Contents

Introduction

This document describes how to setup the Multilayer Data Switch (MDS) 9000 to transfer information via the Secure Shell (SSH) protocol without providing a password for the user.

Problem

Transferring files from an MDS switch over SSH, using protocols like Secure Copy (SCP), requires a password by default. Interactively providing an SSH password can be inconvenient and some external user scripts may not be able to provide the password interactively.

Solution

Generate public/private keypairs on the MDS switch and add the public key to a user account authorized_keys file on the SSH server.

Pre-requisites

For this example, a generic Linux server (RedHat, Ubuntu, etc.) configured with an SSH server and client installed.

Overview

This document outlines the steps required for an SSH transfer from the MDS 9000 to a linux server without providing a password, which is described in four steps.

- Setting up the public/private key pair for the user account which will be setup to “copy” the data out of the switch. (i.e. the account from which the SSH or SCP command will be executed, in this example “testuser”)
- Setting up the public/private key pair for the user account on the Linux host so that user “testuser” should copy or move the information out of the switch without having to provide the password from the switch prompt.
- Test SCP from the switch to the Linux host.

Setting up the public/private key pair for the user account on the MDS

From MDS 9000 switch, create the username “testuser” with password and role as network-admin. Make sure to create the user and network-admin role user for keypair generation to work.

SSH into the switch from the Linux host with the username created in previous step:

Generate the keypair for user testuser using rsa with length of 1024 bits.

Export the keypair to bootflash:, provide the **Passphrase** (Whatever you want, just make a note of it somewhere.)

Setting up the public/private key pair for the user account on the Linux host

Copy the rsa public key for user testuser from the switch onto the Linux host with username "testuser" already present. Please note that you will need to provide the password for username testuser which may or may not be the same as what was previously created on the switch.

> **Note**: These instructions use an example where the testuser account path is **/users/testuser**. Depending on your Linux version this path may be different.

On the Linux server you need to add contents of the testuser_rsa.pub file to the authorized_keys file (or authorized_keys2 file depending on your version of SSH):

Test SCP from the switch to the Linux host.

Test SCP from the switch to Linux server and verify the copy from switch to the server without providing the password. (Please note that “No password is prompted for…”)