CentOS Dojo / May 2021

New authentication platform for CentOS and SIGs

Fabian Arrotin

arrfab@centos.org, @arrfab

/whois arrfab

['ops','infra','floor sweeper'] @ centos.org

Agenda

New authentication platform for CentOS and SIGs

- Why we had to migrate
- How we migrated (and what)
- Benefits for CentOS and Fedora

Why we had to migrate

- Fedora and CentOS both using FAS (https://github.com/fedora-infra/fas)

Why we had to migrate

- Fedora and CentOS both using FAS (https://github.com/fedora-infra/fas)
- python2 / TurboGears

Why we had to migrate

- Fedora and CentOS both using FAS (https://github.com/fedora-infra/fas)
- python2 / TurboGears
- ~ 2008

Why we had to migrate

- Fedora and CentOS both using FAS (https://github.com/fedora-infra/fas)
- python2 / TurboGears
- ~ 2008
- RHEL6/CentOS 6 EOL too

Why we had to migrate

- Fedora and CentOS both using FAS (https://github.com/fedora-infra/fas)
- python2 / TurboGears
- ~ 2008

- RHEL6/CentOS 6 EOL too

- had to .. die :)

Why we had to migrate

"Political" options

- options:
  - CentOS and Fedora still using their own auth system

Why we had to migrate

"Political" options

- options:
  - CentOS and Fedora still using their own auth system
  - or merge once for all (SSO for both projects)

Why we had to migrate

"Technical" options

- FAS3
  - Still "invented here syndrom"
  - Still a need for a custom IdP for openid/openidc/saml
  - Still a dep on ... (Free)IPA for kerberos

Why we had to migrate

"Technical" options

- AWS Cognito
  - Vendor Lock-In !
  - not all standards (think about koji: TLS and Kerberos)
  - Community engagement

Why we had to migrate

"Technical" options

- (Free)IPA
  - (already there for FAS)
  - In House (part of RHEL)
  - lack of community portal (but something already started)

Solution : CentOS and Fedora on same bicycle !

Community Portal

Noggin

upstream project: https://github.com/fedora-infra/noggin

used for:

- https://accounts.centos.org
- https://accounts.fedoraproject.org

API endpoint

FasJson

upstream project: https://github.com/fedora-infra/fasjson

API endpoint: https://fasjson.fedoraproject.org/

API doc: https://fasjson.fedoraproject.org/docs/v1/

- needs kerberos auth (passthrough/proxy to IPA backend)

How we migrated

What was migrated :

- user account[s] (nick, full name, email address, etc)
- groups
- group[s] membership

How we migrated

What was *not* migrated :

How we migrated

What was *not* migrated :

- passwords
- inactive accounts
  - people asked for it
  - admins disabled (spam)

How we migrated

fas2ipa

- https://github.com/fedora-infra/fas2ipa
- existing fedora users => kept and group changes
- new users:
  - conflict[s] : ask for changes
  - no conflict[s] => imported users (reset pass)

How we migrated

Some stats

- ~75k users
- ~1200 groups
- 3 dedicated IPA servers (RHEL8)

CentOS SIG users

TLS cert (centos-cert)

Supported Linux distributions: CentOS 8/8-s , Fedora 32,33,34

```
sudo dnf install -y epel-release # only if your on CentOS 8 / 8-stream
sudo dnf install -y centos-packager
```

CentOS SIG users

TLS cert (centos-cert)

```
You need to call the script like this : /usr/bin/centos-cert -arguments
 -u : username ([REQUIRED] : your existing ACO/FAS username)
 -v : just validates the existing TLS certificate ([OPTIONAL])
 -r : REALM to use for kerberos ([OPTIONAL] : defaults to FEDORAPROJECT.ORG)
 -f : fasjson url ([OPTIONAL]: defaults to https://fasjson.fedoraproject.org)
 -h : display this help
```

2FA

through portal, for web authentication

Easy: just enable it through portal, and you can add multiple devices/token (OTP)

Known to work:

- Yubikey (4 and beyond), through rpm pkg "yubioath-desktop" (available through Fedora or Copr for CentOS 8/8-stream)
- FreeOTP (Android devices)
- OTPClient (Flatpak)
- others ... (?)

2FA

Warning !

Once enabled there is no way to come back to previous auth (except through admin request) Be sure to have backup solution ! (also gpg key id through your profile)

2FA, fun with kinit/kerberos

Aka "why doesn't kinit work by default"

```
kinit: Pre-authentication failed: Invalid argument while getting initial credenti
```

2FA, fun with kinit/kerberos

Aka "why doesn't kinit work by default"

```
sudo dnf install fedora-packager
kinit -n @FEDORAPROJECT.ORG -c FILE:armor.ccache
kinit -T FILE:armor.ccache <username>@FEDORAPROJECT.ORG
```

At this stage, it asks a combination of password + OTP token

Kerberos pass-through for browsers

- Firefox:

```
about:config
network.negotiate-auth.trusted-uris: .fedoraproject.org,.centos.org
```

- Chrome : /etc/opt/chrome/policies/managed/fedora-centos.json
- Chromium : /etc/chromium/policies/managed/fedora-centos.json

```
{
  "AuthServerWhitelist": "*.fedoraproject.org,*.centos.org",
  "AuthNegotiateDelegateWhitelist": "*.fedoraproject.org,*.centos.org"
}
```

Kerberos pass-through for browsers

Warning, needs fedora-packager >= 0.6.0.5-2

```
cat /etc/krb5.conf.d/fedoraproject_org
[realms]
 FEDORAPROJECT.ORG = {
        kdc = https://id.fedoraproject.org/KdcProxy
        pkinit_anchors = FILE:/etc/pki/ipa/fedoraproject_ipa_ca.crt
 }
[domain_realm]
 .fedoraproject.org = FEDORAPROJECT.ORG
 fedoraproject.org = FEDORAPROJECT.ORG
 .centos.org = FEDORAPROJECT.ORG
 centos.org = FEDORAPROJECT.ORG
```

Q&A