Contenu

Introduction

Ce document décrit les raisons pour lesquelles la caractéristique de connexion automatique sur la suite logicielle de gestion Cisco TelePresence (TMS) pourrait pour fonctionner.

La connexion automatique ne fonctionne pas

Parfois vous rencontrez un problème où la connexion automatique ne fonctionne pas à Cisco TMS, et vous êtes incité pour votre nom d'utilisateur et mot de passe. L'ouverture de session simple avec l'authentification intégrée exige le navigateur Web, l'URL, et la compatibilité de réseau.

> Remarque: Assurez que le nom d'utilisateur et mot de passe utilisé pour ouvrir une session à Microsoft Windows est utilisé pour ouvrir une session à Cisco TMS.

Navigateurs compatibles

La connexion automatique est prise en charge en Internet Explorer (IE) sur Microsoft Windows, mais pourrait être due désactivé aux **paramètres de sécurité et aux zones** dans les **options Internet du** navigateur. Ceci peut être modifié si vous ou ajoutez le serveur de Cisco TMS à une zone de Sécurité de confiance dans l'IE, ou si vous changez les configurations d'authentification de l'utilisateur dans les paramètres de sécurité de la zone.

Mozilla Firefox ne prend en charge pas l'ouverture de session simple par défaut, mais il peut être configuré pour faire ainsi :

1. Dans le champ URL, type **environ : config**.
2. Dans le **champ de filtre**, **ntlm de** type.
3. Double clic ou clic droit **network.automatic-ntlm-auth.trusted-uris afin de** modifier la configuration.
4. Saisissez le domaine de Cisco TMS. Si vous devez ajouter plus de domaines, ne les séparez avec des virgules sans aucun espace.
5. Cliquez sur **OK**. La modification est appliquée immédiatement.

URL compatible

La connexion automatique exige l'utilisation d'un URL qui trace au nom de domaine complet interne correct (FQDN) pour l'ordinateur, pas simplement l'adresse IP correcte du serveur.

Par exemple, si l'ordinateur est nommé **CORPTMS2.example.int** et son adresse IP est **43.33.23.2**, puis connexion automatique :

- est possible si un utilisateur entre dans **http://CORPTMS2.example.int/tms**
- n'est pas possible si l'utilisateur entre dans **http://43.33.23.2/tms**

L'utilisation d'un nom de Système de noms de domaine (DNS) qui trace à l'adresse IP, mais pas le FQDN interne, ne permet pas la connexion automatique.

Par exemple, si vous avez l'enregistrement des DN A traçant **tms.example.com à 43.33.23.2**, puis les utilisateurs qui entrent dans **http://tms.example.com/tms** ne pourront pas ouvrir une session automatiquement. C'est parce que les configurations d'adresse directement à l'adresse IP au lieu de au nom de la machine FQDN de Répertoire actif.

Réseau compatible

Les réseaux qui incluent des proxys de Web des méthodes d'authentification du LAN Manager cassent souvent de Kerberos ou de Windows NT (NTLM), qui rend l'authentification intégrée inutilisable, parce que l'authentification intégrée a été conçue pour les réseaux internes qui n'exigent pas des proxys de Web d'être traversés. Dans ces situations, le navigateur Web et le web server négocient la prochaine méthode d'authentification disponible.