Mission Guide: F-Response Collect for Linux

Your Mission: Install and run the F-Response Collect Subject on Linux

Using F-Response Collect to acquire data from a Linux computer

Important Note

Disclaimer: F-Response works diligently to stay on top of operating system and user interface changes between releases. However, you may be dealing with a Linux computer where the display does not match what you see here exactly. Please use your best guess and if you have issues, you are welcome to reach out and we'll do our best to assist you.

Step 1: What is F-Response Collect for Linux?

F-Response Collect for Linux ("fr-collect-sub") is a native software application developed on x86_64 Linux to provide device, filesystem, and user directory collection options for the Linux platform. It is provided on our website on the downloads page (https://www.f-response.com/support/downloads) as RPMS for Redhat/Centos/Rocky Linux 7,8, and 9.

The F-Response Collect for Linux executable is a subject executable, meaning it has no graphical component and is only designed to run in the background. It follows the same process as other F-Response Collect subject executables in that it talks to your Collect Server, retrieves tasking, and executes those tasks.

Step 2: How do I install the rpm file and what is it doing?

In order to install F-Response Collect for Linux you will need root or administrative rights on the Linux machine and the ability to install rpm software. You will also need to use the F-Response Collect Management Console under windows to export a "non-windows" configuration file, specifically the "fr-collect-sub.cfg" file as referenced in the manual.

Once you have both the RPM from the F-Response website and the configuration file from your Management Console on the Linux machine, you are ready to begin.

Start by opening a terminal window or an SSH session (via putty or similar tool) and installing the rpm file using either "yum" or the "rpm" command:

```
#sudo rpm -Uvh F-Response-Collect-Subject-<VERSION>.x86_64.rpm
```

This will make the following changes:

- Create the /etc/fr-collect-sub directory if it does not exist.
- Create an empty /etc/fr-collect-sub/fr-collect-sub.cfg file if it does not exist.
- Copy the fr-collect-sub executable to /usr/local/bin.
- Create a fr-collect-sub.service in the /etc/systemd/system directory.
- Start the fr-collect-sub service.

The final step required is to replace the configuration file at /etc/fr-collect-sub/ with the exported one from the F-Response Collect Management Console. This is how the software will know where to go to connect to the Collect server and obtain tasking.

Once the file is replaced the service can be restarted using the following commands via terminal:

```
#sudo service fr-collect-sub stop
```

```
#sudo service fr-collect-sub start
```

Step 4: What are the Linux targets for Collect and what do they mean?

F-Response Collect for Linux offers device, profile, and custom collection targets. Profiles are simply the contents of the /home/<USERNAME> directory. Custom collections are based off the mount tab (/etc/mtab) mounted volumes and allow you to decide what gets collected just like existing F-Response Collect custom collections.

Important note: While F-Response Collect for Linux will automatically restart in the event of a loss in connectivity, it will NOT resume from where it left off for all targets. The application will see that a task needs to be performed and will restart performing it, but the restart will begin at position zero for profiles/home directories and custom collections. Full device and volume collections will resume within 50 megabytes of where they left off as normal.

In addition, for home directories and custom collections, the percentage complete will rapidly reach 99% or 100% but will still be growing. That’s because, unlike Windows, we are unable to pre-assess the total collection size sufficiently to create an accurate completion percentage. This is just a factor of how the technology works on this platform.