cloudflare / **cfssl**

Unable to create a root and intermediate CA #652

New issue

Closed **bkleef** opened this issue on Jul 30, 2016 · 7 comments

bkleef commented on Jul 30, 2016 • edited

Based on #495 and cfssl pathlen weirdness I'm trying to generate a root and intermediate CA. But I keep getting `[ERROR] local signer policy disallows issuing CA certificate` .

Installed `cfssl` by `go install github.com/cloudflare/cfssl/cmd/...` on OS X 10.11.6.

```
$ cfssl version
Version: 1.2.0
Revision: dev
Runtime: go1.6
```

Root CA

`root.json`

```
{
  "CN": "Root CA",
  "key": {
    "algo": "ecdsa",
    "size": 256
  },
  "ca": {
    "expiry": "262800h",
    "pathlen": 1
  },
  "names": [
    {
      "C": "US",
      "L": "San Francisco",
      "O": "CloudFlare",
      "OU": "Systems Engineering",
      "ST": "California"
    }
  ]
}
```

Intermediate CA

`intermediate.json`

```
{
  "CN": "Intermediate CA",
  "key": {
    "algo": "ecdsa",
    "size": 256
  },
  "ca": {
    "expiry": "262800h",
    "pathlen": 0
  },
  "names": [
    {
      "C": "US",
      "L": "San Francisco",
      "O": "CloudFlare",
      "OU": "Systems Engineering",
      "ST": "California"
    }
  ]
}
```

`config.json`

```
{
 "signing": {
   "default": {
     "usages": [
```

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Notifications

3 participants

```
       "signing",
       "key encipherment",
       "cert sign",
       "crl sign"
      ],
      "expiry": "262800h",
      "is_ca": true
    }
  }
}
```

Makefile

```
all:
    @rm -f ${PWD}/*.csr ${PWD}/*.pem
    cfssl genkey -initca root.json | cfssljson -bare root
    cfssl genkey -initca intermediate.json | cfssljson -bare intermediate
    cfssl sign -ca root.pem -ca-key root-key.pem -config conf.json intermediate.csr | cfssljson -
bare intermediate
```

Log

```
cfssl genkey -initca root.json | cfssljson -bare root
2016/07/30 14:25:05 [INFO] generate received request
2016/07/30 14:25:05 [INFO] received CSR
2016/07/30 14:25:05 [INFO] generating key: ecdsa-256
2016/07/30 14:25:05 [INFO] encoded CSR
2016/07/30 14:25:05 [INFO] signed certificate with serial number
474445957227319139441336640032570256760063350933



cfssl genkey -initca intermediate.json | cfssljson -bare intermediate
2016/07/30 14:25:05 [INFO] generate received request
2016/07/30 14:25:05 [INFO] received CSR
2016/07/30 14:25:05 [INFO] generating key: ecdsa-256
2016/07/30 14:25:05 [INFO] encoded CSR
2016/07/30 14:25:05 [INFO] signed certificate with serial number
618419651942864058216069967767298711443572670314



cfssl sign -ca root.pem -ca-key root-key.pem -config conf.json intermediate.csr | cfssljson -bare
intermediate
2016/07/30 14:25:05 [ERROR] local signer policy disallows issuing CA certificate
{"code":5300,"message":"Policy violation request"}
Failed to parse input: unexpected end of JSON input
make: *** [all] Error 1
```

bkleef commented on Jul 30, 2016

I can confirm that above config works on 1.2.0 branch.

lziest commented on Jul 30, 2016 Contributor

We update the control on signing conf here:
https://github.com/cloudflare/cfssl/blob/master/doc/cmd/cfssl.txt#L121

Since the update "is_ca" is deprecated and replaced by "ca_constraint", and json parser will simply ignore "is_ca" and populate "ca_constraint" with default zero value. So you see the error message.

So you need
`"ca_constraint": {"is_ca": true, "max_path_len":0, "max_path_len_zero": true}` in the place of `"is_ca": true`

The intention is let signer have control on whether to sign a CA csr with given pathlen constraint.

👍 11

lziest commented on Jul 30, 2016 Contributor

Assume this is resolved, feel free to reopen.

lziest closed this on Jul 30, 2016

andrewmgee commented on Aug 18, 2016

I'm receiving the same error on Ubuntu 16.04 LTS. I've modified my intermediate config json file with the ca_constraint.

Version: 1.2.0
Revision: dev
Runtime: go1.6.2

lziest commented on Aug 19, 2016 Contributor

please show the signing.json,

andrewmgee commented on Aug 19, 2016

you mean the config json?

intermediate config json

```
{
    "signing": {
        "default": {
            "expiry": 43800h"
        },
        "profiles": {
            "intermediate": {
                    "usages": [
                        "signing",
                        "key encipherment",
                        "cert sign",
                        "crl sign"
                    ],
                    "expiry": "43800h",
                    "ca_constraint": {
                    "is_ca": true,
                    "max_path_len": 0,
                    "max_path_len_zero": true
                }
                }
        }
    }
}
```

lziest commented on Aug 19, 2016 Contributor

I assume you didn't specify "-profile intermediate" in the cli parameters. By default, it is using "default" policy, which only has "expiry". Anyway, feel free to open a new issue. We don't want to spam others.

andrewmgee referenced this issue on Aug 19, 2016

policy violation error when creating intermediate CA with profile intermediate #657 Open

willp-bl added a commit to alphagov/verify-local-startup that referenced this issue on Jan 15

```
bau: fix newer versions of cfssl  …                                          afce5d6
```

willp-bl referenced this issue on Jan 15

bau: fix newer versions of cfssl #15 Merged