Jitsi on OpenBSD

Puffy presents video conferencing

Philipp Buehler
sysfive.com GmbH
Hamburg, Germany
pb-openbsd@sysfive.com

***Abstract*—This paper will cover all bits and bolts to fully understand the components at play, their intercommunications and how this knowledge can be used to create a Jitsi-on-OpenBSD setup that features a restricted (compartmentalized) setup using dedicated machines or -as shown- VMM based VMs, where each VM runs only one of the components.**

It'll be documented what's necessary to create a sensible pf.conf on each VM and how to add reverse proxy (relayd, haproxy) for distribution of workload.

Also covering pitfalls/hints along underlying components and what to lookout for on the client/browser side for interopability.

***Index Terms*—Jitsi, OpenBSD, VMM**

I. Introduction

Jitsi and OpenBSD are both not covered much as a documented setup. Installation documents for Jitsi are almost always about Linux OS (and there mostly Debian) and do not cover some internals. The reference documentation on the other hand can be very overwhelming.

There is some FreeBSD "all in one" port (package) with no explanation and it cannot be used to install core components (only) on different nodes.

This documentation is to show a distributed install on OpenBSD using pre-packages and need-to-function (minimum) firewall settings (‘pf.conf‘).

The described configurations will enable a fully integrated video conferencing to be available at ‘https://jts.fips.de‘ - adapt the setting accordingly for your domain.

II. Riddles

Both major players show obstacles that have to be overcome to gain a functioning installation.

A. Jitsi

A "full blown" Jitsi installation can consist over over a dozen components and all the necessary networking/firewalling configuration can be exhaustive. Any possible discovery magic is not documented.

Some configuration snippets are undocumented and tend to make the understanding poorer not better. Worst example are necessary DNS settings and ‘nginx.conf.‘

The typical answer to be found on asking question is to use the official ‘all-in-one‘ Debian VM.

B. OpenBSD

This also leds to the question if it's possible to run a (core) Jitsi installation on OpenBSD only or if there's need be for Linux (VM).

Also it's a bit difficult to find example-based documentation on VMM, e.g. for using VMM as the core router, too. (Combination ‘vm.conf‘+‘pf.conf‘s).

Can we scale the installation horizontally and how to use Java based applications with ‘rcctl‘.

III. Components

A. OpenBSD

In this example setup I make heavy use of ‘VMM‘ eco system on OpenBSD which consists of:

- ‘vmm(4) - virtual machine monitor:‘ kernel driver isolating/providing the required resources for the VMs (hypervisor)
- ‘vmd(8):‘ userland daemon to interact with ‘vmm‘
- ‘vmctl(8)‘: administrative tool to create, start/stop, .. VMs
- ‘vm.conf(5)‘: persist VMs resource configuration

B. Jitsi

A ‘core‘ (basic video conferencing) setup comprised by:

- ‘nginx(8)‘ web: serving web assets and reverse proxy BOSH or websockets
- ‘prosody(8)‘ xmpp: conference chat + internal components communication (esp.PubSub for health/discovery)
- ‘jicofo‘ JItsi COnference FOcus: room+session handling in conferences (whos talking to whom and where)
- ‘jvb‘ videobridge: mediastream (WebRTC) handlings between participants (SFU)
- ‘jibri‘ JItsi BRoadcasting Infrastructure (optional): recording + streaming conferences

IV. Architecture

To host the Jitsi components in a VM each, this uses the following architecture (see Figure 1).

V. Communications

Communications between the components and the logical ‘publication‘ + ‘subscription‘ in Jitsi is as follows (needed in ‘pf.conf‘ later on) (see Figure 2+3).

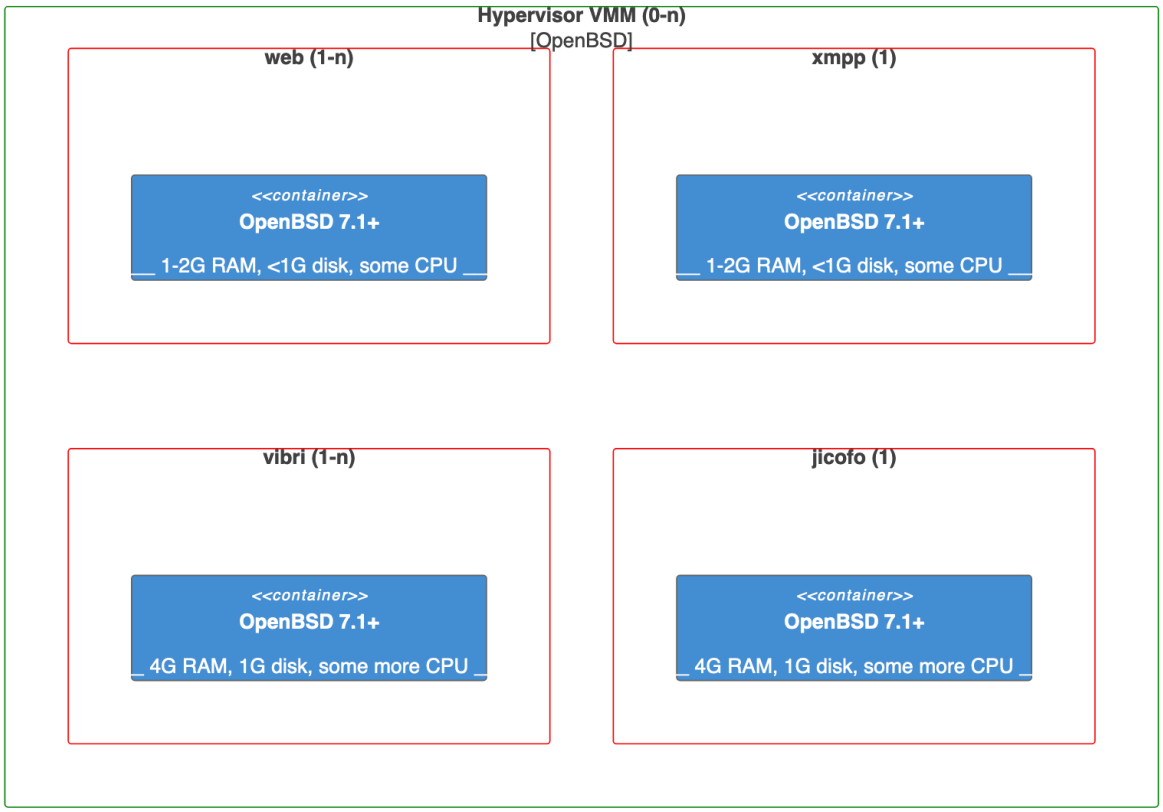

Fig. 1. OpenBSD VMM architecture

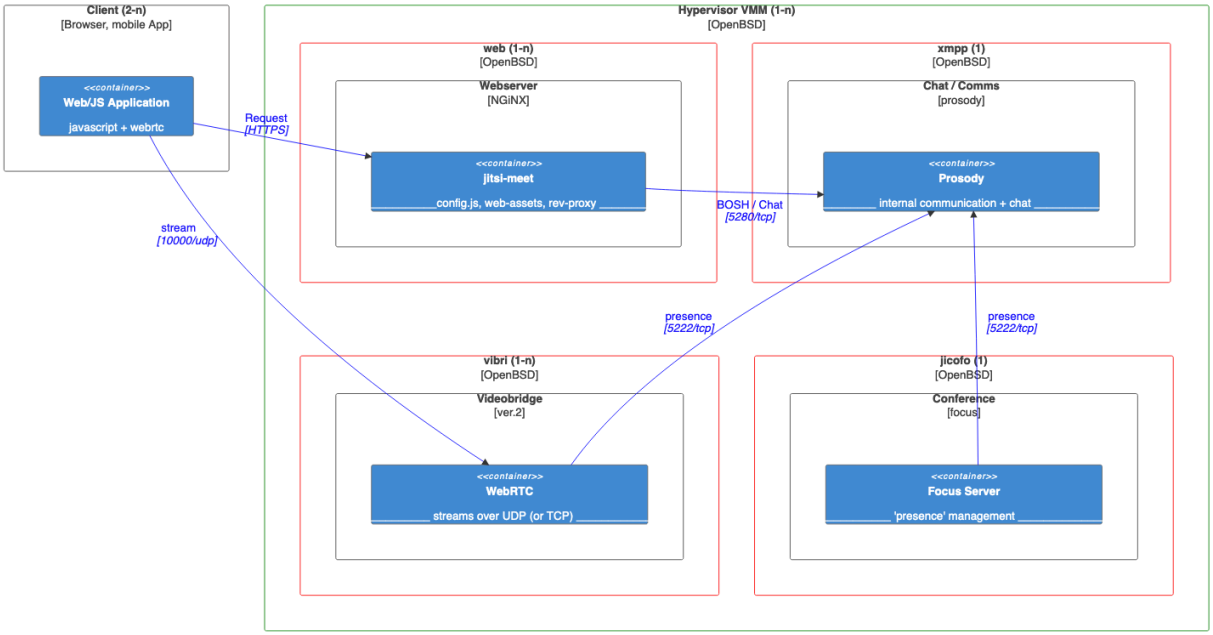

Fig. 2. OpenBSD VMM architecture

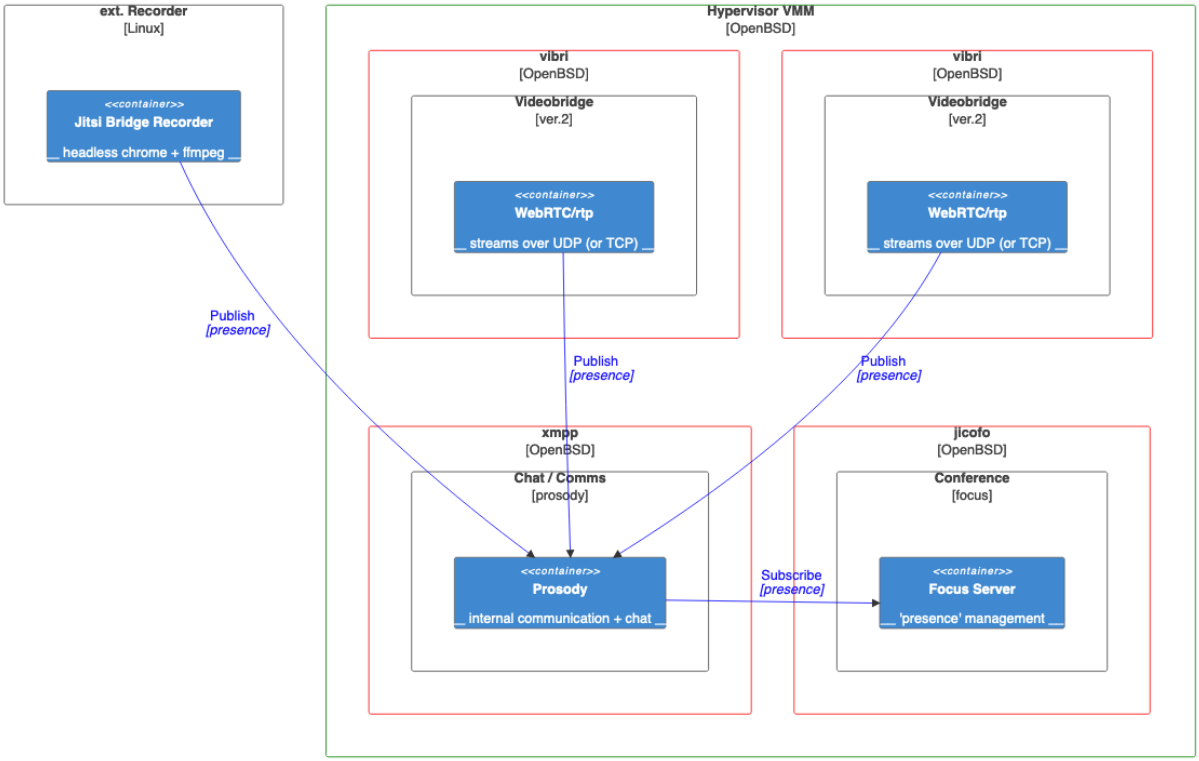

Fig. 3. OpenBSD VMM architecture

VI. Installation

The installation is structered in the following steps:

- create VM images
- construct /etc/vm.conf
- add hosts / DNS
- ‘nginx‘: install, config, certs
- ‘prosody‘: pkg install, config, certs, users
- ‘jicofo‘: pkg install, config
- ‘jvb‘: pkg install, config

A. VM setup

To create an VM image being used in the following setup:

```
rcctl enable vmd; rcctl start vmd
mkdir /home/vmm; cd /home/vmm
vmctl create -s 5G web.qcow2
ftp https://cdn.openbsd.org/pub/OpenBSD
/7.1/amd64/install71.iso
vmctl start -m 2G -L -i 1 -r install71.iso\
-d /home/vmm/web.qcow2 web
vmctl console web
## run the (I)nstaller, default options.
## only one 'a' slice on (w)hole disk
## halt -p (so new sshd_keys per VM)
vmctl stop web
for vm in xmpp jicofo jvb ; do
cp web.qcow2 ${vm}.qcow2; done
echo 'net.inet.ip.forwarding=1' >> \\
/etc/sysctl.conf
```

The VM definitions in ‘/etc/vm.conf‘ as follows. The ”instance” tells ‘vmctl‘ to use ”web”’s configuration as a template and only adapt changes like ”disk” or ”memory” to it.

```
vm "web" {
  enable
  memory 2G
  disk "/home/vmm/web.qcow2" format qcow2
  local interface { up }
}
vm "web" instance "xmpp" {
  disk "/home/vmm/xmpp.qcow2" format qcow2
}
vm "web" instance "jicofo" {
  memory 4G
  disk "/home/vmm/jicofo.qcow2" format qcow2
}
vm "web" instance "jvb" {
  memory 4G
  disk "/home/vmm/jvb.qcow2" format qcow2
}
```

B. DNS + /etc/hosts

DNS: ONE A-RR for jts.fips.de; but local hosts for jicofo (or split DNS).

The following ‘/etc/hosts‘ needs to be on each VM and on the VMM host. Use these names in ‘/etc/myname‘, too.

```
100.64.1.3     web
100.64.2.3     xmpp jts.fips.de
```

```
100.64.3.3    jicofo
100.64.4.3    jvb
```

VII. Firewalling

On each VM the following ‘pf.conf‘ is for good (admin) measure:

```
block return log
pass out quick on egress proto { tcp udp }
  to any port { 123 53 80 443 }
pass in quick on egress proto tcp
  from $admin to port 22
```

A. VMM

Assumption that all traffic hits the VMM external IP-address (on egress) here:

```
pass in on egress proto tcp to any
  port { 80 443 } rdr-to web
pass in on egress proto udp to any
  port { 10000 } rdr-to jvb
pass in proto tcp from { jvb jicofo }
  to xmpp port 5222 # native
pass in proto tcp from web to xmpp
  port 5280 # http/BOSH
pass in on egress proto tcp to any
  port 5280 rdr-to xmpp # debug
# DNS
vms={ web xmpp jicofo jvb }
pass in proto { udp tcp } from $vms
  to any port domain rdr-to $resolver
```

B. web/nginx

The webserver needs the basic ports and for the proxy connection to BOSH an outgoing to 5280/tcp.

```
pass in quick on egress proto tcp
  to self port { 80 443 }
pass out quick on egress proto tcp
  to xmpp port 5280
```

C. prosody

The XMPP ”native” only used from jicofo and jvb. The BOSH as above and if need be the dedicated auth via 5347/tcp (not covered here).

```
pass in proto tcp from { jicofo jvb }
  to self port { 5222 }
pass in proto tcp from web
  to self port 5280
pass in proto tcp from { $admin }
  to self port { 5280 5347} # debug
```

D. jicofo

Jicofo talks to prosody as above. The webclient connects to jicofo via 10000/udp. There is an administrative connection possible to 8080/tcp to establish e.g. monitoring with prometheus. for scale out the 10000/udp can be changed and would make use of a port range e.g. 10000:10050 vertically or explicit rdr-to in VMM for horizontally.

```
pass out quick on egress proto
  tcp to xmpp port { 5222 5280 }
pass in quick on egress proto
  udp to self port 10000
pass in quick on egress proto
  tcp from $monitor to self port 8080
```

E. videobridge

The videobridge only needs to reach out to prosody. The monitoring exporter on 8888/tcp seems to be broken (no values) as of this writing.

```
pass out quick on egress proto
  tcp to xmpp port 5222
pass in quick on egress proto
  tcp from $monitor to self port 8888
```

VIII. Prosody

To install prosody some simple steps are enough:

```
pkg_add unzip--
pkg_add prosody
pkg_add jitsi-prosody-plugins
```

The ‘jitsi-prosody-plugins‘ does contain two needed plugins and some more for use cases not mentioned in this document. Need be is ‘mod_client_proxy‘ and ‘mod_roster_command‘. The modules do not need further configuration in ‘prosody.cfg.lua‘. ‘client_proxy‘ gets loaded from the ”Component” configuration. ‘roster_command‘ is CLI only. The configuration key bits in ‘/etc/prosody/prosody.cfg.lua‘ are:

```
http_interfaces = { "*", "::" }
VirtualHost "jts.fips.de"
    authentication = "anonymous";

    modules_enabled = { "bosh";
      "pubsub"; }
    c2s_require_encryption = false

VirtualHost "auth.jts.fips.de"
    admins = { "focus@auth.jts.fips.de",
     "jvb@auth.jts.fips.de" }

    ssl = { key =
     "/var/prosody/auth.jts.fips.de.key";
        certificate =
    "/var/prosody/auth.jts.fips.de.crt"; }

    authentication = "internal_hashed"

Component "conference.jts.fips.de" "muc"
Component "jvb.jts.fips.de"
    component_secret = "CHANGE_jvb"
Component "focus.jts.fips.de" "client_proxy"
    target_address =
      "focus@auth.jts.fips.de"
Component "internal.auth.jts.fips.de" "muc"
    muc_room_locking = false
    muc_room_default_public_jids = true
```

The additional ‘FQDN‘ are internally only and do NOT need any DNS configuration (like an HTTP ‘Host‘ header).

It’s possible that ‘jvb‘ follows the example of ‘focus‘ to change authentication from shared secret to a user (‘target_-address‘).

A. Users

The connection for ‘jvb‘ uses a shared secret as shown on the previous page. For further users in use here:

```
rcctl enable prosody
rcctl start prosody
prosodyctl register focus \
  auth.jts.fips.de CHANGE_FOCUS
prosodyctl mod_roster_command \
  subscribe focus.jts.fips.de \
  focus@auth.jts.fips.de
```

B. TLS

Besides WebRTC demanding to use ‘https‘ between browser and server side, we shall encrypt all internal traffic, too. For the prosody connections:

```
prosodyctl cert generate \
  auth.jts.fips.de
# fill in `openssl req` dialog

cd /var/prosody
yes | /usr/local/jdk-11/bin/keytool
  -import -alias prosody -file \
  auth.jts.fips.de.crt -keystore \
  jicofo-key.store -storepass jitsicool

cp jicofo-key.store jvb-key.store
# copy to VM jicofo and jvb accordingly
```

‘keytool‘ comes with JDK, this task can also be done on jicofo or jvb VM - or copy over the resulting store-files to jicofo/jvb VM respectivly. Do NOT change JDK’s ‘lib/security/cacerts‘ - any later upgrade from jdk-11 would ”forget” the changed keystore.

IX. NGINX

To install nginx and the jitsi web elements (javascript, images, ..) only two packages are needed:

```
pkg_add nginx
pkg_add jitsi-meet
```

Any TLS setup is mandatory or Chrome/Firefox/.. will refuse to let you use the camera and microphone. Using Let’s Encrypt with ‘acme-client‘ for the TLS setup is easily possible and included in ‘./testing-config/nginx.conf‘ (see ”Availability” section).

A. web

The configuration for nginx is pretty straight forward:

```
server_name  jts.fips.de;
root         /var/www/jitsi-meet;
ssi on;
ssi_types application/x-javascript
  application/javascript;

location ~ ^/(libs|css|static|images|
  fonts|lang|sounds|
  connection_optimization)/(.*)$ {
  add_header
    'Access-Control-Allow-Origin' '*';
  alias /var/www/jitsi-meet/$1/$2; }
location /external_api.js { alias
  /var/www/jitsi-meet/libs/external_api.min.js; }
location = /http-bind {    # BOSH
  proxy_pass      http://xmpp:5280/http-bind;
  proxy_set_header X-Forwarded-For
    $remote_addr;
  proxy_set_header Host $http_host; }
location ~ ^/([a-zA-Z0-9=\?]+)$ {
  rewrite ^/(.*)$ / break; }
```

If using Let’s Encrypt, put the ‘.well-known‘ location first after ‘ssi‘ configuration.

B. jitsi-web

The configuration for the webclient goes to ‘/var/www/jitsi-meet/config.js‘:

```
var config = {
  hosts: {
    domain: 'jts.fips.de',
    muc: 'conference.jts.fips.de'
  },
  bosh: '//jts.fips.de/http-bind',
  useTurnUdp: false,
  ^^IenableWelcomePage: true,
  prejoinConfig: {
    enabled: true,
    hideExtraJoinButtons:
      ['no-audio', 'by-phone'] },
  p2p: {
    stunServers: [
    { urls:
     'stun:meet-jit-si-turnrelay.jitsi.net:443'
    } ] }
}
```

The use of TURN servers depend on NAT environment(s), most often it is needed (esp. p2p).

X. JICOFO

The installation is one package and the configuration is split into two files plus adaptions of the infra/systems configuration.

A. JVM / startup

```
pkg_add jicofo
cat << EOF > /etc/jicofo/jicofo.in.sh
JICOFO_CONF=/etc/jicofo/jicofo.conf
JICOFO_LOG_CONFIG=\
 /usr/local/share/\
 jicofo/lib/logging.properties
JICOFO_TRUSTSTORE=\
```

```
 /etc/ssl/jicofo-key.store
JICOFO_TRUSTSTORE_PASSWORD=jitsicool
JICOFO_MAXMEM=3G
JICOFO_DHKEYSIZE=2048
JAVA_SYS_PROPS=""
EOF
```

jicofo-key.store is generated from prosody certificate, see prosody in section 'VIII/B'. One can enable an XMPP-packet-debug-log in logging.properties if need be.

B. Parameters

The main configuration for jicofo is '/etc/jicofo/jicofo.conf':

```
jicofo { bridge {
  brewery-jid =
    "JvbBrewery@internal.auth.jts.fips.de"
  xmpp-connection-name = Client }
  sctp { enabled = false }
  xmpp {
    client {
      port = 5222
      domain = "auth.jts.fips.de"
      username = "focus"
      password = "CHANGE_FOCUS"
      use-tls = true
    }
    // trusted service domains.
    //  Logged in -> advance to bridges
    trusted-domains =
      [ "auth.jts.fips.de" ]
  }
}
```

For proper startup and reachability it's needed to add "jicofo_-flags="–host=jts.fips.de"" to '/etc/rc.conf.local'. This needs to be present in '/etc/hosts' or in (split) DNS and the resolved IP address must point to the VM's local address! Since this is used as a matching string for "virtual host" one cannot use an IP address here!

For proper logging add this to syslog configuration and then jicofo can be started

```
cat <<EOF >> /etc/syslog.conf
!jicofo
*.*     /var/log/jicofo
EOF
rcctl enable jicofo
rcctl start jicofo
```

XI. VIDEOBRIDGE

The installation is one package and the configuration is split into two files plus adaptions of the infra/systems configuration.

Installing 'jitsi-srtp' is optional, but the speedup in encryption of WebRTC is substantial. There's no additional configuration needed, if present JVB will load the native library just by standard means ('ld.so(1)').

A. JVM / startup

```
pkg_add jitsi-videobridge
pkg_add jitsi-srtp
cat << EOF > /etc/jicofo/jvb.in.sh
JVB_CONF=/etc/jvb/jvb.conf
JVB_LOG_CONFIG=\
 /usr/local/share/jvb/lib/logging.properties
JVB_TRUSTSTORE=/etc/ssl/jvb-key.store
JVB_TRUSTSTORE_PASSWORD=jitsicool
JVB_MAXMEM=3G
JVB_DHKEYSIZE=2048
JVB_GC_TYPE=G1GC
JAVA_SYS_PROPS=""

#/etc/jvb/sip-communicator.properties
JVB_SC_HOME_LOCATION='/etc'
JVB_SC_HOME_NAME='jvb'
EOF
```

jvb-key.store is generated from prosody certificate as for jicofo. Can be same file as /etc/jicofo/jicofo-key.store if both are on one VM.

B. Parameters

The main configuration file is '/etc/jvb/jvb.conf' as referenced above.

```
videobridge { apis {
  xmpp-client {
   configs {
    ourprosody {
     hostname = "xmpp"
     domain =
      "auth.jts.fips.de" // realm
     username = "jvb"
     password = "CHANGE_jvb"
     muc_jids =
      "JvbBrewery@internal.auth.jts.fips.de"
     muc_nickname = "jvb-foo"
     disable_certificate_verification =
      true
    } } } }
  sctp { enabled = false } // n/a on OpenBSD
  ice { tcp {
    enabled = false
    port = 443
   } udp {
    port = 10000
   }
  }
}
```

The 'JvbBrewery' part is a fixed string and cannot be replaced!

A third party library needs its own configuration file in '/etc/jvb/sip-communicator.properties' as referenced in 'jvb.in.sh'. The following must be written in three lines and are just split up due to format reasons.

```
org.ice4j.ice.harvest.\
 NAT_HARVESTER_LOCAL_ADDRESS=100.64.4.3
org.ice4j.ice.harvest.\
 NAT_HARVESTER_PUBLIC_ADDRESS=87.253.170.146
org.ice4j.ice.harvest.\
 DISABLE_AWS_HARVESTER=true
```

The LOCAL is the VMs internal address, the PUBLIC must be the one ”presented” to the outside world (e.g. nat-to on egress).

JVB does not need any ‘rc.conf‘ settings, but add this for logging and startup:

```
cat <<EOF >> /etc/syslog.conf
!jvb
*.*      /var/log/jvb
EOF
rcctl enable jvb
rcctl start jvb
```

XII. Pitfalls / Hints

There are some typical pitfalls that should be avoided eventually.

A. OpenBSD

- ‘rc.conf‘: using IP address instead of hostname/FQDN
- startup ordering: nginx, prosody, jicofo, jvb – or wait times increase (pubsub)

B. Jitsi

Jitsi can have some more subtle ones and some are just advisable.

- xmpp: host vs. virtualhost vs. domain
- DNS: one and only one (or mess up xmpp fallback)
- not disabling sctp (jvb AND jicofo)
- (hidden) version bumps (”no longer component!”)
- jicofo has an XMPP-packetlogger (see ‘logging.properties‘)
- patience, be really patient (at initial start)
- always check the ‘,‘ in config.js (JSON after all..)

XIII. Status

It works! Most of the packages have landed in 7.2 already:

- ‘net/jitsi/meet‘
- ‘net/jitsi/jicofo‘
- ‘net/jitsi/videobridge‘
- ‘net/jitsi/srtp‘
- ‘net/jitsi/prosody-plugins‘

A ‘meta‘ package to bundle all of the above is still in development/review.

XIV. Outlook

The jitsi component ‘jibri‘ for recording and/or streaming conferences can only run on Linux for now. Main work would be needed to realize that in an Alpine or NixOS VM or going the long way to get ”chromedriver” running on OpenBSD.

Another component might be ‘jigasi‘ for SIP/POTS, but unsure about demand and feasability.

XV. Acknowledgments

I want to make a shoutout to ‘Jitsi‘ and ‘OpenBSD‘ of course. A sincere ”THANK YOU” to Aisha Tammy spending lots of effort on making the packages and get them upstream.

My employer to be thanked as well allowing so many hours working on this project.

XVI. Availability

This paper, presentation slides and other directly related resources can be found on github: https://github.com/double-p/presentations/AsiaBSDCon/2022/

References

[1] OpenBSD project https://www.openbsd.org/
[2] Jitsi https://github.com/jitsi/
[3] sysfive.com GmbH https://www.sysfive.com/

XVII. Logfiles

Some typical logfiles pointing to ”known” errors:

```
# wrong/missing keystore [in prosody logfile]:
Sep 16 14:35:58 c2s60a86b47480  info
  Client connected
Sep 16 14:35:58 c2s60a86b47480  info
  Client disconnected: sslv3 alert certificate unk

# wrong password [in prosody logfile]:
Sep 16 14:36:20 c2s60b1aced0c0  info
  Stream encrypted (TLSv1.3 with TLS_AES_256_GCM_S
Sep 16 14:36:21 c2s60b1aced0c0  info
  Client disconnected: connection closed

# all good [in prosody logfile]:
Sep 16 14:37:00 c2s60a5b549900  info
  Stream encrypted (TLSv1.3 with TLS_AES_256_GCM_S
Sep 16 14:37:01 c2s60a5b549900  info
  Authenticated as focus@auth.jts.fips.de

# on cannot use a jvb before this log [in jicofo l
Jicofo 2022-09-16 14:45:24.260 INFO: [35]
 [type=bridge brewery=jvbbrewery]
 BaseBrewery.addInstance#341: Added brewery
 instance: jvbbrewery@internal.auth.jts.fips.de/jv

# JVB loading SRTP lib (only active connections)
INFO: [71] JitsiOpenSslProvider.<clinit>#52:
 jitsisrtp successfully loaded for OpenSSL 1.1
```