Contenido

Introducción

Este documento describe cómo poner el switch de datos de múltiples capas (MDS) 9000 para transferir la información vía el protocolo del Secure Shell (SSH) sin proporcionar a una contraseña para el usuario.

Problema

La transferencia clasifía de un Switch MDS sobre SSH, usando los protocolos como el Secure Copy (SCP), requiere una contraseña por abandono. Recíprocamente proporcionar a una contraseña de SSH puede ser incómodo y algunos scripts del usuario externo pueden no poder proporcionar la contraseña recíprocamente.

Solución

Genere los keypairs públicos/privados en el Switch MDS y agregue la clave pública a los authorized_keys de una cuenta de usuario clasifían en el servidor SSH.

Requisitos previos

Por este ejemplo, un servidor Linux genérico (RedHat, Ubuntu, etc.) configurado con un servidor SSH y el cliente instalado.

Información general

Este documento delinea los pasos requeridos para una transferencia SSH del MDS9000 a un servidor del linux sin proporcionar a una contraseña, que se describe en cuatro pasos.

- ¿Configurando los pares del público/de clave privada para la cuenta de usuario a la cual será puesto? ¿copia? el Switch de los de los datos. ¿(es decir la cuenta de las cuales el comando de SSH o de SCP será ejecutada, en este ejemplo? testuser?)
- ¿Configurar los pares del público/de clave privada para la cuenta de usuario en el host de Linux de modo que usuario? ¿testuser? si la copia o mover el Switch de los de la información

sin tener que proporcionar la contraseña del prompt del Switch.
- Pruebe SCP del Switch al host de Linux.

Configurar los pares del público/de clave privada para la cuenta de usuario en el MDS

¿Del Switch MDS9000, cree el nombre de usuario? ¿testuser? con la contraseña y el papel como red-admin. Aseegurese crear el usuario y al usuario del papel red-admin para que la generación del keypair trabaje.

SSH en el Switch del host de Linux con el nombre de usuario creado en el paso anterior:

Genere el keypair para el testuser del usuario usando el rsa con la longitud de 1024 bits.

Exporte el keypair al bootflash: , proporcione el **passphrase** (sea cual sea usted quiere, apenas anota él en alguna parte.)

Configurar los pares del público/de clave privada para la cuenta de usuario en el host de Linux

Copie la clave pública rsa para el testuser del usuario del Switch sobre el host de Linux con el nombre de usuario presente del “testuser” ya. Observe por favor que usted necesitará proporcionar la contraseña para el testuser del nombre de usuario que pueden o no pueden ser lo mismo que lo que fue creada previamente en el Switch.

> Nota: Estas instrucciones utilizan un ejemplo donde está **/users/testuser la** trayectoria de la cuenta del testuser. Dependiendo de su versión de Linux esta trayectoria puede ser diferente.

En el servidor Linux usted necesita agregar el contenido del archivo testuser_rsa.pub al archivo de los authorized_keys (o al archivo authorized_keys2 dependiendo de su versión de SSH):

Pruebe SCP del Switch al host de Linux.

Pruebe SCP del Switch al servidor Linux y verifique la copia del Switch al servidor sin proporcionar a la contraseña. ¿(Observe por favor eso? No se indica ninguna contraseña para??)