Instructions for Setting Up F-Secure to F-Secure SSH File Transfer

Version 0.11

Purpose

ECS/EMD secure ingest and secure distribution use applications collectively known as secure shell (ssh) to download and upload files. ECS/EMD uses the F-Secure ssh implementation but any ssh implementation should work on the target system. By default, password authentication will be used and files transferred in an encrypted tunnel. F-Secure Secure Shell (ssh2) provides the capability to send files from an F-Secure ssh2 client to an F-Secure ssh2 server in the clear after the session is authenticated. Since the stream is sent in the clear, the overhead associated with encryption is saved providing the best throughput. However, to implement the no encryption capability, F-Secure must be implemented on the target host, ECS/EMD user keys must be generated and uploaded to the target system and the target system account needs to be setup to accept user key based connections.

Prerequisites

1. An account and password on the target host.
2. An initial login capability on the target host in order to establish a user public/private key pair.
3. The target host must have a version of Perl installed. No additional modules are required.
4. On each target host, the installer will need to know in which directory ssh is installed (/usr/local/bin us the default) and the user's home directory name (/home/<username> is the default).
5. F-Secure ssh 3.2.3 must be installed on the ECS/EMD system.

ECS/EMD Installation

The genkeys.pl script should be copied to /usr/local/bin on those hosts from which secure ingest or secure distribution is installed.

Conventions

Bold - represents user input to the keyboard and ↵ means to press the enter/return key
<targethost> - information within <> is site specific

Procedure

1. The installer should login to a secure distribution/secure ingest host using the account that will be used by the ECS/EMD application.

2. The installer must know the local passphrase. Coordinate with other users if this is a group account or you may break something in the system. If after such coordination the passphrase is not known and there is an existing home .ssh2 directory (~/.ssh2), then move the existing directory using the commands:

   % **mv ~/.ssh2 ~/.ssh2.OLD ↵**

3. Run sshsetup to make sure that all the ancillary files are available to secure shell using the command:

   % **sss ↵**
   Use a passphrase of at least 10 characters which should include
   numbers or special characters and MAY include spaces

   New passphrase: <**useagoodonebutnotthisone> ↵**
   Retype new passphrase: <**useagoodonebutnotthisone> ↵**

   Generating ssh2 keys. This can take up to 240 seconds...
   Done with sshsetup!

NOTE: Select a good passphrase! If there is already a local passphrase, you will not be prompted to put in another. Running sss is still useful because it assures that the ancillary files that ssh uses are there.

4. Using the account and password provided by the data provider, the installer should next upload the genkeys.pl file to the target host using the command:
   % **scp2 /usr/local/bin/genkeys.pl <targethost>: ↵**

5. Ssh to the target host using the command:
   % **ssh2 <targethost> ↵**

6. Determine the home directory by using the command:
   % **pwd ↵**
   Record the results.

7. Find out where ssh2 lives by using the command:
   % **which ssh2 ↵**
   Record the results.

8. Using the information from the previous two steps, setup the keys and other ancillary files using the command:
   % **/usr/local/bin/genkeys.pl ↵**

```
Enter ssh local directory (default: /usr/local/bin): ↵

Enter user's local home directory (default: /home/user): ↵

Enter key name (default: ecs): <targethost> ↵

Generating keys...
When prompted, respond with a passphrase.
Generating 1024-bit dsa key pair

   1 oOo.oOo.oOo.

Key generated.
1024 bit DSA key for user @ targethost.pub
Passphrase : <useagoodonebutnotthisone> ↵
Again      : <useagoodonebutnotthisone> ↵

(NOTE: THE PASSPHRASE IS NOT ECHOED!!!)

Private key saved to /home/user/.ssh2/id_dsa_1024_a
Public key saved to /home/user/.ssh2/id_dsa_1024_a.pub
Generating an ssh identification file.
Generating a local environment file.
Generating the sshconcat2 utility.
Generating a configuration file.
Concatenating the keys...
Done!
```

   NOTE: If you get a “bad interpreter” or similar error when running the command, use the command:
   % **perl genkeys.pl ↵**

9. Exit from the target host using the command:
   % **exit ↵**

10. Upload the ECS public key from the secure ingest/secure distribution host using the command:

```
% /usr/local/bin/upload.pl ↵
Enter ssh local directory (default: /usr/local/bin): ↵

Enter user's local home directory (default: /home/user): ↵

Enter remote port (default: 22): ↵

Enter remote account (default: user): ↵

Enter remote host (default: t1acg04u.ecs.nasa.gov): ↵

Enter key name (default: ecs): pvc ↵

Uploading the key to t1acg04u.ecs.nasa.gov...
Please respond with the requested password/passphrase.
If a yes/no question is asked, press y <enter>.

Host key not found from database.

Key fingerprint:

xurav-dytut-guzan-kosis-rolyd-rypin-cisez-panop-dysop-zemef-zuxux

You can get a public key's fingerprint by running

% ssh-keygen -F publickey.pub

on the keyfile.

Host key saved to
/home/user/.ssh2/hostkeys/key_22_t1acg04u.ecs.nasa.gov.pub

host key for t1acg04u.ecs.nasa.gov, accepted by user Wed Oct 29 2
003 09:39:26 -0500

**************************************************************

                  U.S. GOVERNMENT COMPUTER
     If not authorized to access this system, disconnect now.

            YOU SHOULD HAVE NO EXPECTATION OF PRIVACY
By continuing, you consent in your keystrokes and data content
being monitored.

**************************************************************


Keyboard-interactive:

Password authentication
```

```
user's password: <targethostpassword> ↵
pvc.pub                  |   718B |   718B/s | TOC: 00:00:01 | 100%

Concatenating the keys... Please respond with the requested
password/passphrase.
user's password: <targethostpassword> ↵
Done!
```

11. Verify that the procedure was done correctly by first starting the secure shell agent:
    % **ssa** ↵
    Enter passphrase: <**useagoodonebutnotthisone**> ↵

12. Ssh to the target using the command:
    % **ssh2 <targethost>** ↵

13. You should NOT be prompted for a password or passphrase.

14. Attempt an ssh2 session with each <targethost> so that the host keys will be automatically setup.

15. Logoff.

16. If you are prompted for a password or a passphrase, remove the ~/.ssh2 directories on each end and try again. If the repeat effort does not work, call the ECS/EMD helpdesk.