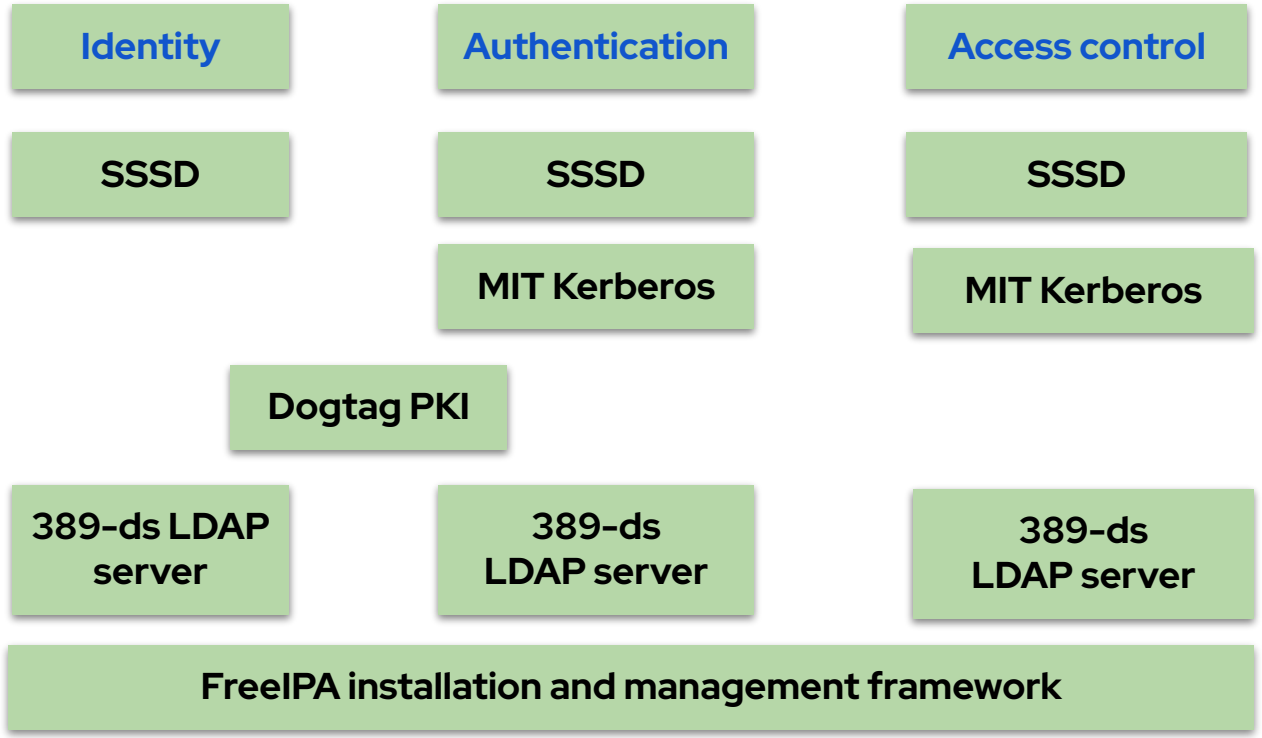
Discuss your identity

How FreeIPA helps running CentOS community infrastructure

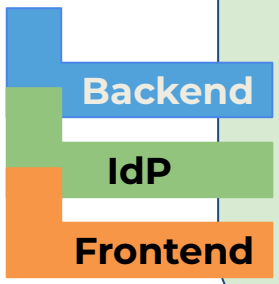
Alexander Bokovoy
Sr. Principal Software Engineer // Red Hat

FreeIPA pillars



abbra@fedoraproject.org

CentOS ecosystem usage of FreeIPA



Fedora	CentOS	Rocky Linux	Alma Linux
FreeIPA	• FreeIPA	• FreeIPA	• FreeIPA
Ipsilon	• Ipsilon	• Ipsilon	• Keycloak
Noggin	• Noggin	• Noggin	• Noggin

Red Hat Enterprise Linux (Red Hat infrastructure)

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

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

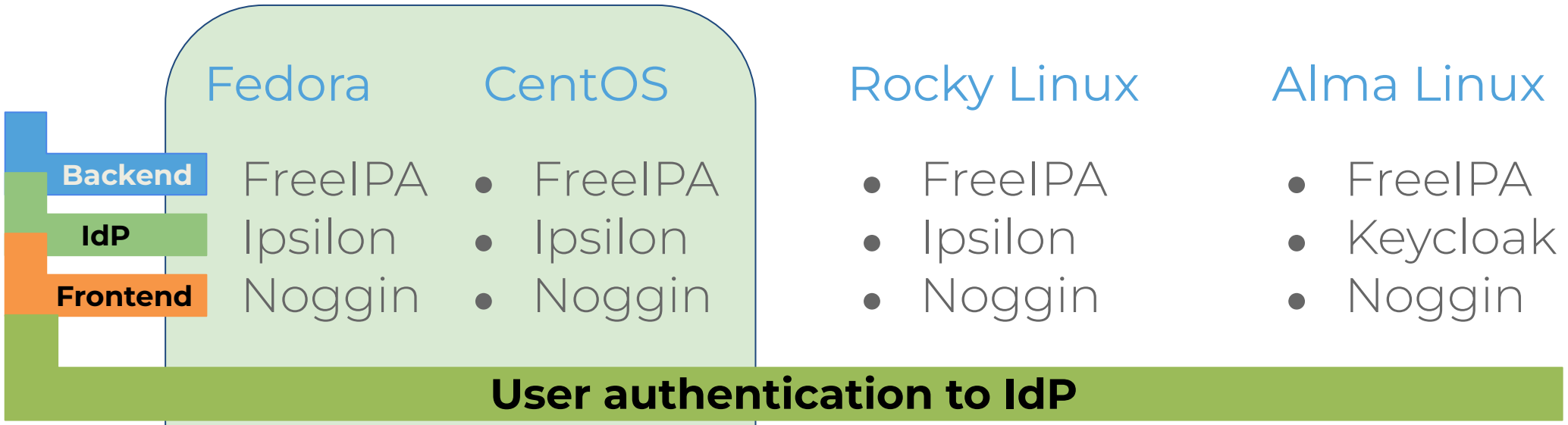
- Replicated IPA servers
- User and group mgmt
  - TOTP/HOTP
  - SSH keys
- Custom roles and permissions
- Hosts:
  - HBAC
  - SUDO
- **Integrated DNS server management**
- Services
  - Constrained delegation (fasjson and noggin)
- Certificate management
- **ansible-freeipa**

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

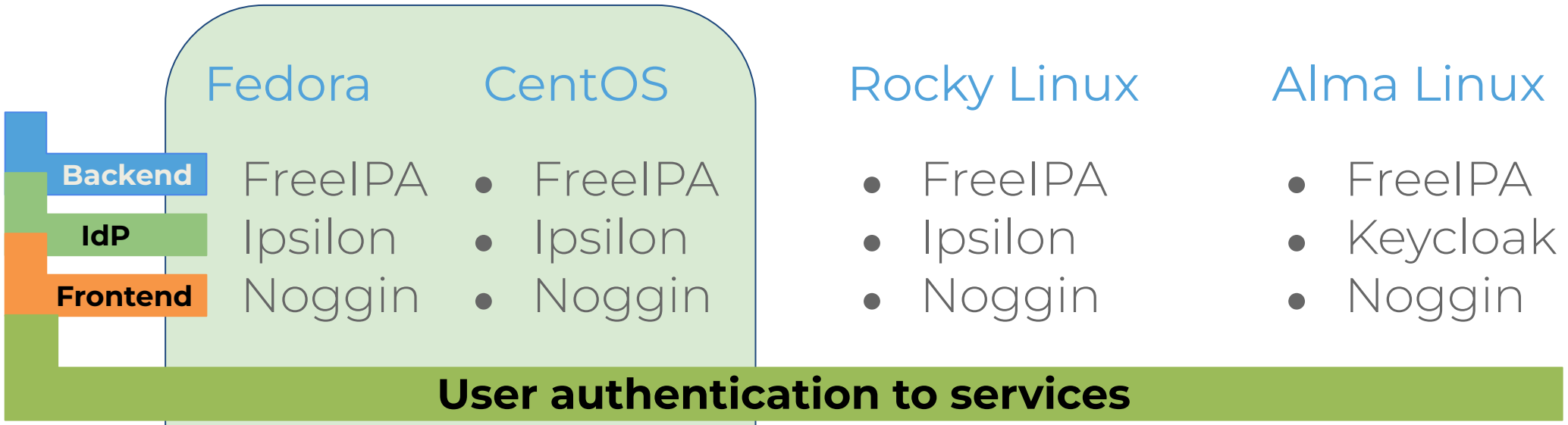
abbra@fedoraproject.org

CentOS ecosystem usage of FreeIPA



abbra@fedoraproject.org

CentOS ecosystem usage of FreeIPA



abbra@fedoraproject.org

* 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

abbra@fedoraproject.org

FreeIPA less-known or upcoming features (CentOS ecosystem perspective)

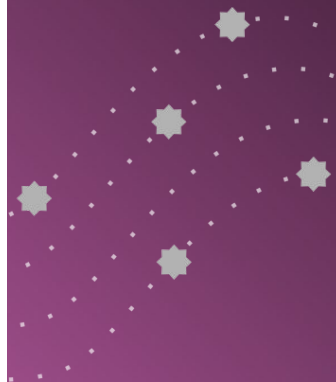
- Integration with IdPs
  - external IdP authentication in Kerberos
    - OAuth 2.0 device authorization grant flow
    - RHEL 8.7+/9.1+/Fedora 36+
  - FIDO2 authentication in Kerberos
    - CentOS Stream/Fedora 39
  - coming: SCIMv2 bridge
    - native Keycloak provider
    - FOSDEM talk on Sunday
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

abbra@fedoraproject.org

Feedback about FreeIPA?

abbra@fedoraproject.org

Thank you!



abbra@fedoraproject.org