Configurazione dell'autenticazione server Secure Shell (SSH) per i client SSH sugli switch impilabili serie Sx500

Obiettivo

La funzionalità server Secure Shell (SSH) permette di stabilire una sessione SSH con gli switch impilabili della serie Sx500. Una sessione SSH è proprio come una sessione telnet, ma una sessione SSH è più sicura. La protezione viene ottenuta dal dispositivo quando genera automaticamente le chiavi pubbliche e private. Questi tasti possono anche essere modificati dall'utente. È possibile aprire una sessione SSH utilizzando l'applicazione PuTTy.

In questo documento viene spiegato come abilitare l'autenticazione SSH per i client SSH e definire i server trusted sugli switch impilabili della serie Sx500.

Dispositivi interessati

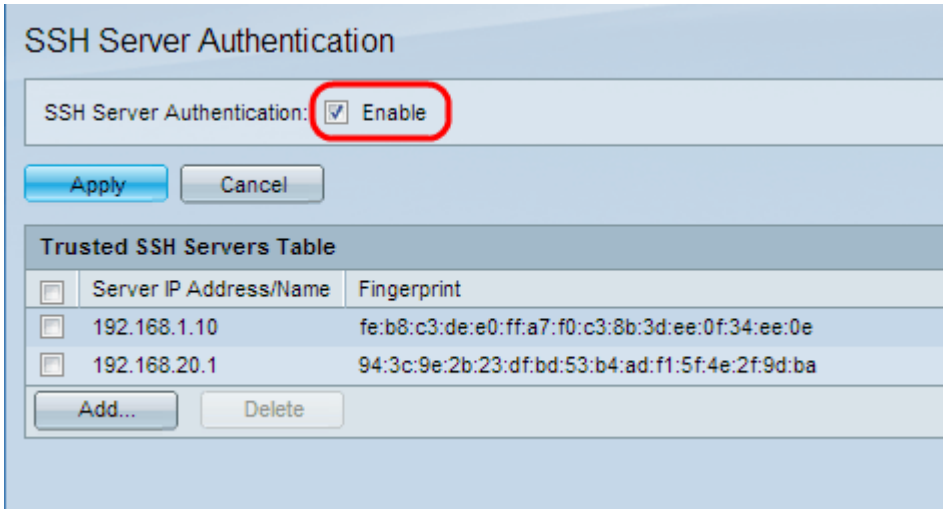
·Switch Stack Serie Sx500

Versione del software

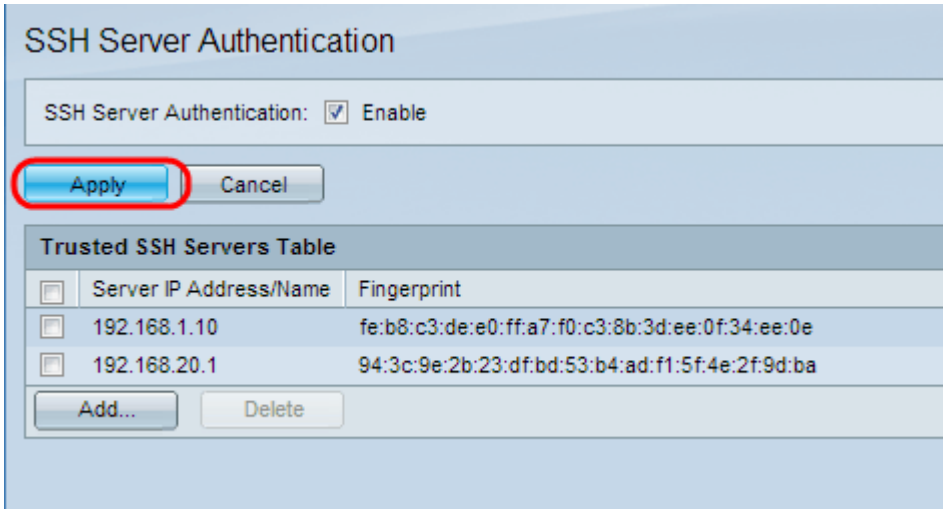
·v1.2.7.76

Configurazione dell'autenticazione del server SSH

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **Sicurezza > Client SSH > Autenticazione server SSH**. Si apre la pagina *SSH Server Authentication*:

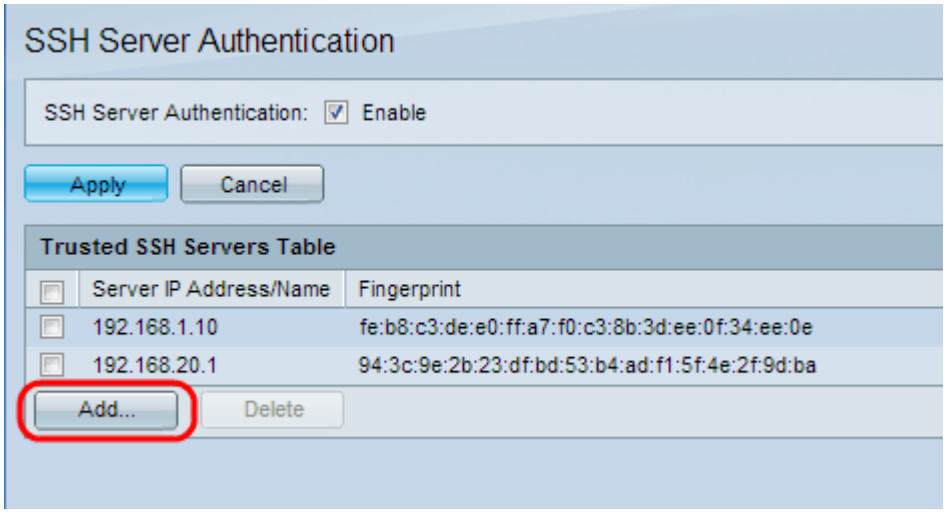


Passaggio 2. Selezionare **Enable** per abilitare l'autenticazione del server SSH.



Passaggio 3. Fare clic su **Applica** per salvare la configurazione.

Aggiungi server SSH attendibile



Passaggio 1. Nella tabella dei server SSH trusted è possibile trovare l'indirizzo IP e l'impronta digitale del server SSH. Fare clic su **Add** (Aggiungi) per aggiungere il server ssh attendibile. Viene visualizzata la finestra *Add Trusted SSH Server* (Aggiungi server SSH attendibile).

Passaggio 2. Fare clic sul pulsante di opzione **Per indirizzo IP** per immettere un indirizzo IP nel campo Indirizzo/nome IP server. Fare clic sul pulsante di opzione **Per nome** per immettere il nome del server nel campo Indirizzo IP server/Nome.

Passaggio 3. Fare clic sul pulsante di opzione **Versione 4** o **Versione 6** per immettere un

indirizzo IP IPv4 o IPv6, rispettivamente, nel campo Nome/Indirizzo IP server. È possibile selezionare la versione IP 6 solo se nel dispositivo è stato configurato un indirizzo IPv6.

Passaggio 4. Immettere un indirizzo IP IPv4 o IPv6 dell'utente SSH attendibile nel campo Indirizzo/nome IP server.

Passaggio 5. Immettere 16 coppie di valori esadecimali per l'impronta digitale del server SSH nel campo Impronta digitale. Per ottenere il valore relativo alle impronte digitali del server SSH, selezionare **Sicurezza > Server SSH > Autenticazione server SSH.** Questa funzionalità del protocollo SSH consente di proteggere il client da attacchi in cui un utente malintenzionato guida il client su un server o un computer diverso per conoscere il nome utente e la password del server SSH attendibile. Il client deve controllare l'impronta digitale del server e quindi immettere le credenziali.

Passaggio 6. Fare clic su **Apply** (Applica) per salvare la configurazione.