InstantSSH Plugin

> This documentation is for the latest version available in our plugins store. For an oldest documentation, see the **README** file inside the plugin archive.

Introduction

This plugin allows to give your customers a full or restricted shell.

A customer to which SSH permissions are given can create SSH users and use them to login on the server.

For each customer, you can set the maximum number of allowed SSH users and choose if they can override the default authentication options. The authentication options are those specified in the documentation of the authorized_keys file.

Requirements

- i-MSCP version >= 1.2.3
- openSSH server with both, password and key-based authentication support enabled

> If you want allow only the key-based authentication, you can set the **passwordless_authentication** configuration option to **TRUE** in the plugin configuration file.

> Be aware that this plugin doesn't handle the **AllowUsers** SSH configuration parameter. Thus, if you're using this parameter in your **/etc/ssh/sshd_config**, this plugin will not work. Support for this parameter will be added in later release.

Debian / Ubuntu packages

- bash
- binstats
- build-essential
- busybox-static or busybox

- flex
- libpam-chroot
- psmisc
- python
- strace

You can install these packages by executing the following commands:

```
# aptitude update
# aptitude install bash build-essential busybox-static flex \
libpam-chroot psmisc python strace
```

Installation

1. Be sure that all requirements as stated in the requirements section are meets
2. Upload the plugin through the plugin management interface
3. Install the plugin through the plugin management interface

Note: Depending on your system, installation can take up to several minutes. Time is needed to build jail.

Update

1. Be sure that all requirements as stated in the requirements section are meets
2. Backup your plugin configuration file if needed
3. Upload the plugin archive through the plugin management interface
4. Restore your plugin configuration file if needed (compare it with the new version first)
5. Update the plugin list through the plugin management interface

Note: Prior any update attempt, do not forget to read the **UPDATE** file inside the plugin archive.

Configuration

Authentication options

Default authentication options are set as follow;

```
no-agent-forwarding,no-port-forwarding,no-X11-forwarding
```

which in order:

- Forbids authentication agent forwarding
- Forbids TCP forwarding
- Forbids X11 forwarding

You can override default authentication options by editing the **default_ssh_auth_options** option

which is defined in the plugin configuration file. In that file, you can also restrict the list of authentication options that your customers can add by editing the **allowed_ssh_auth_options** option. You must note that any authentication option appearing in the the default authentication string must also be specified in the **allowed_ssh_auth_options** option.

Jailed shells

The jailed shells allow you to provide SSH access to your customers in a restricted environment from which they can theoretically not escape. It's the preferable way to give an SSH access to an un-trusted customer.

Several commands can be added into the jails by simply adding the required application sections to the app_sections configuration option.

The default configuration comes with a set of preselected application sections which allow to setup very restricted jailed shell environments.

Be aware that the creation of the jailed environments may take time, depending on many factors such as the type of your server, the number of file to copy inside the jails and so on...

See the config.php file inside the plugin archive for further details.

Note: When changing a configuration parameter in the plugin configuration file, do not forget to trigger plugin change by updating the plugin list through the plugin management interface.

Troubleshootings

PAM chroot module

The PAM chroot module shipped with some libpam-chroot package versions doesn't work as expected. For instance, You can see the following logs in the /var/log/auth.log file:

```
...
Oct 13 21:04:31 lucid sshd[1509]: PAM unable to
dlopen(/lib/security/pam_chroot.so): /lib/security/pam_chroot.so: undefined
symbol: __stack_chk_fail_local
Oct 13 21:04:31 lucid sshd[1509]: PAM adding faulty module:
/lib/security/pam_chroot.so
...
```

You can fix this easily by following this procedure:

```
# cd /usr/local/src
# mkdir libpam-chroot
# cd libpam-chroot
# apt-get install build-essential debhelper libpam0g-dev
# apt-get source libpam-chroot
```

```
# cd libpam-chroot*
```

Edit the Makefile file to replace the line:

```
CFLAGS=-fPIC -O2 -Wall -Werror -pedantic
```

by

```
CFLAGS=-fPIC -O2 -Wall -Werror -pedantic -fno-stack-protector
```

Rebuild and reinstall the package as follow:

```
# dpkg-buildpackage -uc -us
# cd ..
# dpkg -i libpam-chroot*.deb
```

License

```
i-MSCP InstantSSH plugin

@author Laurent Declercq <l.declercq@nuxwin.com>
@copyright (C) 2014-2015 Laurent Declercq <l.declercq@nuxwin.com>
@license i-MSCP License <http://www.i-mscp.net/license-agreement.html>
```

See the **LICENSE** file inside the archive for further details.