Discuss your identity
How FreeIPA helps running CentOS community infrastructure

Alexander Bokovoy
Sr. Principal Software Engineer // Red Hat
FreeIPA pillars

Identity
- SSSD
- MIT Kerberos

Authentication
- SSSD
- 389-ds LDAP server

Access control
- SSSD
- 389-ds LDAP server

Dogtag PKI

FreeIPA installation and management framework
## CentOS ecosystem usage of FreeIPA

<table>
<thead>
<tr>
<th>Fedora Backend</th>
<th>CentOS IdP</th>
<th>Rocky Linux Backend</th>
<th>Alma Linux Backend</th>
</tr>
</thead>
<tbody>
<tr>
<td>FreeIPA</td>
<td>FreeIPA</td>
<td>FreeIPA</td>
<td>FreeIPA</td>
</tr>
<tr>
<td>Ipsilon</td>
<td>Ipsilon</td>
<td>Ipsilon</td>
<td>Keycloak</td>
</tr>
<tr>
<td>Noggin</td>
<td>Noggin</td>
<td>Noggin</td>
<td>Noggin</td>
</tr>
</tbody>
</table>

### Red Hat Enterprise Linux (Red Hat infrastructure)

- Dustin Minnich talk at FOSDEM 2018
  - Migrating to Red Hat IdM in a large Linux Environment

[Email: abbra@fedoraproject.org]
## FreeIPA features in use

### Fedora
- Replicated IPA servers
  - Automated backup
- User and group mgmt
  - TOTP/HOTP
  - SSH keys
- Custom roles and permissions
- Hosts:
  - HBAC
  - SUDO
- Services
  - **Constrained delegation**
  - Kerberos auth
- Certificate management

### CentOS
- Shared with Fedora:
  - Replicated IPA servers
  - Automated backup
  - User and group mgmt
  - TOTP/HOTP
  - SSH keys
  - Hosts:
    - HBAC
    - SUDO
  - Services
  - Constrained delegation (fasjson and noggin)
  - Certificate management and authentication

### Rocky Linux
- Replicated IPA servers
- User and group mgmt
  - TOTP/HOTP
  - SSH keys
- Custom roles and permissions
- Hosts:
  - HBAC
  - SUDO
- Services
  - Constrained delegation (fasjson and noggin)
- Certificate management
- ansible-freeipa

### Alma Linux
- Replicated IPA servers
- User and group mgmt
  - TOTP/HOTP
  - SSH keys
- Custom roles and permissions
- Hosts:
  - HBAC
  - SUDO
- Services
  - Constrained delegation (fasjson and noggin)
- Certificate management
CentOS ecosystem usage of FreeIPA

### Fedora
- Backend
  - FreeIPA
- IdP
  - Ipsilon
- Frontend
  - Noggin

### CentOS
- Backend
  - FreeIPA
- IdP
  - Ipsilon
- Frontend
  - Noggin

### Rocky Linux
- Backend
  - FreeIPA
- IdP
  - Ipsilon
- Frontend
  - Noggin

### Alma Linux
- Backend
  - FreeIPA
- IdP
  - Keycloak
- Frontend
  - Noggin

#### User authentication to IdP
- Fedora
  - Kerberos
  - Password
  - Password + OTP token

- CentOS
  - Kerberos
  - Password
  - Password + OTP token

- Rocky Linux
  - Password
  - Password + OTP token
  - Kerberos? *(exposed in IdP but not configured for users)*

- Alma Linux
  - Password
  - Password + OTP token
CentOS ecosystem usage of FreeIPA

Fedora
- FreeIPA
- Ipsilon
- Noggin

CentOS
- FreeIPA
- Ipsilon
- Noggin

Rocky Linux
- FreeIPA
- Ipsilon
- Noggin

Alma Linux
- FreeIPA
- Keycloak
- Noggin

User authentication to services

- Kerberos
- OAuth token
- Certificates
- OAuth token
- Kerberos**

Rocky Linux
- OAuth token*

Alma Linux
- OAuth token*

* using a service-specific IdP, disconnected from the project’s IdP
** CentOS Stream infra uses non-IPA Kerberos realm (Red Hat legacy setup)
Fedora Infrastructure outage in January 2024

Upgrade to RHEL 9
- Migration from RHEL 7
- Datacenter migration
- Migration from RHEL 8
- Collaboration

Technical debt
- “Works: do not touch”
- POSIX ID legacy
- Staged users and sidgen
- Legacy Kerberos services

https://pagure.io/fedora-infrastructure/issue/11740
FreeIPA less-known or upcoming features (CentOS ecosystem perspective)

● Integration with IdPs
  ○ external IdP authentication in Kerberos
    ■ OAuth 2.0 device authorization grant flow
    ■ RHEL 8.7+/9.1+/Fedora 36+
  ○ FIDO2 authentication in Kerberos
    ■ CentOS Stream/Fedora 39
  ○ coming: SCIMv2 bridge
    ■ native Keycloak provider
    ■ FOSDEM talk on Sunday
  ○ coming: native OAuth2 POSIX identity mapping
    ■ FOSDEM talk on Sunday

● Multi-domain management
  ○ coming: IPA to IPA trust

● Certificate management
  ○ ACME support (in-deployment Let’s Encrypt service to issue certificates)
  ○ coming: HSM support

● Container management integration
  ○ centralized subid management

● Kerberos authentication indicators
  ○ pam_sss_gss for use of Kerberos tickets for PAM services
  ○ Tutorial at FreeIPA Workshop

email: abbra@fedoraproject.org
Feedback about FreeIPA?

abbra@fedoraproject.org
Thank you!