Configuration de l'authentification du serveur Secure Shell (SSH) pour les clients SSH sur les commutateurs empilables de la gamme Sx500

Objectif

La fonctionnalité de serveur Secure Shell (SSH) permet à l'utilisateur d'établir une session SSH avec les commutateurs empilables de la gamme Sx500. Une session SSH est comme une session telnet, mais une session SSH est plus sécurisée. La sécurité est obtenue par le périphérique lorsqu'il génère automatiquement les clés publiques et privées. Ces clés peuvent également être modifiées par l'utilisateur. Une session SSH peut être ouverte à l'aide de l'application PuTTY.

Cet article fournit des informations sur la façon d'activer l'authentification du serveur SSH pour les clients SSH et de définir les serveurs de confiance sur les commutateurs empilables de la gamme Sx500.

Périphériques pertinents

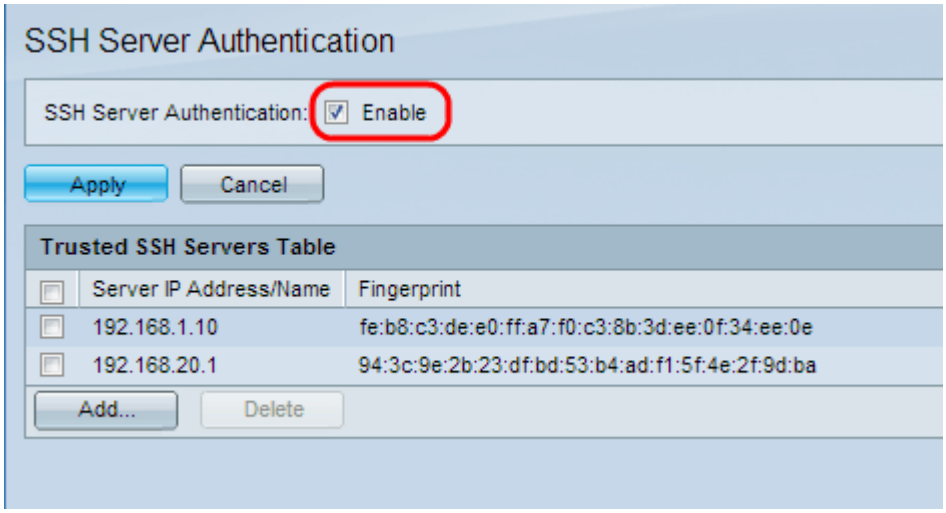
Commutateurs Empilables · Sx500

Version du logiciel

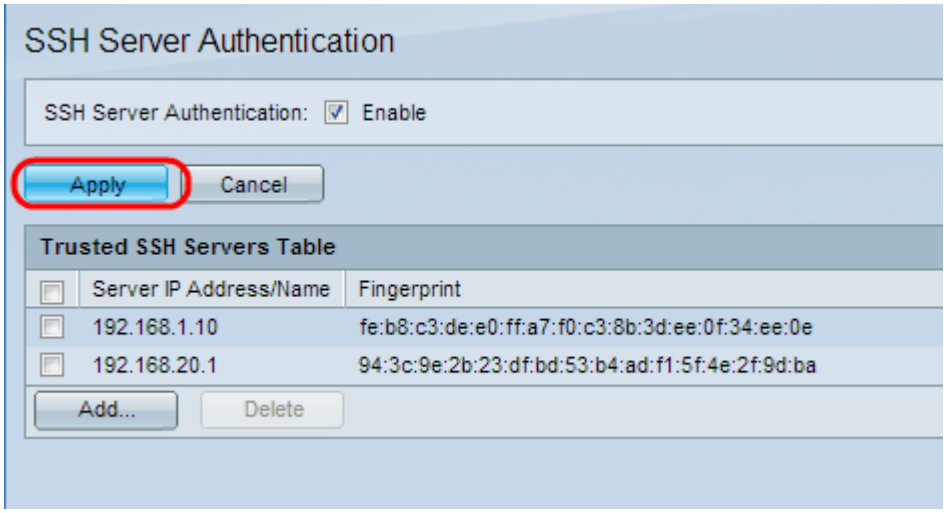
•v 1.2.7.76

Configuration de l'authentification du serveur SSH

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Security > SSH Client > SSH Server Authentication**. La page *SSH Server Authentication* s'ouvre :

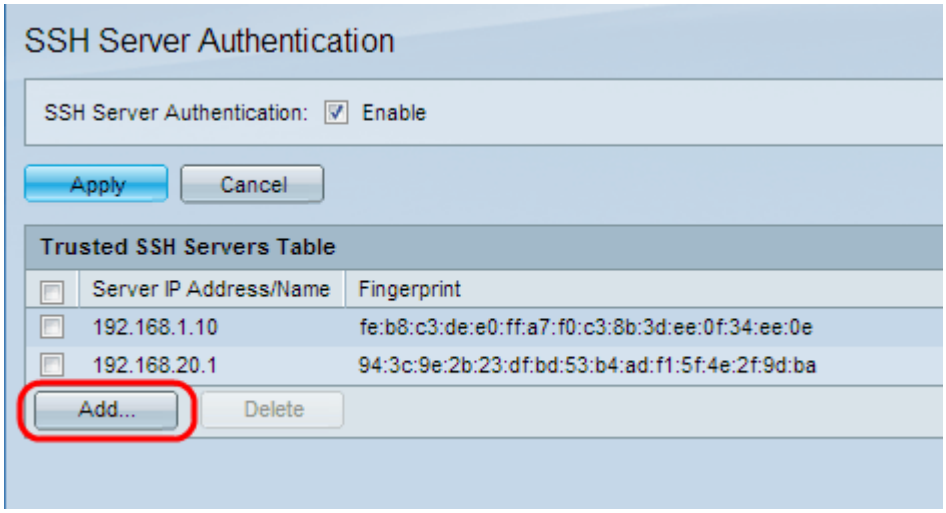


Étape 2. Cochez **Enable** pour activer l'authentification du serveur SSH.



Étape 3. Cliquez sur **Apply** pour enregistrer la configuration.

Ajouter un serveur SSH approuvé



Étape 1. Dans le tableau Serveurs SSH approuvés, vous trouverez l'adresse IP et l'empreinte digitale du serveur SSH. Cliquez sur **Ajouter** pour ajouter le serveur ssh approuvé. La fenêtre *Add Trusted SSH Server* apparaît.

Étape 2. Cliquez sur la case d'option **Par adresse IP** pour entrer une adresse IP dans le champ Adresse IP/Nom du serveur. Cliquez sur la case d'option **Par nom** pour entrer le nom du serveur dans le champ Adresse IP/Nom du serveur.

Étape 3. Activez la case d'option **Version 4** ou **Version 6** pour saisir une adresse IP IP IPv4 ou IPv6, respectivement, dans le champ Server IP Address/Name. La version IP 6 ne peut

être sélectionnée que si une adresse IPv6 a été configurée sur le périphérique.

Étape 4. Saisissez une adresse IP IPv4 ou IPv6 de l'utilisateur SSH approuvé dans le champ Server IP Address/Name.

Étape 5. Entrez 16 paires de valeurs hexadécimales pour l'empreinte digitale du serveur SSH dans le champ Empreinte digitale. Pour obtenir la valeur d'empreinte du serveur SSH, accédez à **Security > SSH Server > SSH Server Authentication.** Il s'agit d'une fonctionnalité de SSH permettant de se protéger contre une attaque lorsqu'un utilisateur malveillant guide le client vers un autre serveur ou ordinateur pour apprendre le nom d'utilisateur et le mot de passe du serveur SSH approuvé. Le client est invité à vérifier l'empreinte digitale du serveur, puis à saisir ses informations d'identification.

Étape 6. Cliquez sur **Apply** pour enregistrer la configuration.