Exigences en matière de certificat lorsque vous utilisez EAP-TLS ou PEAP avec EAP-TLS

IMPORTANT : Cet article est issu du système de traduction automatique mis au point par Microsoft (http://support.microsoft.com/gp/mtdetails). Un certain nombre d'articles obtenus par traduction automatique sont en effet mis à votre disposition en complément des articles traduits en langue française par des traducteurs professionnels. Cela vous permet d'avoir accès, dans votre propre langue, à l'ensemble des articles de la base de connaissances rédigés originellement en langue anglaise. Les articles traduits automatiquement ne sont pas toujours parfaits et peuvent comporter des erreurs de vocabulaire, de syntaxe ou de grammaire (probablement semblables aux erreurs que ferait une personne étrangère s'exprimant dans votre langue !). Néanmoins, mis à part ces imperfections, ces articles devraient suffire à vous orienter et à vous aider à résoudre votre problème. Microsoft s'efforce aussi continuellement de faire évoluer son système de traduction automatique.

Consulter l'article original en anglais : 814394

INTRODUCTION

Cet article décrit la configuration requise que les certificats de vos clients et vos certificats de serveur lorsque vous utilisez Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)

Propriétés

ID d'article : 814394 - Dernière mise à jour : 31 mars 2017 - Révision : 3

ou protégé par l'authentification PEAP (Extensible Protocol) avec EAP-TLS.

Plus d'informations

Lorsque vous utilisez EAP avec un type EAP fort, tels que TLS avec les cartes à puce ou TLS avec des certificats, le client et le serveur utilisent des certificats pour vérifier leur identité à l'autre. Les certificats doivent répondre aux exigences spécifiques sur le serveur et sur le client pour l'authentification.

Une condition requise est que le certificat doit être configuré avec un ou plusieurs rôles dans les extensions Utilisation de clé étendue (EKU) qui correspondent à l'utilisation du certificat. Par exemple, un certificat qui est utilisé pour l'authentification d'un client à un serveur doit être configuré avec le rôle Authentification du Client. Ou bien, un certificat qui est utilisé pour l'authentification d'un serveur doit être configuré avec le rôle Authentification du serveur. Lorsque les certificats sont utilisés pour l'authentification, l'authentificateur examine le certificat client et recherche de l'identificateur d'objet rôle correct dans les extensions EKU. Par exemple, l'identificateur d'objet pour le rôle Authentification du Client est 1.3.6.1.5.5.7.3.2.

Exigences minimales de certificat

Tous les certificats qui sont utilisés pour l'authentification de l'accès réseau doivent satisfaire la configuration requise pour les certificats X.509 et ils remplissent également les conditions requises pour les connexions qui utilisent le cryptage Secure Sockets Layer (SSL) et le cryptage de sécurité TLS (Transport Level Security). Une fois ces conditions minimales sont remplies, à la fois les certificats client et les certificats de serveur doivent répondre aux exigences supplémentaires suivantes.

Configuration requise du certificat client

Avec EAP-TLS ou PEAP avec EAP-TLS, le serveur accepte l'authentification du client si le certificat remplit les conditions suivantes :

- Le certificat client est émis par une autorité de certification d'entreprise (CA), ou il est mappé à un compte d'utilisateur ou à un compte d'ordinateur dans le service d'annuaire Active Directory.
- L'utilisateur ou le certificat d'ordinateur sur les chaînes de client à une autorité de certification racine de confiance.

- L'utilisateur ou le certificat d'ordinateur sur le client inclut le rôle Authentification du Client.
- L'utilisateur ou le certificat d'ordinateur n'échoue pas l'une des vérifications effectuées par le magasin de certificats CryptoAPI et le certificat transmet les besoins de la stratégie d'accès distant.
- L'utilisateur ou le certificat d'ordinateur n'échoue pas l'un des contrôles d'identificateur d'objet certificat qui sont spécifiées dans la stratégie d'accès distant Service d'authentification Internet (IAS).
- Le client 802. 1**x** n'utilise pas les certificats basés sur le Registre qui sont des certificats de carte à puce ou des certificats qui sont protégées par un mot de passe.
- L'extension (SubjectAltName) autre nom du sujet dans le certificat contient le nom utilisateur principal (UPN) de l'utilisateur.
- Lorsque les clients utilisent le protocole EAP-TLS ou PEAP avec l'authentification EAP-TLS, une liste de tous les certificats installés s'affiche dans le composant logiciel enfichable Certificats, avec les exceptions suivantes :
  - Les clients sans fil n'affichent pas les certificats basés sur le Registre et les certificats d'ouverture de session de carte à puce.
  - Clients sans fil et les clients de réseau privé virtuel (VPN) n'affichent pas les certificats qui sont protégées par un mot de passe.
  - Les certificats qui ne contiennent pas le rôle Authentification du Client dans leurs extensions EKU ne s'affichent pas.

Configuration requise du certificat serveur

Vous pouvez configurer les clients pour valider les certificats de serveur à l'aide de l'option **Valider le certificat du serveur** dans l'onglet **authentification** dans les propriétés de connexion réseau. Lorsqu'un client utilise l'authentification PEAP-EAP-MS-CHAP Challenge Handshake Authentication Protocol () version 2, PEAP avec l'authentification EAP-TLS ou l'authentification EAP-TLS, le client accepte le certificat du serveur lorsque le certificat remplit les conditions suivantes :

- Le certificat d'ordinateur sur le serveur provient d'une des opérations suivantes :
  - Une Microsoft AC racine de confiance.
  - Une racine autonome de Microsoft ou tierce autorité de certification dans un domaine Active Directory qui possède une Boutique NTAuthCertificates qui contient le certificat publié. Pour plus d'informations sur l'importation de certificats d'autorité de certification tiers, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft :

    295663 comment importer des certificats d'autorité de certification tierce dans le magasin NTAuth de Microsoft Enterprise
- Le service IAS ou le certificat d'ordinateur serveur VPN est configuré avec le rôle Authentification du serveur. L'identificateur d'objet pour l'authentification du serveur est 1.3.6.1.5.5.7.3.1.
- Le certificat d'ordinateur n'échoue pas l'une des vérifications effectuées par le magasin de

certificats CryptoAPI, et elle n'échouera pas l'une des exigences de la stratégie d'accès distant.

- Le nom de la ligne d'objet du certificat du serveur correspond au nom configuré sur le client pour la connexion.
- Pour les clients sans fil, l'extension (SubjectAltName) autre nom du sujet contient le nom de domaine complet du serveur (FQDN).
- Si le client est configuré pour faire confiance à un certificat de serveur avec un nom spécifique, l'utilisateur est invité à prendre une décision sur l'approbation d'un certificat avec un nom différent. Si l'utilisateur rejette le certificat, l'authentification échoue. Si l'utilisateur accepte le certificat, le certificat est ajouté pour le magasin de certificats racine de confiance.

Remarque Avec PEAP ou avec l'authentification EAP-TLS, les serveurs affichent une liste de tous les certificats installés dans le composant logiciel enfichable Certificats. Toutefois, les certificats qui contiennent le rôle Authentification du serveur dans les extensions EKU ne sont affichent pas.

Références

Pour plus d'informations sur les technologies de réseau sans fil, visitez le site Web de Microsoft à l'adresse suivante :

http://www.microsoft.com/whdc/connect/wireless/default.mspx

Pour plus d'informations, cliquez sur le numéro ci-dessous pour afficher l'article correspondant dans la Base de connaissances Microsoft :

313242 comment faire pour résoudre les problèmes de connexion réseau sans fil dans Windows XP