1. Setting Up

1.1. General Prerequisites

`Linux x86_64` server accessible by valid domain name (DNS) from the Internet.

1.2. Minimal Hardware Requirements for server

- 2 CPU/vCPU cores
- 4 GB RAM
- SSD storage

> The CPU can be high if you are using the video recording function in rooms.

1.3. Requirements for Brocha client software

Supported browsers

- Chrome 74+
- Firefox 70+
- Safari 14+

1.4. Network Accessibility Checklist

- The firewall allows inbound TCP/UDP connections to the following ports
  - HTTP `80`, HTTPS `443`
  - WebRTC RTP ports `49152..65535`

A `brocha` executable must be run by a non-root user and be allowed to listen on `80` and `443` network ports. To do this, run the following `setcap` command on Linux:

```
sudo /usr/sbin/setcap 'cap_net_bind_service=+ep' ./brocha
```

Brocha server must be accessible by `https` protocol and this is a mandatory requirement. Thus, you need to point your domain registrar's DNS server to the actual IP address of the Brocha server.

1.5. Running a Server

```
Usage: ./brocha [options]

  -c <cfg>             .ini configuration file
  -d <dir>             Data files directory
  -n <domain>          Domain name used to obtain Let's Encrypt certs
  -l <ip>[@<pub ip>]   Listen IP or IP mapping if server behind NAT
  -p <port>            Server network port number
  -a <password>        Resets the password for `admin` account
  -s                   The server runs behind an HTTPS proxy
  -t                   Clear database data on start
  -v                   Show version and license information
  -h                   Show this help message
```

Use `-a` option to set an initial password for `admin` account at first run. Later in `Admin UI` you may add other users and change your password.

1.6. Brocha server with Real IP Address

```
./brocha -n <domain name>
```

Example:

```
./brocha -n conferences.mycompany.com
```

In this case, Brocha automatically installs Let's Encrypt HTTPS certificates for `https://conferences.mycompany.com`

1.7. Brocha server behind NAT

```
./brocha -n <domain name> -l '<private ip>@<public ip>'
```

1.8. Brocha server behind an HTTP proxy

We do not advice running Brocha behind an HTTP proxy, as this will break one of the strongest features of this product — the ease of installation and configuration.

Keep in mind — Brocha WebRTC RTP ports (usually in range `49152..65535`) must be accessible from external network even when server is behind a HTTP proxy. So it is wrong to bind the server to `localhost` behind the proxy.

Example of Apache2 Proxy Configuration

```
<VirtualHost *:443>
    SSLCertificateFile /etc/letsencrypt/live/<domain name>/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/<domain name>/privkey.pem
    Include /etc/letsencrypt/options-ssl-apache.conf

    ProxyRequests            Off
    ProxyPreserveHost        On

    ProxyPass         /ws/channel  ws://<brochaip>:8080/ws/channel
    ProxyPassReverse  /ws/channel  ws://<brochaip>:8080/ws/channel

    ProxyPass         /            http://<brochaip>:8080/
    ProxyPassReverse  /            http://<brochaip>:8080/

    <Location "/">
        RequestHeader set X-Forwarded-Proto "https"
        RequestHeader set X-Forwarded-Port "443"
    </Location>
</VirtualHost>
```

```
a2enmod ssl proxy proxy_http proxy_wstunnel
```

```
./brocha -s -p 8080
```

Example of NGINX Proxy Configuration

```
server {
  server_name     <domain name>;
  listen 443 ssl;
  ssl_certificate /etc/letsencrypt/live/<domain name>/fullchain.pem;
  ssl_certificate_key /etc/letsencrypt/live/<domain name>/privkey.pem;
  include /etc/letsencrypt/options-ssl-nginx.conf;
  ssl_dhparam  /etc/letsencrypt/ssl-dhparams.pem;

  location /ws/channel {
    proxy_pass http://<brochaip>:8080/ws/channel;
    proxy_http_version 1.1;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "upgrade";
  }
  location / {
    proxy_pass       http://<brochaip>:8080/;
    proxy_redirect  default;
  }
}
server {
  server_name     <domain name>;
  listen  80;
  if ($host = <domain name>) {
    return 301 https://$host$request_uri;
  }
  return 404;
}
```

```
./brocha -s -p 8080
```

2. Brocha.ini Configuration

Server parameters can be specified in the `.ini` configuration file, as shown in the example below.

```
./brocha ... -c ./brocha.ini ...
```

2.1. Example of brocha.ini

```
./brocha -c <config.ini>
```

```
;; Brocha example configuration.
;;
;; Any part of configuration may contain placeholders ( {...} )
```

```
;; which will be replaced by the following variables:
;;
;;  {home}              Path to the user home directory.
;;  {cwd}               Current working directory of brocha process.
;;  {config_file_dir}   Path to directory where configuration file resides.
;;  {program}           Path to brocha executable.
;;

[main]

;; IP address to listen.
;; Also defines a mapping between private and public ip
;; for servers behind NAT of Docker for webrtc protocol.
;;
;;  The following forms are supported:
;;
;;  - auto - server will autodetect IP address to listen.
;;  - <ip> - real ip address to listen.
;;  - <private ip>@<public ip> - Mapping of <private ip> to <public ip> if
server behind NAT.
;;
;; `ip` option is overridden by `-l <ip>[@<pub ip>]` command line option
;;
;; Example:
;;  ip = 0.0.0.0@192.168.1.37

ip = auto

;; HTTP/HTTPS listen port.
;; If cert_file / cert_key_file / domain_name specified this
;; port will be used for HTTPS traffic.
;; Overridden by `-p <port>` command line option
;;
;; Example:
port = 8888

;; DNS domain name of server in order to obtain Let's Encrypt TLS
certificate.
;; Overridden by `-n <domain>` command line option
;;
;; Example:
domain_name = foo.example.com

;; HTTP port used to redirect incoming HTTP request to HTTPS protocol
endpoint.
;; Option used to pass ACME challenge during process of generating Let's
Encrypt TLS certificates.
https_redirect_port = 80

;; Data directory with database, screen recordings and uploads.
data = {cwd}
```

```
;; Path to x509 PEM certificate and key file for TLS layer
;;
;; Example:
cert_file = {config_file_dir}/cert.pem
cert_key_file = {config_file_dir}/key.pem

;;
;; Max age of sessions cookies in seconds.
;; Default: 2592000 (30 days)
;;
;; If -1 specified the session cookies will be removed when browser closed.

session_cookies_max_age = 2592000

;; Stun / turn servers
[servers]

;; Stun and turn servers.
;;
;; Examples:
;; ice_servers = stun:stun.l.google.com:19305 stun:stun1.l.google.com:19305
stun:stun2.l.google.com:19305
;; ice_servers = turn:openrelay.metered.ca:444
;; ice_servers = turn:openrelay.metered.ca:443?transport=tcp
;; ice_servers =
openrelayproject:openrelayproject@turn:openrelay.metered.ca:443?transport=tcp

;


;; RTC / WebRTC options
[rtc]

;; WebRTC RTP ports range
ports = 49152..65535
```

Brocha server configuration reference