OpenSSH Server

OpenSSH is a freely available version of the SSH connectivity tools, and is the standard version of SSH used by many Linux distributions. See http://www.openssh.org/ for more information.

Contents

1. Overview

No current version of OpenSSH currently natively supports Moonshot, but patches are available for versions 5.3p1, 5.9p1 and 6.6p1 of OpenSSH to fix the issues that stop it from working. Ultimately we hope that these patches will become a standard part of OpenSSH, so that OpenSSH will work without any extra work being necessary.

2. Installation Instructions

How you set up a Moonshot-enabled version of the OpenSSH server will differ depending on your OS. See the relevant pages for your particular distribution:

- CentOS / RHEL / SL
- Debian / Ubuntu / Raspbian
- Alpine Linux

3. Building Instructions

Although we endeavour to supply packages in our own repositories, we also provide build instructions for popular distributions.

4. Client Compatibility

The following clients are known to work with this server software using Moonshot authentication (click on the link to see further information about enabling Moonshot in that client):

- OpenSSH Client

5. Next Steps

Once you have installed the software, what happens next?

5.1. Configuration Instructions

Once installed, the Moonshot-enabled OpenSSH server will still need a few quick tweaks in order to turn on the Moonshot support.

1. Ensure that `/etc/radsec.conf` and the certificates referenced in it can be read by the SSH user:

   ```
   su - --shell=/bin/bash sshd
   cat /etc/radsec.conf
   cat path_to_ca.pem
   cat path_to_client.pem
   cat path_to_client.key
   ```

   If they cannot be read by the SSH user, add the SSH user to the group that can read the certificates.
2. Configure the OpenSSH server to use GSSAPI by editing `/etc/ssh/sshd_config`. Check the following lines are present and uncommented:

```
GSSAPIAuthentication yes
GSSAPIKeyExchange no
GSSAPIStrictAcceptorCheck yes
```

GSSAPIStrictAcceptorCheck

If your SSH server has a different hostname to the one given publicly (for example, you have CNAME entries you give to your users instead of the internal name), you must switch the **`GSSAPIStrictAcceptorCheck`** to **`no`**. Disabling (commenting out) the check configuration defaults it to **`yes`**.

CentOS 6 and UsePrivilegeSeparation

OpenSSH server versions before 6.6p1 cannot use Moonshot authentication when **`UsePrivilegeSeparation`** is switched to **`yes`** or **`sandbox`**. You must switch **`UsePrivilegeSeparation`** to **`no`** on those versions.

3. Restart the OpenSSH server.
4. Configure the OpenSSH Client.

5.2. Account Mapping

Read our General account mapping advice page before you go any further to get an overview of the general options available for mapping federation provided identities to local accounts.

Moonshot functions by using SAML or RADIUS attributes to convey user information. You can use one or multiple attributes to check which account the user should log into your SSH Server as. We have made available two versions of the Moonshot mechanism, one by default uses Shibboleth libraries, while the other uses internal JSON attribute resolution.

To read more about this, visit Configure a Linux Server's Attribute Resolution, and use either mechanism to configure the attribute '`local-login-user`' which the SSH server will use to establish the account to log in with.