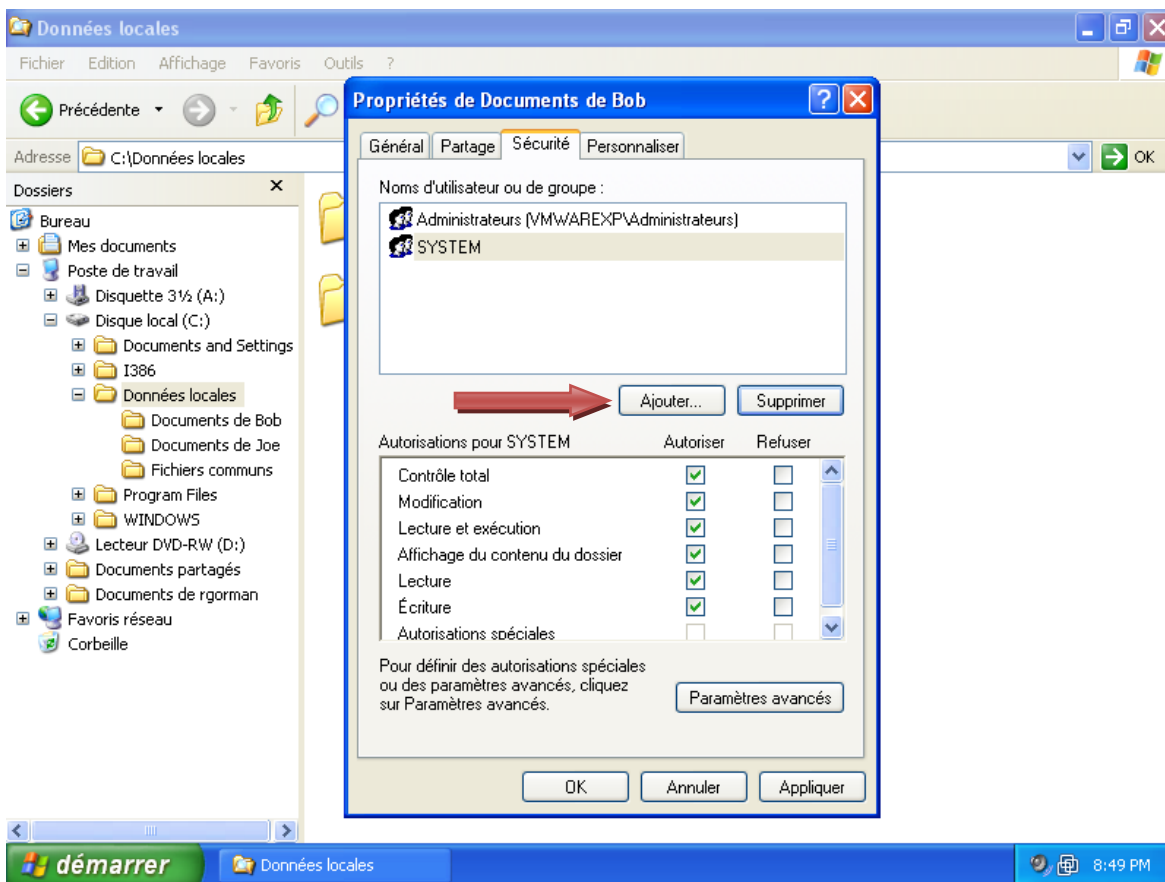


- I. Sélectionnez le groupe **Utilisateurs** et cliquez sur **Supprimer**. Poursuivez la sélection des autres utilisateurs et groupes restants, à l'exception des administrateurs et de SYSTEM, puis cliquez sur **Supprimer**.

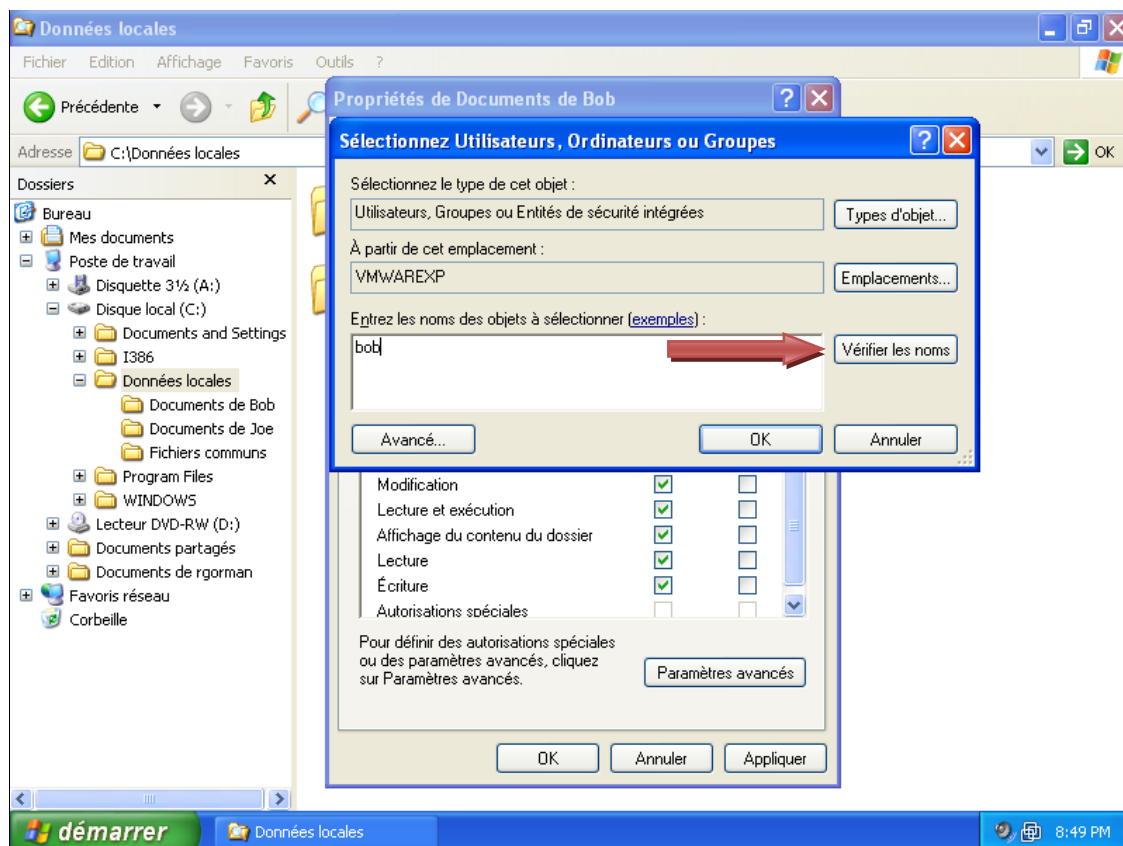
REMARQUE : accordez toujours aux groupes SYSTEM et Administrateurs l'accès avec contrôle total aux répertoires et fichiers afin d'assurer que les fichiers puissent être sauvegardés, restaurés et analysés correctement par le système informatique.



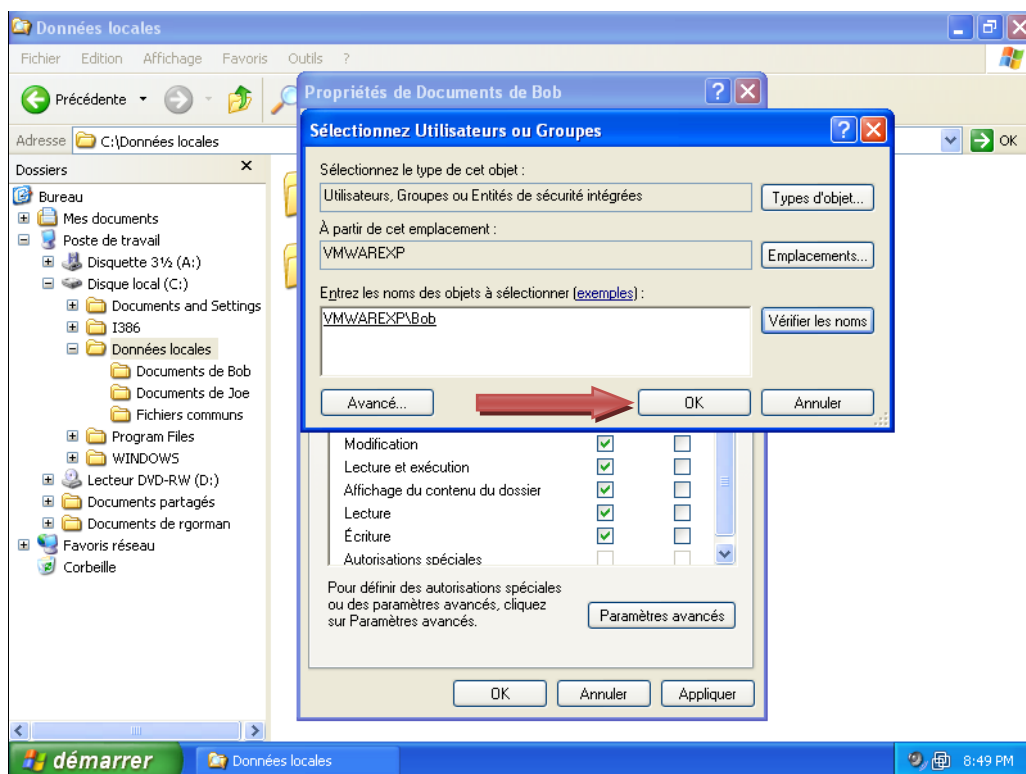
m. Ajoutez maintenant Bob à la liste. Cliquez sur **Ajouter**.



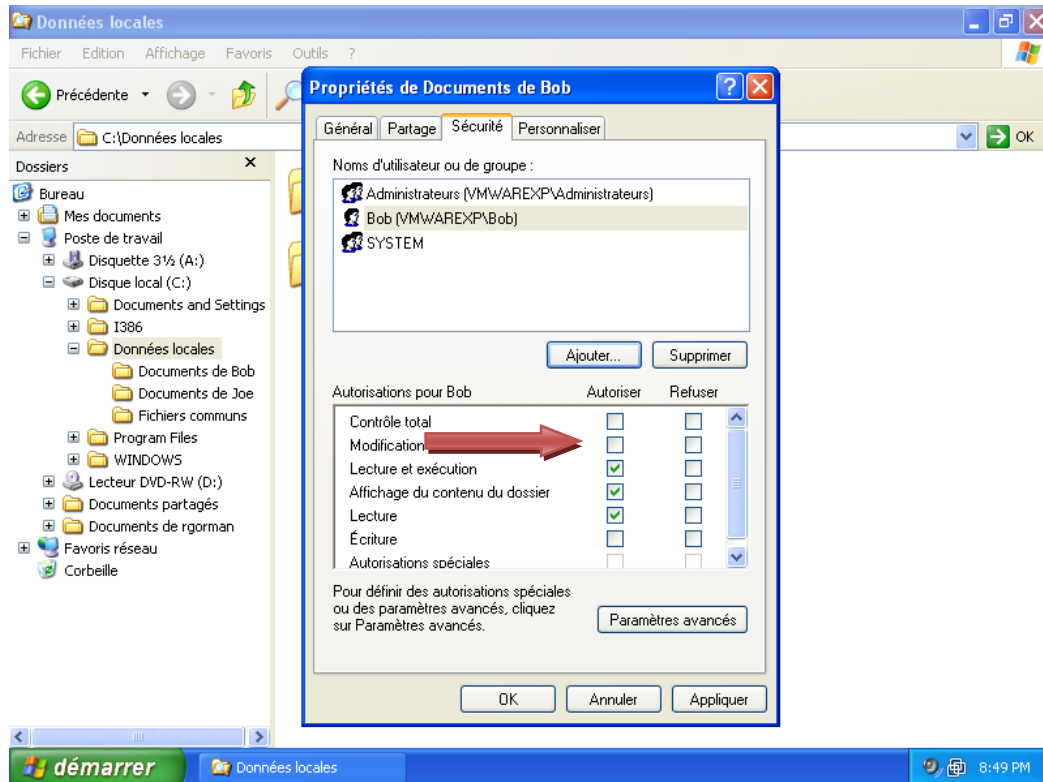
- n. Tapez **Bob** dans la zone de texte et cliquez sur le bouton **Vérifier les noms** pour contrôler son compte.



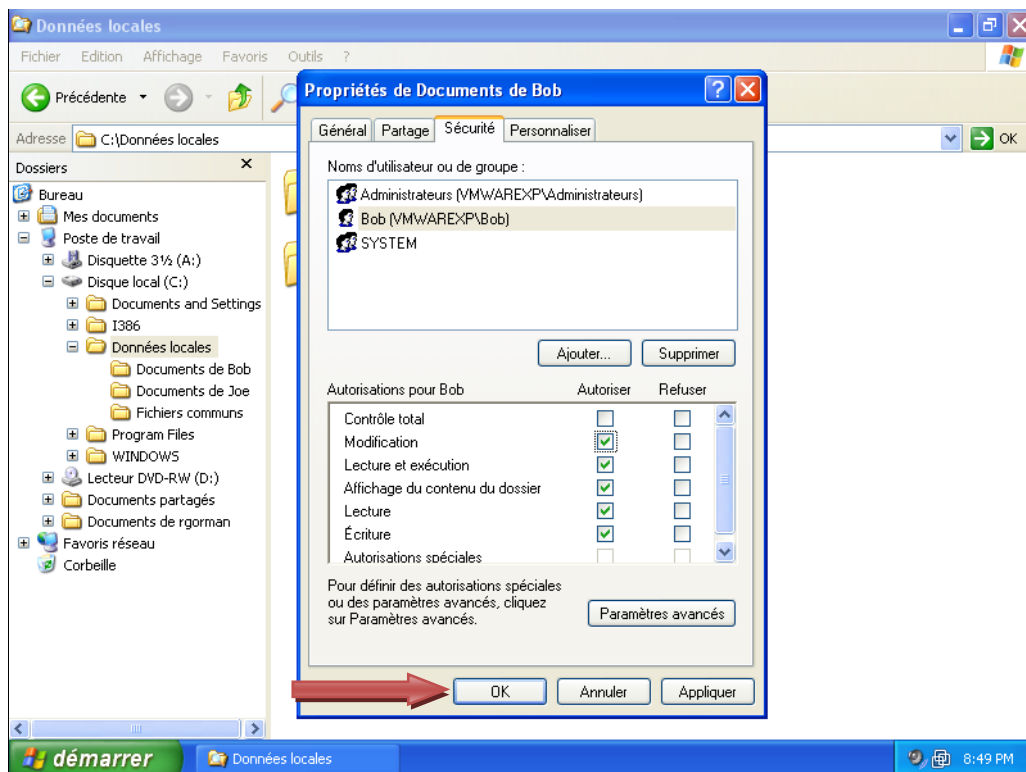
- o. Une fois que Bob a été contrôlé, cliquez sur **OK**.



- p. Bob est maintenant ajouté à la liste. Remarquez qu'il dispose actuellement des autorisations Lecture et exécution, Affichage du contenu du dossier et Lecture. Comme Bob a besoin d'écrire de nouveau fichiers et de supprimer des fichiers existants, accordez à Bob l'autorisation Modifier. Activez la case à cocher dans la colonne **Autoriser** en regard de **Modification**.

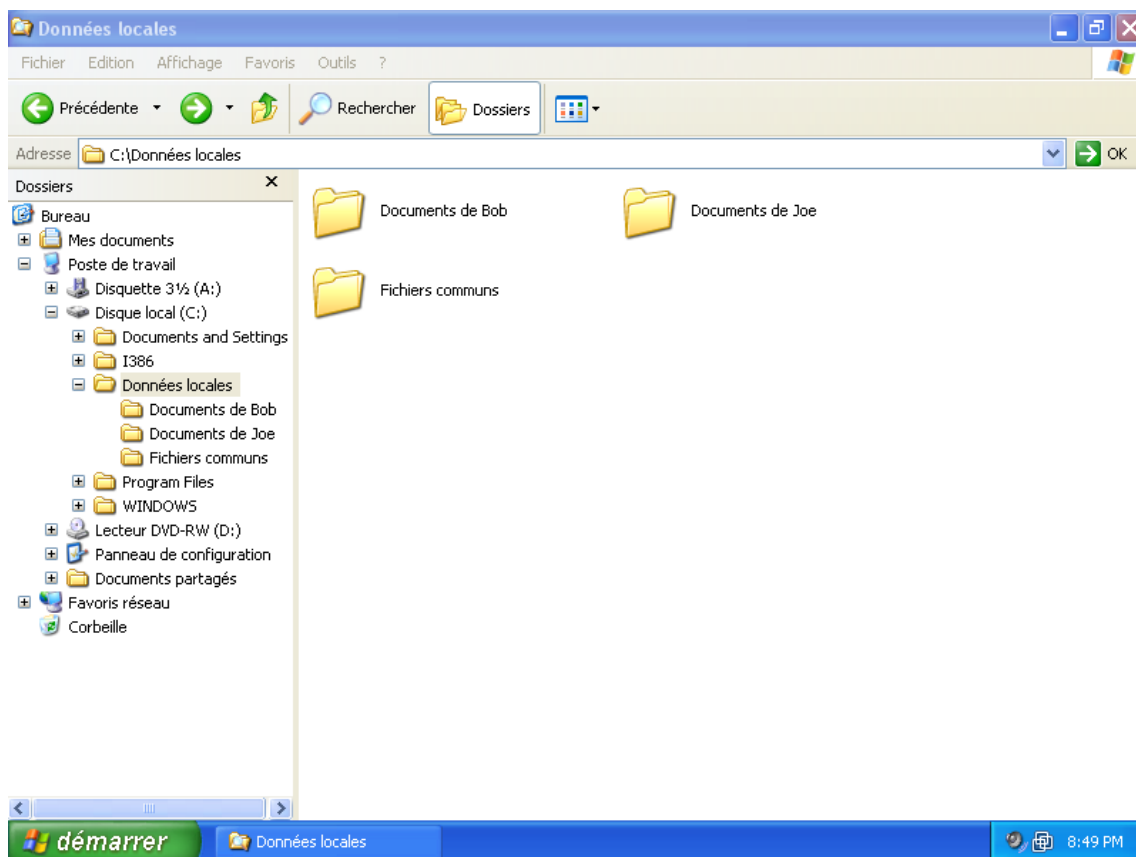


- q. Une fois que l'autorisation Modification a été accordée à Bob, cliquez sur **OK** pour définir la sécurité.

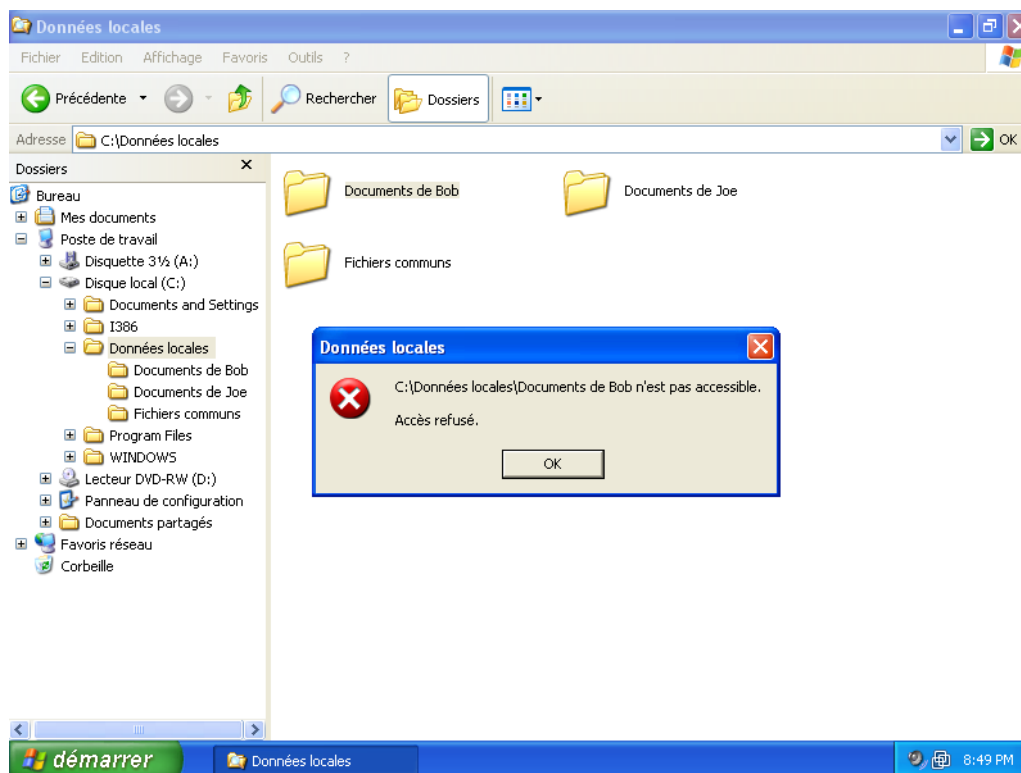


Étape 2 : test de l'accès de Joe au dossier Documents de Bob

- Ouvrez une session sur le PC local en tant que Joe et essayez d'accéder au répertoire **Documents de Bob**.



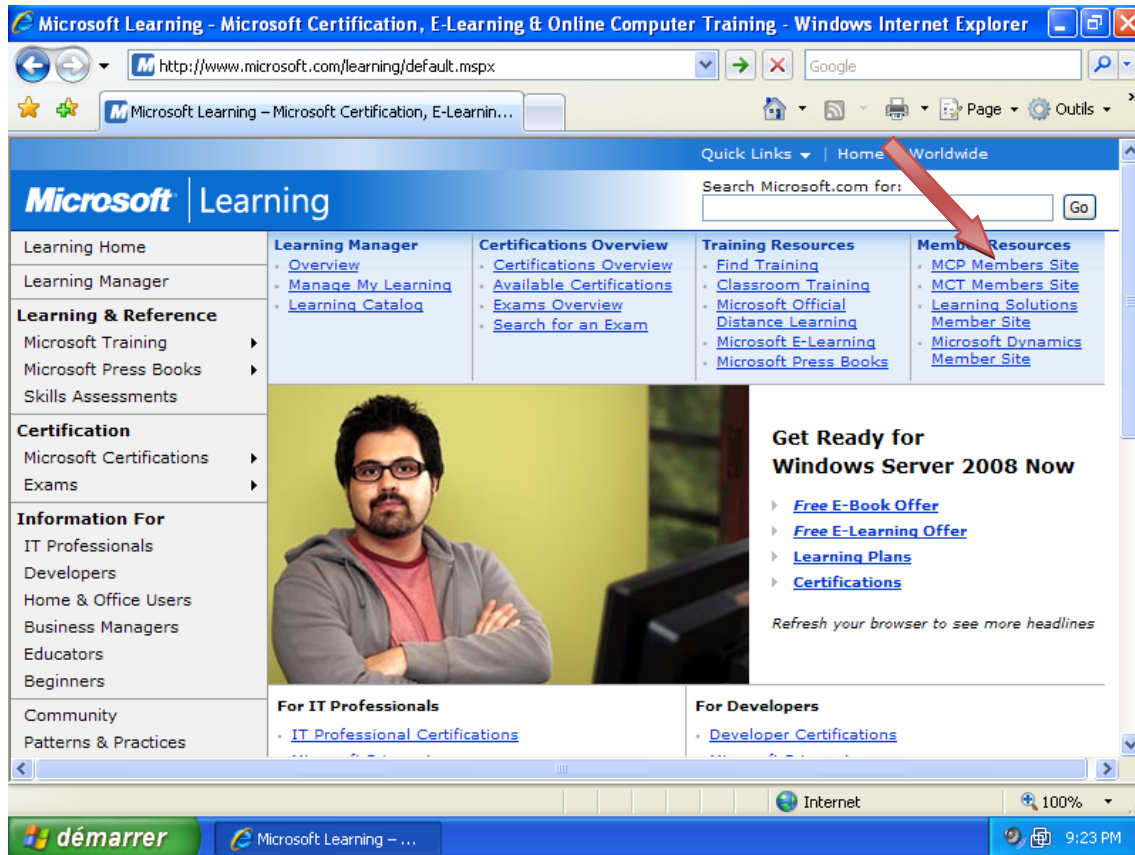
- b. Remarquez qu'une boîte de dialogue contextuelle s'affiche pour indiquer que Joe n'est pas autorisé à accéder à ces fichiers. Comme Joe ne possède pas les droits d'accès d'administrateur, il n'est pas autorisé à accéder au dossier **Documents de Bob**.



Partie 2 : identification d'un canal de communication sécurisé pour la transmission de données sur Internet

Étape 1 : identification d'une page Web sécurisée

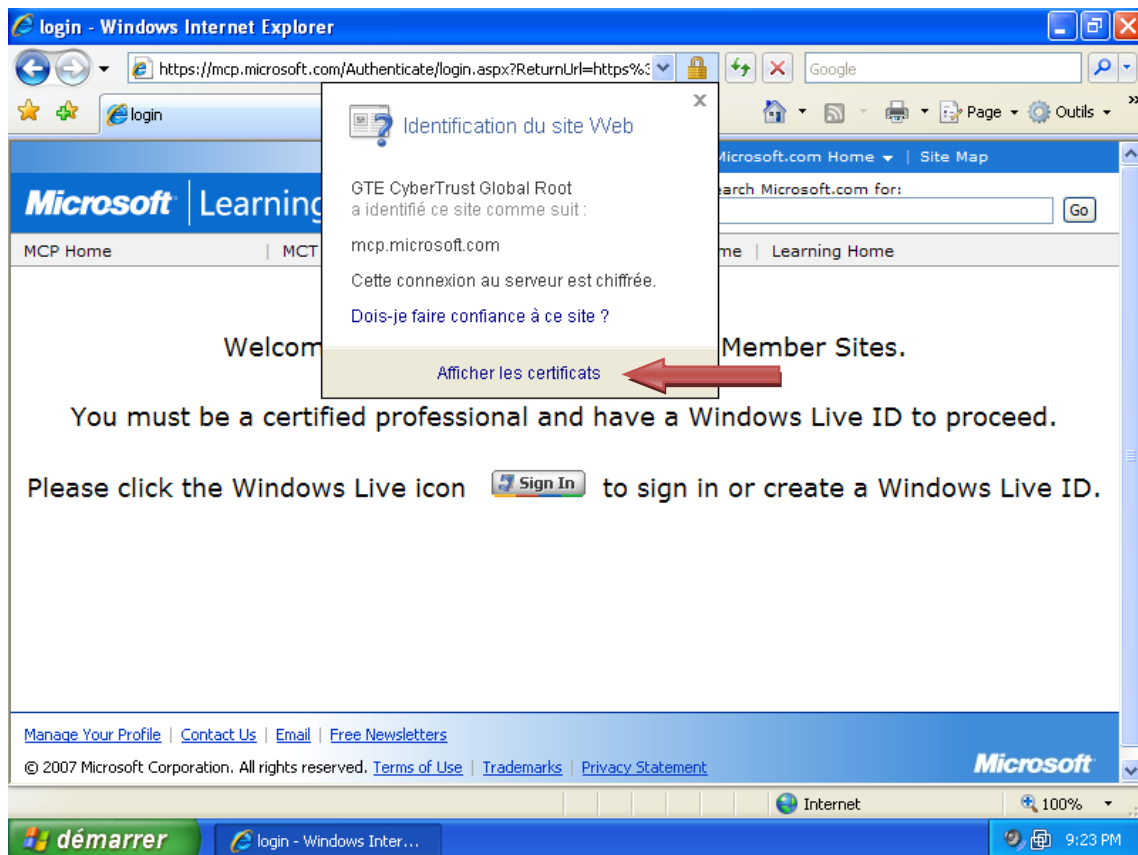
- Lancez Internet Explorer et accédez à <http://www.microsoft.com/learning>. Ce site constitue une page non sécurisée typique. Cliquez sur le lien **MCP Members Site**.



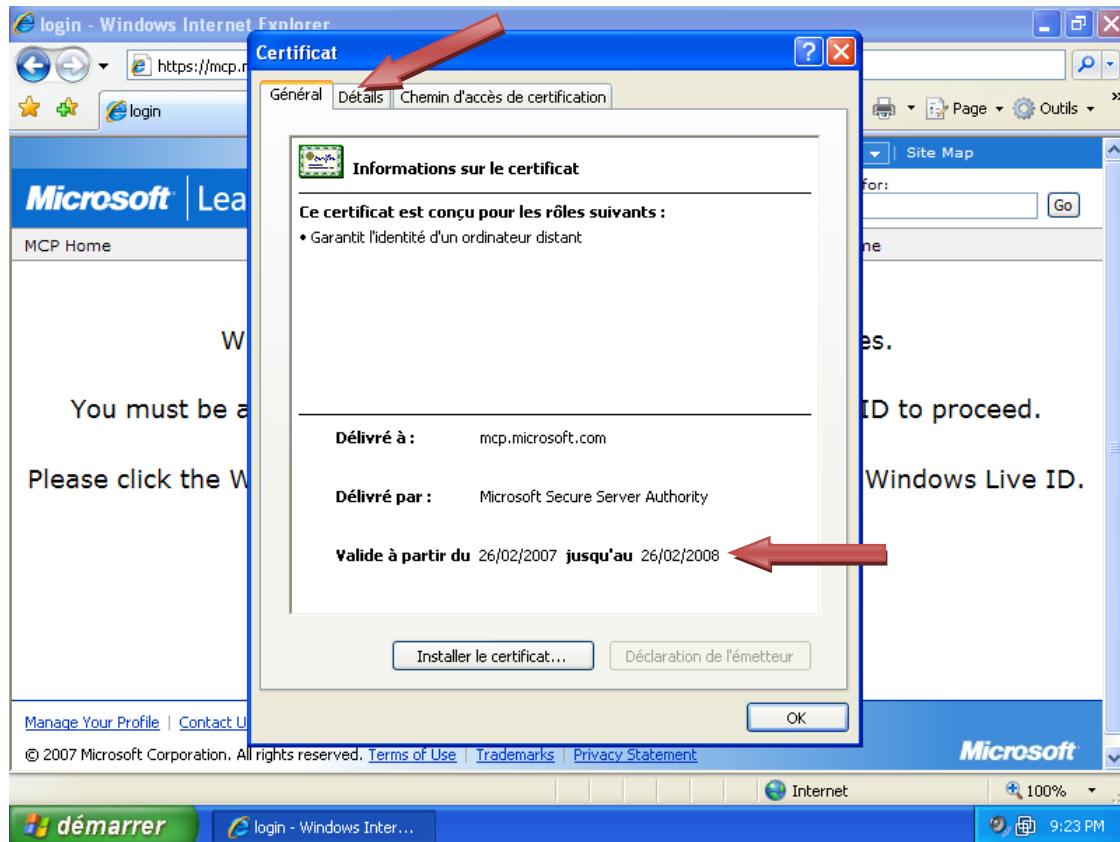
- b. Remarquez que l'adresse URL HTTP est remplacée par HTTPS. HTTPS est la version sécurisée de HTTP et utilise le protocole SSL pour sa sécurité. Remarquez également l'apparition d'une icône **verrou** à la droite de l'URL. La présence de cette icône indique que le site est sécurisé. Cliquez sur le **verrou** pour afficher plus de détails sur le site sécurisé.



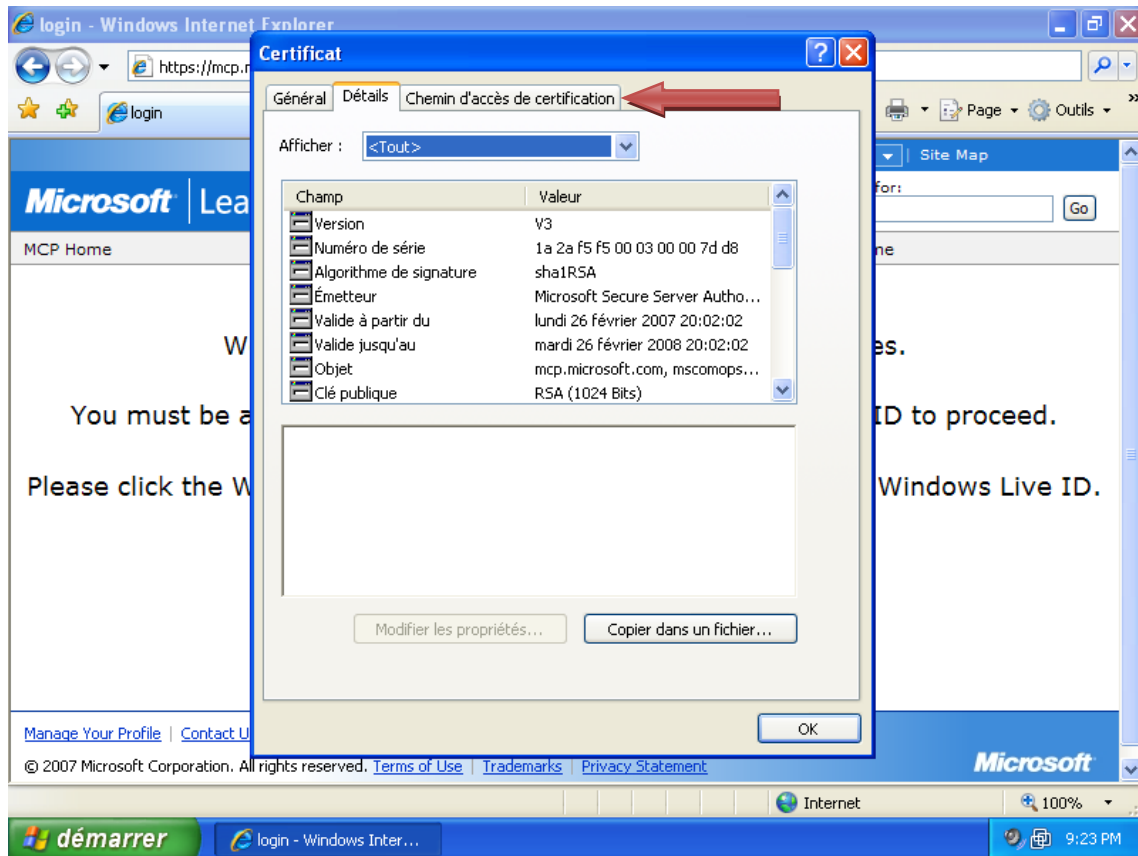
- c. La fenêtre contextuelle affiche des informations sur l'émetteur du certificat de sécurité pour ce site Web. Elle indique également que la connexion à ce serveur est sécurisée. Cliquez sur le lien **Afficher les certificats** situé au bas de la fenêtre contextuelle.



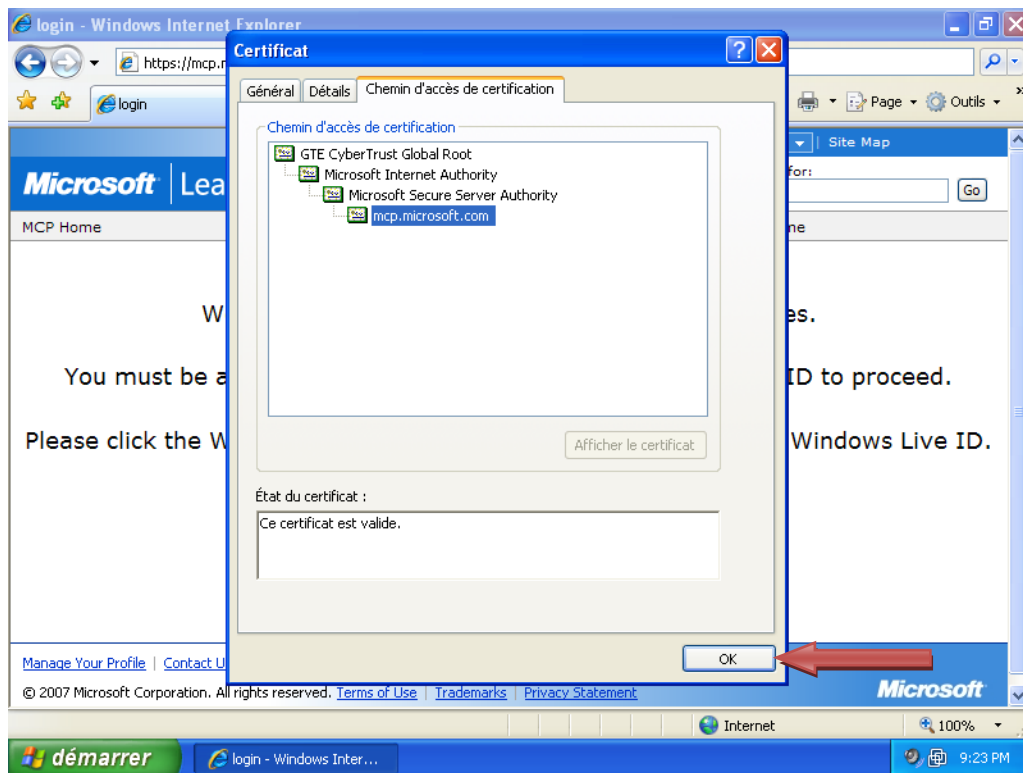
- d. La fenêtre de certificat s'ouvre et affiche le certificat installé sur le serveur Web pour lui permettre d'utiliser le protocole SSL. Remarquez la plage de dates **Valide à partir du** située au bas de la fenêtre. Les certificats ne sont valides que pour une période spécifique à l'issue de laquelle ils doivent être renouvelés. Le processus de renouvellement assure que les administrateurs de serveurs Web valident constamment leurs serveurs auprès de l'autorité de certification qui a émis le certificat. Cliquez sur l'onglet **Détails** pour plus d'informations.



- e. L'onglet **Détails** affiche des informations sur le certificat. Cliquez sur l'onglet **Chemin d'accès de certification**.

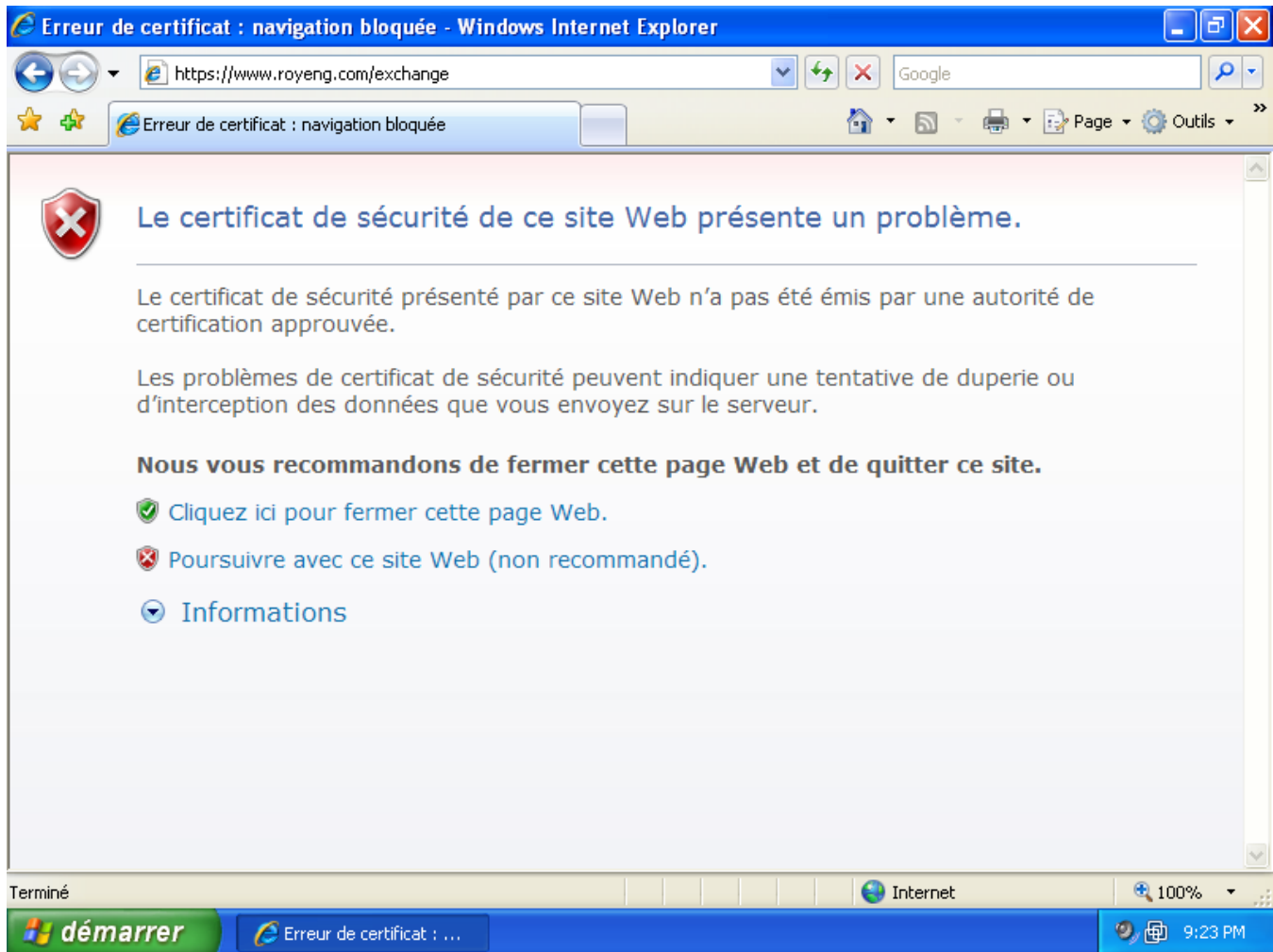


- f. L'onglet **Chemin d'accès de certification** affiche la liste hiérarchique des autorités de certification qui sont autorisées à émettre le certificat de serveur Web. Cliquez sur **OK** pour fermer la fenêtre du certificat.



Étape 2 : examen de l'avertissement d'accès sécurisé à une source non fiable

- a. Si le certificat de sécurité présenté par un site Web ne provient pas d'une autorité fiable, Internet Explorer affiche l'écran ci-dessous pour vous avertir du problème. Vous avez alors le choix de fermer la page Web ou de poursuivre votre visite du site Web.



- b. À moins d'être sûr que le site Web est légitime, vous ne pouvez peut-être pas vous fier au serveur ni au contenu qu'il fournit. Si vous naviguez sur le chemin d'accès de certification, comme décrit précédemment, aucune liste d'autorités de certification fiables ne s'affiche. Vous travaillez peut-être sur un site Web sécurisé (HTTPS), mais celui-ci est peut-être auto-certifié et non pas certifié par une autorité agréée.