Last Stand Cloud - Alpha Build 3.0

Introduction:

Hello! Thank you for enrolling in the latest Alpha build of Last Stand Cloud! The goal of this software is to allow anyone to create and host their own home cloud, accessible from both their own local network as well as anywhere out in the world! This software is intended to be used like popular cloud services from big companies, (iCloud, OneDrive, etc.) that you own yourself. This latest alpha build is the second to last alpha release for Last Stand Cloud. Following the next release, Last Stand Cloud will officially move to the Beta Stage hopefully by the next year. I am working on the final features needed on the checklist, including the most necessary features that have been Last Stand Cloud's most marketable feature.

The following features, promised in the last alpha, are finally here:
- Timed, scheduled backups for a drive/file/directory that you can pass in as an argument to the client
- A database that the client utilizes upon the startup of your computer to continue your scheduled backups
- A database where the server stores the hashes of all files to ensure correctness with file retrieval without adding massive overhead to the server
- A configuration file for the server so no direct interaction with the server executable is required
- An installer script that will configure and allow the server to be run as a daemon process in the background so you don't have to run it actively in a terminal, there is also an installer script for the client.

The final list, the features required for the end of the alpha stage are:
- Finally, the ability to remotely connect to your server outside of your local LAN, and connect to it over the internet. End to end encrypted, without our API acting as a middle man
- The ditching of the 'server_id' file, and the ability to connect to any of your servers from any client installed on any computer

Now, these features may take longer than expected to develop, so I don't know whether or not it will be completed before the new year, but I will try day in and day out to get this software to the next level. We are trying to surpass Nextcloud and Owncloud with our usability, because right now, Last Stand Cloud is just an inferior version of those companies' products. I also have begun deciding a different monetization structure for the business, and that will be reflected on laststandcloud.com once the beta stage is reached.

Usage:

This alpha has expanded the user interface and functionality to allow for much more control on the client end. For many of the added features, there are flags to be passed in for statistics and version info. For laststandserver, you can call the executable with these flags to get information separately from the running version of the server. Now, once you run the install.sh and client-install.sh scripts, laststandcloud and laststandserver will be able to be called globally in your terminal/bash shell.

For dependencies, you will need to have OpenSSL, libssl and curl installed, which are included by default in many operating systems or can be installed easily with your operating system's package manager.

However, if they are not installed, the installer scripts for the server AND the client will install them for you. Python3 is a requirement once again, but it is only used by the installer scripts and are not needed to run the client or the server.

Also, a brand new service called Last Stand Verify has gone live to better authenticate servers AND protect your privacy. Previously, laststandcloud.com would authenticate your server and generate a certificate and private key, storing it in a database and the client would have to check if the certificate is valid after connecting to the server. This caused lots of problems in the previous version, and it would allow Last Stand Cloud to decrypt your data and analyze it. This has been completely overhauled and re-secured with Last Stand Verify. Last Stand Verify is our new Certificate Authority, and it functions just like a Certificate Authority that helps your favorite websites utilize HTTPS and secure mail, and coming soon you will be able to use Last Stand Verify for a web certificate. What this means for Last Stand Cloud, however, is that each server will create its own private key when it is first run, and generate a certificate request that will return a signed Last Stand Verify certificate. Then, the server will check every few hours to see if the certificate will expire, and request a new one when they certificate expires. This means that all we see is the server's public certificate and we cannot decrypt your data even if we wanted to. Also, another step has been included so that the server will not run/handle clients if the server is using a self-signed certificate. This is done to ensure that the server is who it says it is and your data will not be compromised. Outside certificates are also fine, but the server will automatically grab a new signed certificate from Last Stand Verify for free whenever it needs one.

Now, for the actual usage of the server:
- First of all, with the permissions and writing that the server needs to do its job, it must be run as 'sudo' or a superuser, or else it will exit. The server will not run if it is not being used as a superuser.

Next, to run the server, you call the executable without any arguments or flags.
The flags available are:
[i,v,o,d]

i/v - stands for [INFORMATION/VERSION] get the current information about the current version of Last Stand Cloud

o - this flags stands for [OUTPUT]. it takes an argument and will output to the console various usage statistics of a currently running laststandserver instance.

[OPTIONS]

if - prints out the server's private and public IPv4 addresses

hardware - prints out the server's RAM and disk usage

time - the current running time of the server

all - print out all of the above information

h - prints out a manual page that describes all of this information

For the client:
- This version of the client does not require 'sudo' access when it is first called. When the client requires root access, it will ask for the sudo password
to run the client and backup a file, run:

./laststandcloud [filepath]

and it with back up the file specified in [filepath]. Now, similar to the server,
it can be called with flags:
[i,v,f,s,t,b]

i/v - same as server, get the information about the current version of Last Stand Cloud

f [filepath] - stands for [FETCH] grab the file specified by [filepath] and store it in the designated location, ex. "home/user/file.ext" will store "file.ext" in"home/user/"

s - this stands for [STATS] and is similar to -o all on the server end, it will query the server for its

usage statistics and print them to the terminal.

t [hours] - stands for [TIMED] set to backup a file every [hours] hours. You will next be prompted for the file path of the file you want to backup periodically

b - stands for [BACKUPS], and you can get the information on all your timed backups, or remove one

[OPTIONS]

list - list the current backups running, shows the file being backed up and how often it is being run

remove - lists the current backups running, and their current PID, 0 if it is not currently running

Scope:

This alpha is the last alpha to add non-keystone features of Last Stand Cloud before its beta stage. With this version, FreeBSD support has been added once again. The server is pretty much in its final state before it is released for beta, and the client still needs major work. Once beta is reached, more refined security and a GUI will be the main development goals. For now, the server will be installed as a daemon like it will in the finished product and run perpetually on your computer, so there is always major room for errors there.

What I Need You to Do:

Bugs:

The bug hunt is the most important part of this alpha, and the most valuable help that Last Stand Cloud can be given. Simple one-off errors like being unable to run the client or server because its dedicated port is in use, or your network connection going out and cancelling or corrupting a backup is not what I'm looking for. Generally, if an easy to read error message is printed out or something is written in either the net_errors or bit_errors logs, it's not what I'm talking about. However, something like, one specific file type causing the same error to be printed in the logs would count. Anything that causes a core dump, abort trap or and kind of segmentation fault is key for us to learn about. Anything unusual, that doesn't seem like it was intentional or even anything you think can be optimized and improved, let us know!

Reporting:

This is the most boring part of the task I need you to complete for me. I need to, once you find a legitimate bug, report to me in the most descriptive way possible, using screenshots, timestamps, anything you can find or can tell me about exactly what happened. I need you to accurately describe to me every little detail you can think of. Anyone who finds me a legitimate bug will get 1 free year of the premium version of Last Stand Cloud. At this time, I cannot offer any financial rewards or compensation, but that may of course change over time. While Last Stand Cloud is still small, we unfortunately can't repay you like Microsoft or Valve would for finding bugs but we will not forget you, and if we ever can we will help repay Of course, final say for whether or not you get credited is up to me based on the quality of your report. Reports are of course a first-come, first-served basis; and the first person to report the bug will be the one who is rewarded. This is done based on when the issue was sent, not by the time we received it for fairness' sake.

To report a bug, message me at: laststandcloud@protonmail.com with your

full report, or fill out the issue report form on the website
Also, send me feature requests and if it I decide to use it, you will receive the same rewards as above

Thank you to everyone who signed up! I appreciate what you are doing for me -Vincent Trolia