Expiration de certificat et inscription automatique pour la réinscription automatique auprès de l'autorité de certification Cisco IOS

Contenu

Introduction

Tous les certificats numériques ont une durée d'expiration intégrée dans le certificat qui est attribuée par le serveur de l'autorité de certification (AC) émettrice lors de l'inscription. Lorsqu'un certificat numérique est utilisé pour l'authentification VPN IPSec d'ISAKMP, il y a une vérification automatique du délai d'expiration du certificat du périphérique communiquant et de l'heure système sur le périphérique (point d'extrémité VPN). Cela garantit qu'un certificat utilisé est valide et n'a pas expiré. C'est également la raison pour laquelle vous *devez* configurer l'horloge interne sur chaque point d'extrémité VPN (routeur). Si le protocole NTP (Network Time Protocol) (ou SNTP [Simple Network Time Protocol]) n'est pas possible sur les routeurs de chiffrement VPN, utilisez la commande **set clock** manuelle.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur tous les routeurs qui exécutent l'image cXXXX-advsecurityk9-mz.123-5.9.T pour cette plate-forme respective .

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Quand un certificat numérique est-il considéré comme expiré ou non ?

- Un certificat a expiré (non valide) si l'heure système est postérieure à l'heure d'expiration du certificat ou antérieure à l'heure émise du certificat.
- Un certificat n'a pas expiré (valide) si l'heure système est comprise entre l'heure de délivrance du certificat et celle du certificat.

L'objectif de la fonctionnalité d'inscription automatique est de fournir à l'administrateur de l'autorité de certification un mécanisme permettant à un routeur actuellement inscrit de s'inscrire automatiquement à nouveau avec son serveur d'autorité de certification sur un pourcentage configuré de la durée de vie du certificat de routeur. Il s'agit d'une caractéristique importante pour la facilité de gestion et la prise en charge des certificats en tant que mécanisme de contrôle. Si vous avez utilisé une autorité de certification particulière pour émettre des certificats à des milliers de routeurs VPN de filiale potentiels avec une durée de vie d'un an (sans inscription automatique), alors dans exactement un an du temps délivré, tous les certificats expirent et toutes les filiales perdent la connectivité via IPSec. Sinon, si la fonction d'inscription automatique est définie sur « 70 inscriptions automatiques », comme dans cet exemple, dans 70 % de la durée de vie du certificat émis (1 an), chaque routeur émet automatiquement une nouvelle demande d'inscription au serveur CA Cisco IOS® répertorié dans le point de confiance.

Remarque : Une exception à la fonction d'inscription automatique est que si elle est définie sur *inférieur ou égal à 10*, elle est en minutes. S'il est *supérieur à 10*, il s'agit d'un pourcentage de la durée de vie du certificat.

L'administrateur de l'autorité de certification Cisco IOS doit tenir compte de certaines mises en garde lors de l'inscription automatique. L'administrateur doit exécuter ces actions pour que la réinscription réussisse :

1. Accorder ou rejeter manuellement chaque demande de réinscription sur le serveur AC Cisco IOS (sauf si « grant auto » est utilisé sur le serveur AC Cisco IOS).Le serveur d'autorité de certification Cisco IOS doit toujours accorder ou rejeter chacune de ces demandes (en supposant que l'autorité de certification Cisco IOS ne dispose pas de l'option grant auto activée). Cependant, aucune action administrative n'est requise sur le routeur d'inscription pour démarrer le processus de réinscription.
2. Enregistrez le nouveau certificat réinscrit dans le routeur VPN réinscrit, le cas échéant.Si aucune modification de configuration non enregistrée n'est en attente dans le routeur, le nouveau certificat est automatiquement enregistré dans la mémoire vive non volatile (NVRAM). Le nouveau certificat est écrit dans la mémoire NVRAM et le certificat précédent est supprimé.Si des modifications de configuration non enregistrées sont en attente, vous devez émettre la commande **copy run start** sur le routeur d'inscription afin d'enregistrer les modifications de configuration et le nouveau certificat réinscrit dans la mémoire vive non volatile. Une fois la commande **copy run start** terminée, le nouveau certificat est écrit dans la mémoire NVRAM et le certificat précédent est supprimé.**Remarque :** Lorsqu'une nouvelle réinscription réussit, cela *ne* permet *pas* de révoquer le certificat précédent pour ce périphérique inscrit sur le serveur AC. Lorsque des périphériques VPN communiquent, ils s'envoient mutuellement le numéro de série du certificat (un numéro unique).**Remarque :** Par exemple, si vous êtes à 70 % de la durée de vie du certificat et qu'une succursale VPN

devait s'inscrire de nouveau auprès de l'AC, celle-ci a deux certificats pour ce nom d'hôte. Cependant, le routeur d'inscription en possède un seul (le plus récent). Si vous le choisissez, vous pouvez révoquer administrativement l'ancien certificat ou le laisser expirer normalement.**Remarque :** Les nouvelles versions de code de la fonction d'inscription automatique ont la possibilité de « régénérer » les paires de clés utilisées pour l'inscription.Cette option n'est pas définie par défaut pour régénérer les paires de clés.Si cette option a été sélectionnée, soyez conscient du bogue Cisco ayant l'ID CSCea90136. Ce correctif de bogue permet de placer la nouvelle paire de clés dans des fichiers temporaires pendant que la nouvelle inscription de certificat a lieu sur un tunnel IPSec existant (qui utilise l'ancienne paire de clés).L'inscription automatique permet de générer de nouvelles clés au moment du renouvellement de la certification. À l'heure actuelle, cela entraîne une perte de service pendant le temps nécessaire à l'obtention d'un nouveau certificat. En effet, il existe une nouvelle clé, mais aucun certificat ne la correspond.Cette fonctionnalité conserve l'ancienne clé et le certificat jusqu'à ce que le nouveau certificat soit disponible.La génération automatique de clés est également implémentée pour l'inscription manuelle. Les clés sont générées (selon les besoins) pour l'inscription automatique ou manuelle.Version trouvée - 12.3PIH03Version à corriger dans - 12.3TVersion appliquée à - 12.3PI03Intégré dans - AucunPour plus d'informations, contactez le support technique Cisco.

Informations connexes

- Page d'assistance IPsec
- Support technique - Cisco Systems