Contenu

Introduction

Ce document décrit comment installer le commutateur de données multicouche (MDS) 9000 pour transférer les informations par l'intermédiaire du protocole de Protocole Secure Shell (SSH) sans fournir un mot de passe pour l'utilisateur.

Problème

Transférer classe d'un commutateur MDS au-dessus de SSH, utilisant des protocoles comme le Secure Copy (SCP), exige un mot de passe par défaut. En mode interactif la fourniture d'un mot de passe de SSH peut être incommode et quelques scripts d'utilisateur externe peuvent ne pas pouvoir fournir le mot de passe en mode interactif.

Solution

Générez keypairs publics/privés sur le commutateur MDS et ajoutez la clé publique aux authorized_keys d'un compte utilisateur introduisent sur le serveur de SSH.

Conditions préalables

Pour cet exemple, un serveur Linux générique (RedHat, Ubuntu, etc.) configuré avec un serveur de SSH et le client installé.

Aperçu

Ce document trace les grandes lignes de l'étape nécessaire pour un transfert de SSH à partir du MDS 9000 à un serveur de Linux sans fournir un mot de passe, qui est décrit dans quatre étapes.

- Installant paire de clés publique/privée pour le compte utilisateur au lequel sera installé ? copie ? les données hors du commutateur. (c.-à-d. le compte la commande de SSH ou SCP dont sera exécuté, dans cet exemple ? testuser ?)
- Installation de paire de clés publique/privée pour le compte utilisateur sur l'hôte de Linux de sorte qu'utilisateur ? testuser ? au cas où la copie ou déplacer les informations hors du

commutateur sans devoir fournir le mot de passe de la demande de commutateur.
- Testez le SCP du commutateur à l'hôte de Linux.

Installation de paire de clés publique/privée pour le compte utilisateur sur le MDS

Du commutateur MDS 9000, créez le nom d'utilisateur ? testuser ? avec le mot de passe et le rôle comme réseau-admin. Veillez à créer l'utilisateur et l'utilisateur de rôle de réseau-admin pour que la génération de keypair fonctionne.

SSH dans le commutateur de l'hôte de Linux avec le nom d'utilisateur créé dans l'étape précédente :

Générez le keypair pour le testuser d'utilisateur utilisant la RSA avec la longueur de 1024 bits.

Exportez le keypair au bootflash : , fournissez la **phrase de passe** (celui qui vous voulez, notez juste lui quelque part.)

Installation de paire de clés publique/privée pour le compte utilisateur sur l'hôte de Linux

Copiez la clé publique de la RSA pour le testuser d'utilisateur du commutateur sur l'hôte de Linux avec le nom d'utilisateur présent de « testuser » déjà. Veuillez noter que vous devrez fournir le mot de passe pour le testuser de nom d'utilisateur qui peut ou peut ne pas être identique comme ce qui a été précédemment créé sur le commutateur.

> Remarque: Ces instructions utilisent un exemple où le chemin de compte de testuser est **/users/testuser**. Selon votre version Linux ce chemin peut être différent.

Sur le serveur Linux vous devez ajouter le contenu du fichier testuser_rsa.pub au fichier d'authorized_keys (ou à fichier authorized_keys2 selon votre version de SSH) :

Testez le SCP du commutateur à l'hôte de Linux.

Testez le SCP du commutateur au serveur Linux et vérifiez la copie du commutateur au serveur sans fournir le mot de passe. (Notez s'il vous plaît cela ? Aucun mot de passe n'est incité pour ? ?)