

Kamailio as a Stateless, Containerized SBC

Jan Lorenz

WHOIS?

pascom®





- About 10 years experience
- Developer @pascom since 2012
- Hobbyist Photographer
- jan.lorenz@pascom.net

WHOAMI

WHAT?



We build the pascom PBX for small to medium sized businesses



SIP-via-TLS

SRTTP for Media

-Provisioning

HTTPS-Management

Multi-tenant cloud solution - encrypt as
much as possible

WHY KAMAILIO?

- Dashboard
- mobydick instances
- Proxy instances
- Images
- System
- Jobs

Dashboard

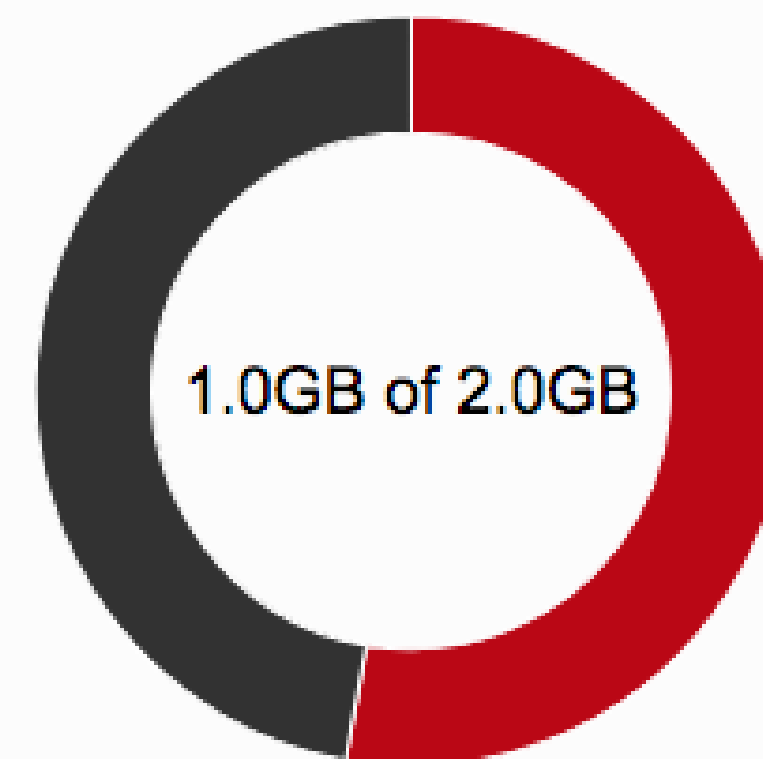
License

This is a Community License. You can create at most 2 mobydick instances with community edition license.

CPU

Load average: 0.13 0.09 0.09

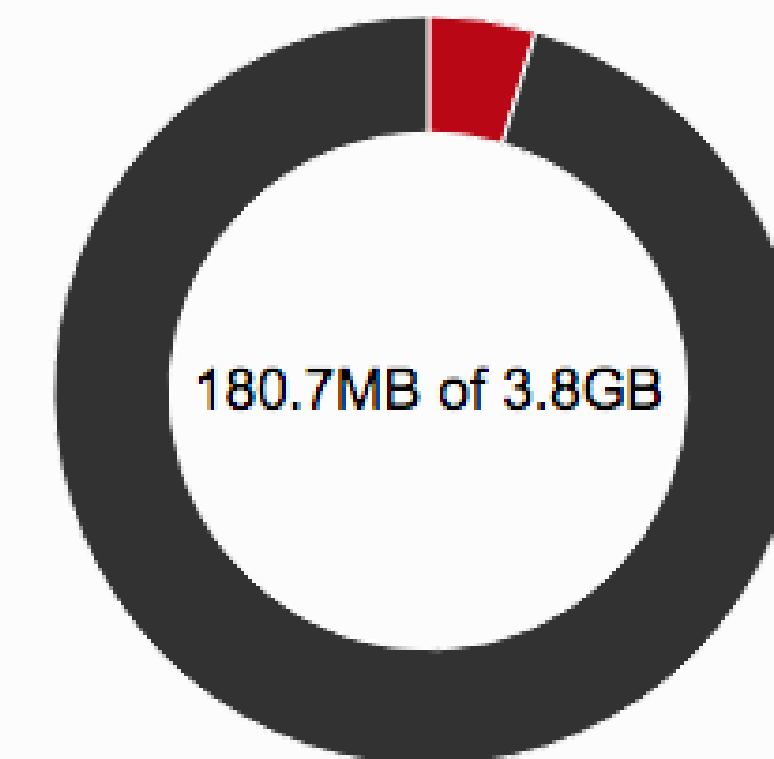
Memory



Images

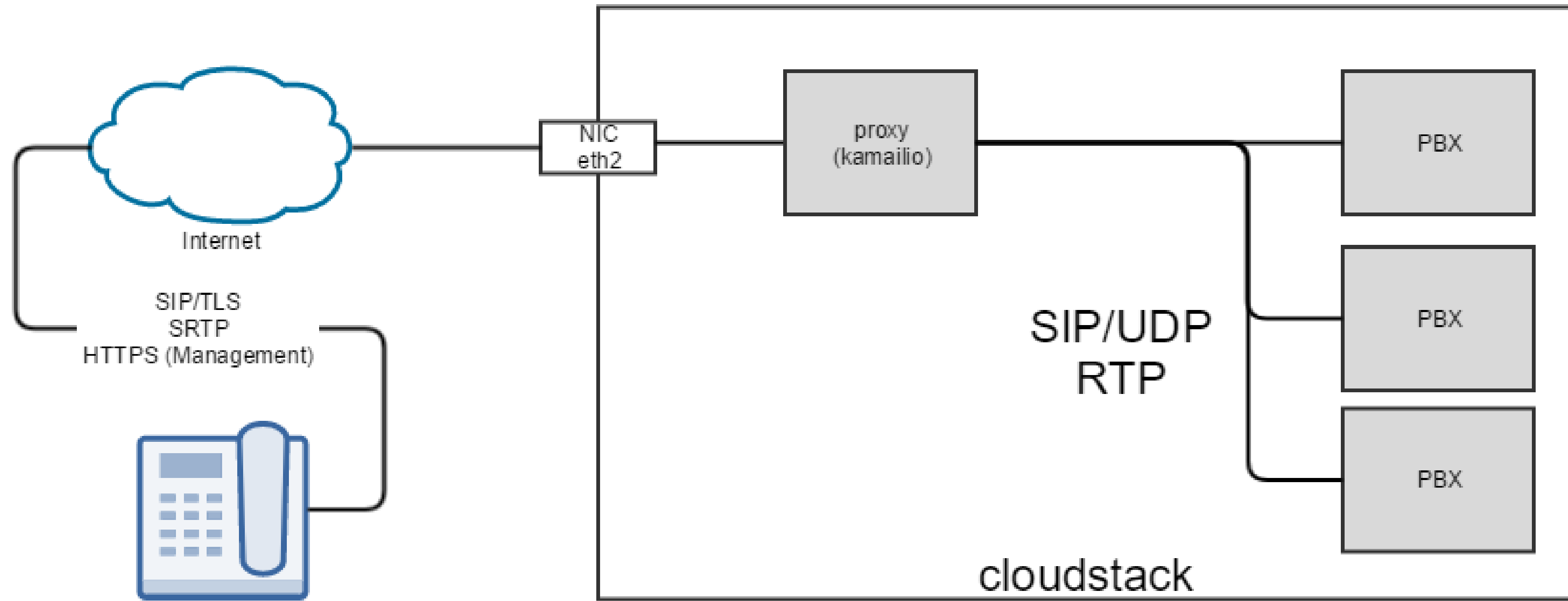
6 images installed

Swap



To protect our containerized PBX instances in our multi-tenant cloud solution

IMPLEMENTATION



Architecture Overview


```
},  
"memory" : {  
  "default" : 256,  
  "min" : 256,  
  "max" : 512  
},  
  
"variables": {  
  "INTERFACE_MODE": {  
    "en": { "label": "Type of network connection: nat, bridge"},  
    "de": { "label": "Art der Netzerkanbindung: nat, bridge" },  
    "required": true,  
    "matches": "^nat|bridge$",  
    "default": "nat"  
  },  
  "PUBLIC_NIC": {  
    "en": { "label": "Public Interface"},  
    "de": { "label": "Public Interface" },  
  },  
}
```

Kamailio in an (almost) stateless lxc container

```
}  
  
# Handle SIP registrations  
route[REGISTRAR] {  
    if (!is_method("REGISTER")) return;  
    if(isflagset(FLT_NATS)) {  
        setbflag(FLB_NATB);  
    }  
  
    route(TOMD);  
    route(RELAY);  
    exit;  
}
```

Offload registration to Asterisk

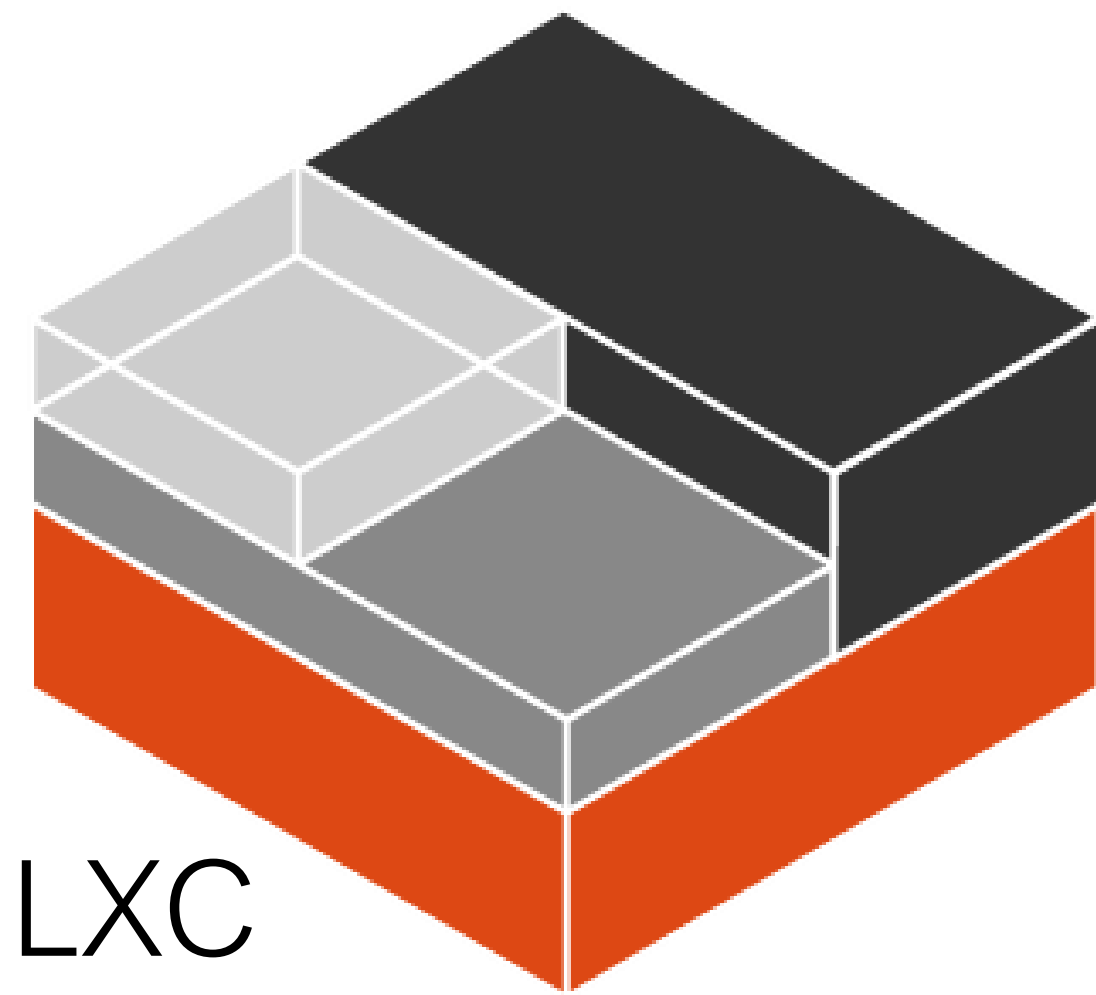


Routing without state

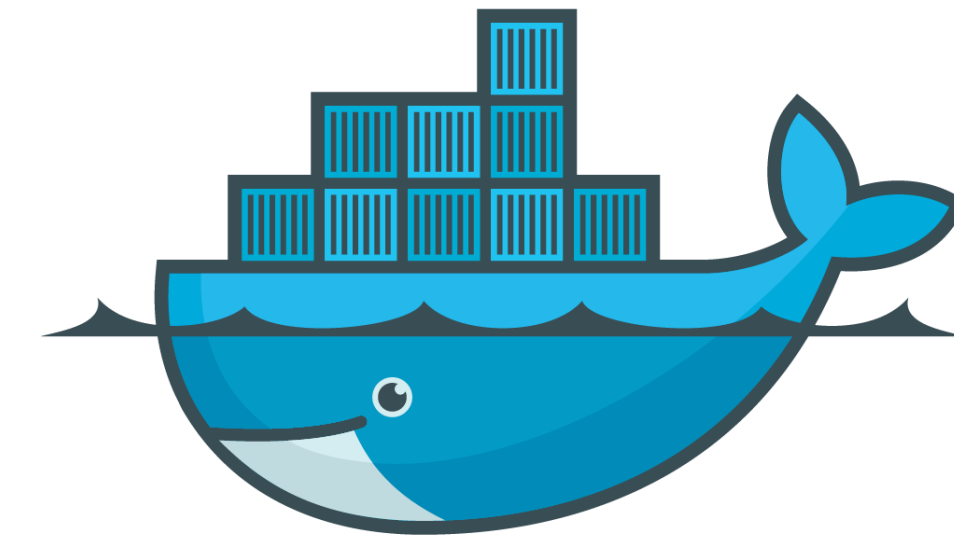

```
Allowed.Trsp : UDP
Def. Username: rky5BZu588400c2
SIP Options : (none)
Codecs      : (gsm|ulaw|alaw|h264)
Codec Order : (alaw:20,ulaw:20,gsm:20,h264:0)
Auto-Framing : No
Status      : OK (23 ms)
Useragent   : snomD315/8.9.3.40
Reg. Contact : sip:rky5BZu588400c2@10.5.6.233;xmd=31302e312e312e31315e33343836325e7369703a726b7935425a753538
Qualify Freq : 60000 ms
Keepalive   : 0 ms
Variables   :
|           MDC_DEVICE_FAMILY = Snom Phone
Sess-Timers : Accept
Sess-Refresh : uas
Sess-Expires : 1800 secs
Min-Sess     : 90 secs
```

10.1.1.11^34862^sip:rky5BZu588400c2
@192.168.100.115:34862;transport=Tls

**Solution: "sip path workaround": Extend
Contact Header**



LXC



docker

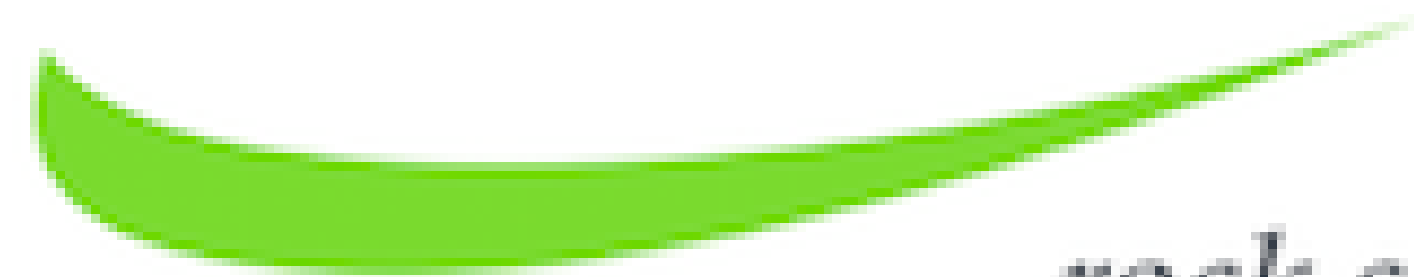


LXC instead of Docker

EXPERIENCES



KAMAILIO



*rock solid SIP server
excellence in SIP since 2001*

We really love kamailio!
Reliable and flexible.



Endpoints + Security = pain

- ▶ Frame 2: 682 bytes on wire (5456 bits), 682 bytes captured
- ▶ Ethernet II, Src: Xensourc_8f:dc:ff (00:16:3e:8f:dc:ff), D:
- ▶ Internet Protocol Version 4, Src: 10.0.3.103, Dst: 10.0.3.
- ▶ User Datagram Protocol, Src Port: 5060, Dst Port: 5060
- ▼ Data (640 bytes)
 - Data: 00000000000000000005349502f322e3020323030204f4b0d0a.
 - [Length: 640]

```

SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.0.3.132:5060;received=10.0.3.132;branch=z9
Max-Forwards: 69
From: "asterisk" <sip:asterisk@twebers>;tag=as5438739d
To: <sip:LxYf6yz2982B155@192.168.88.80:51215;transport=TCP;lin
Call-ID: 1cdf536430fe28cd11b215474fb44185@twebers
CSeq: 102 OPTIONS
Accept: application/sdp
Accept-Encoding: identity
Accept-Language:
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NO
Date: Wed, 26 Apr 2017 12:21:38 GMT
Supported: replaces, timer
User-Agent: snomM700/03.55.0021 (MAC=00041361031F; SER= 00000;
Content-Length: 0

```

95	16:30:09.561589	192.168.88.5	192.168.88.80	TCP	54	5061 → 51215 [ACK] Seq=3781 Ack=
104	16:30:41.352867	192.168.88.80	192.168.88.5	SSL	60	Continuation Data
105	16:30:41.352961	192.168.88.5	192.168.88.80	TCP	54	5061 → 51215 [ACK] Seq=3781 Ack=

Unnecessary keepalive packets via TCP
confuses kamailio

Provisioning URL

← Home	← Abbrechen	Filter: <input type="text"/>			
Bezeichnung ▲	MAC ▼	URL ▼	Proxy ▼	SIP Modus ▼	RTP Media Modus ▼
Yealink 00156585b629 [Jan Lorenz]	00156585b629	https://10.5.6.101:8884/p/Nhvfgzs_ZVpd_TjqmwVG-dqgTKtAQVDj4-rR7ZGRIXaCeryNzpewYmlfy28Bm6S-+	proxy	tls	srtp
Yealink 001565b7ae7b [Jan Lorenz]	001565b7ae7b	https://10.5.6.101:8884/p/Dc9Q_KOak7r2yRpD_p1zS5Ixq9qs1Qtn9zCVFNJy1C5eYDARKnjrGbpSZEdkcIXp+	proxy	tls	srtp

Secure provisioning of endpoints via internet
is HARD

FUTURE

```
route[PNPSUBSCRIBE] {
    # did we receive a subscribe on the pnp broadcast ip?
    if (is_method("SUBSCRIBE") && $Ri = "224.0.1.75" ) {
        xlog("L_NOTICE", "***** PNP SUBSCRIBE : [$ci] $si: $rm $fu => $ru ($ct)\n");
        $uac_req(method)="NOTIFY";
        pv_printf("$uac_req(ruri)", "sip:$sel(contact.uri.host):$sel(contact.uri.port)");
        $uac_req(furi)="sip:192.168.88.10";
        $uac_req(turi)="sip:192.168.88.10";
        $uac_req(hdrs)="Event: ua-profile\r\nContent-Type: application/url\r\n";
        $uac_req(body)="https://192.168.88.10:8884/p/twebers/000413740052";
        $uac_req(sock)="udp:192.168.88.10:5060";
        uac_req_send();
        t_release();
        exit;
    }
}
```

SIP-based Provisioning via kamailio

```
root@cloudstack:/persistent/home/admin# cs container info proxy -c
{
  "cpu": "241158835148",
  "image": {
    "name": "cs-proxy",
    "version": "7.15.00.D98_6951ebe"
  },
  "ips": [
    "10.0.3.112"
  ],
  "mem_limit": "268435456",
  "mem_used": "202604544",
  "memory": "256M",
  "memsw_limit": "335544320",
  "memsw_used": "202604544",
  "name": "proxy"
}
```

Reconfigure kamailio on-the-fly

Q&A