

FreeIPA

Open Source identity management

Fraser Tweedale
Software Engineer, Red Hat
2015-01-16

About me

- Developer at Red Hat, Inc.
- Identity management team.
 - Dogtag PKI (certificate authority)
 - FreeIPA
- Blog: <http://blog-ftweedale.rhcloud.com/>
- Twitter: @hackuador

This talk

- Introduction to *identity management*
- Introduction to FreeIPA
 - Features
 - Deployment
- Architecture overview
- Roadmap

Identity Management

Definition

*“**Identity management** (IdM) describes the management of individual **principals**, their **authentication**, **authorization**, and privileges within or across system and enterprise boundaries with the goal of increasing **security** and **productivity** while decreasing cost, downtime and repetitive tasks.”*

Wikipedia

Concerns

- **Identities:** users, services, hosts, groups
- **Authentication:** passwords, 2FA, SSO
- **Authorisation:** identity-related policies
- **Management:** how to manage these concerns in a large organisation (thousands of users/machines)?

Related technologies

- LDAP (directory services)
- Kerberos (authentication)
- X.509 (digital certificates, public key infrastructure)
- DNS
- NFS (Network File System)



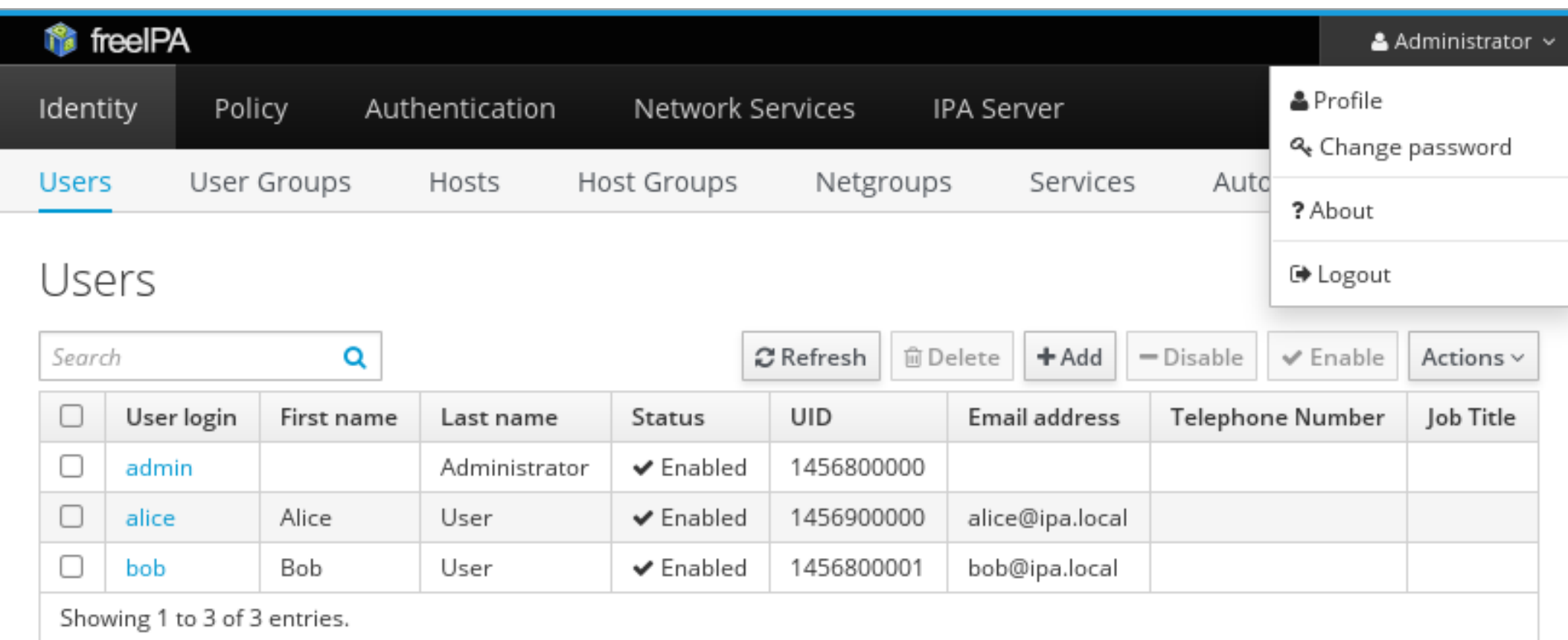
freeIPA

Open Source Identity Management Solution

FreeIPA

- Intity, Policy, Audit
- Centralised identity management suite
- Simple web UI and CLI
 - Hides complexity, user self-service.
- Simple deployment
 - How simple? One command!
- Active Directory integration

FreeIPA – Web UI









freelPA Administrator ▾

Identity Policy Authentication Network Services IPA Server

Users User Groups Hosts Host Groups Netgroups Services Auto

Users

Search 

 Refresh  Delete  Add  Disable  Enable Actions ▾

<input type="checkbox"/>	User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
<input type="checkbox"/>	admin		Administrator	✓ Enabled	1456800000			
<input type="checkbox"/>	alice	Alice	User	✓ Enabled	1456900000	alice@ipa.local		
<input type="checkbox"/>	bob	Bob	User	✓ Enabled	1456800001	bob@ipa.local		

Showing 1 to 3 of 3 entries.


Profile
Change password
About
Logout

Components (server)

- 389 Directory Server
 - Main database for other services
- MIT Kerberos KDC
- Dogtag Certificate System
 - Other external CAs are supported
- Apache httpd
 - Web UI and API
- BIND
 - DNS



Features - authentication

- Password policies
- Kerberos ticket policies
- Kerberos over HTTP (MS-KKDCP)
- One-time password (**OTP**)
 - Native HOTP/TOTP or external via RADIUS proxy
 -  FreeOTP app for Android / iOS
 - **Yubikey**
- **SSH** `authorized_keys` management

Features – users and groups

- Automatic group membership rules
- **Sudo** integration
 - commands, command groups and rules
- **SELinux** user roles
- **Automount**
- Role-based access control (RBAC)

Features – hosts, host groups and netgroups

- One-command host enrolment (`ipa-client-install`)
- Automatic **DNS** record
 - DNSSEC support in FreeIPA 4.1
- Host-based access control (**HBAC**)
- Automatic host group membership rules
- SSH `known_hosts` management

Features – services

- Services are first-class identities
- Kerberos keytab management
- Certificate provisioning via **Certmonger**
 - Automatic renewal

Features – SSSD (client)

- SSSD: System Security Services Daemon
- Connects UNIX client to central identity store(s)
 - Available on most Linux distros + FreeBSD
 - Supports FreeIPA, AD, bare LDAP
- Credential and offline support (replaces nscd, nslcd)
- PAM and NSS modules
- D-Bus API



Features – Active Directory integration

- Cross-realm trust
- Manage users in AD, hosts/services/groups in FreeIPA
- AD users can access resources in FreeIPA domain
 - POSIX attributes: stored in AD or use *views*
- Simple configuration
 - No AD-specific host/service configuration
 - No data synchronisation between domains
 - No additional software needed on AD domain controller

Features – legacy client compatibility tree

- Old systems may not have SSSD with AD support
 - Cannot connect to AD and FreeIPA at same time
- *Compatibility LDAP tree*
 - Managed by *slapi-nis* plugin
 - For FreeIPA user: bind against FreeIPA LDAP tree
 - For AD user: authenticate to AD **via SSSD**

Server deployment

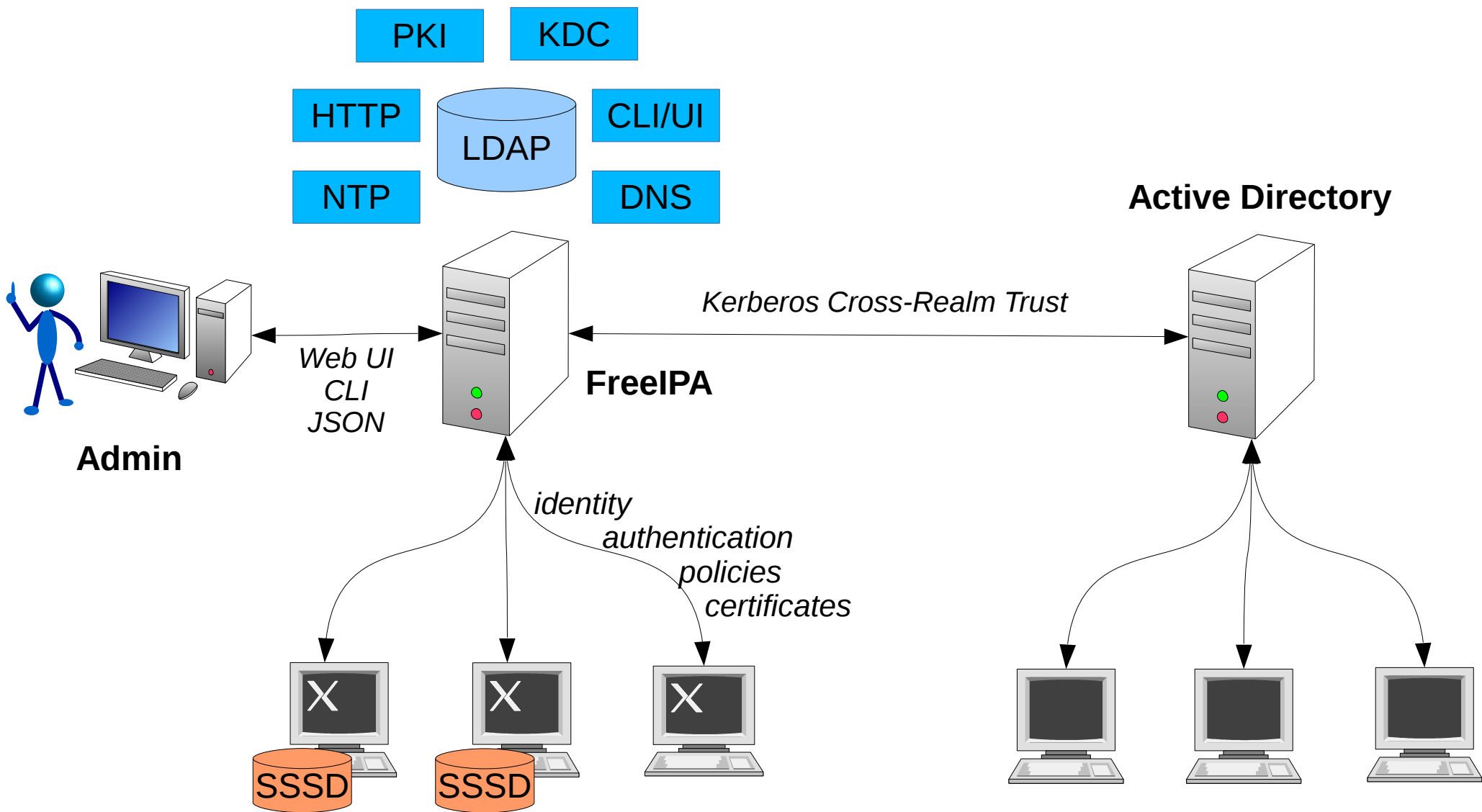
- Supported on Fedora, RHEL, CentOS
 - Available but less supported on Debian, Ubuntu
- One command: `ipa-server-install`
 - Answer some questions, wait a few minutes, done!
- Slightly more work to set up replica

Client enrolment

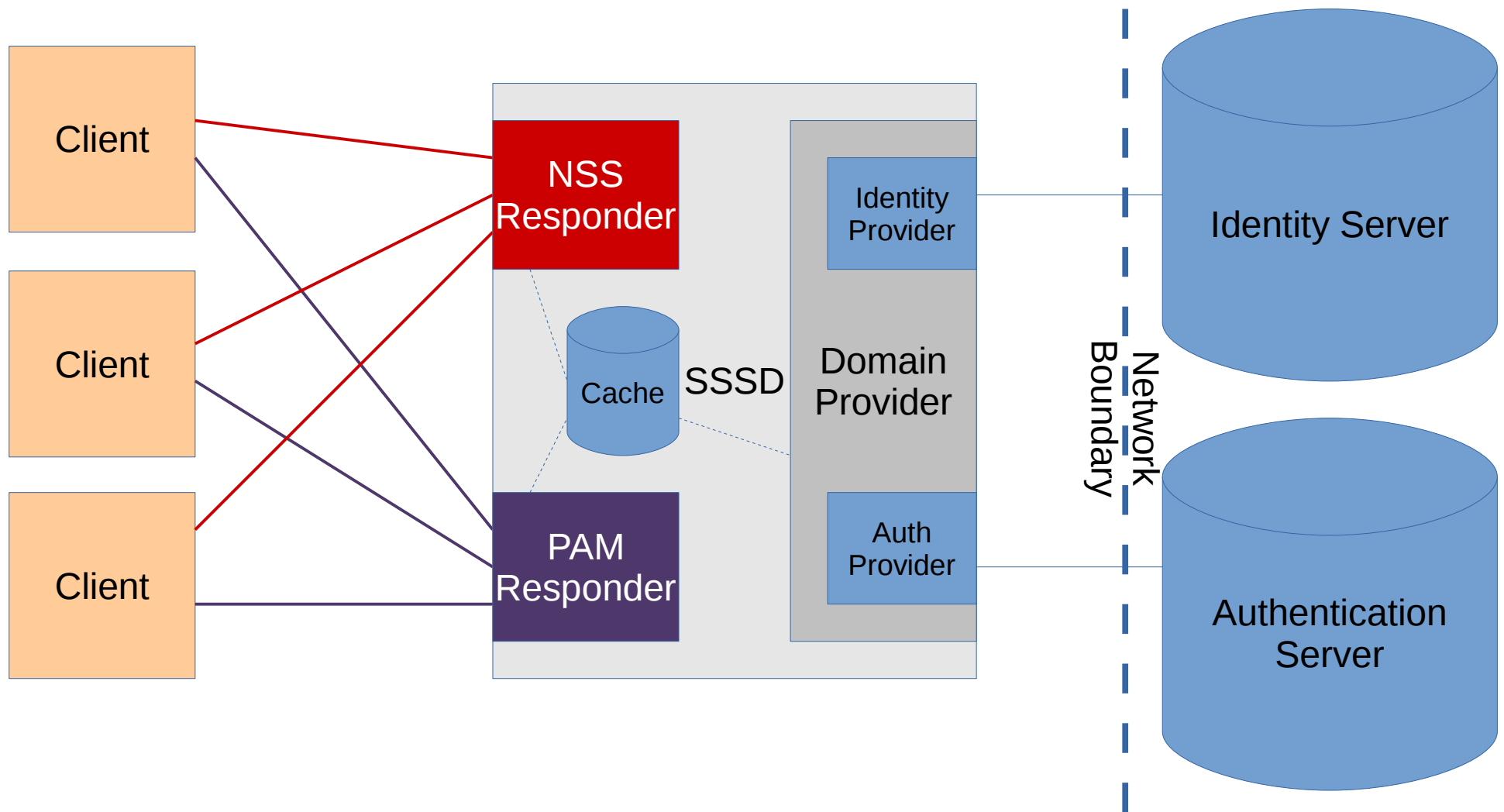
- One command: `ipa-client-install`
 - Answer some questions, wait a few minutes, done!
 - Options for unattended install
 - Configures SSSD and related services.
- Provisioning system integration:
 - Satellite / Spacewalk
 - OpenLMI / realmd
 - Foreman smart proxy

FreeIPA Architecture

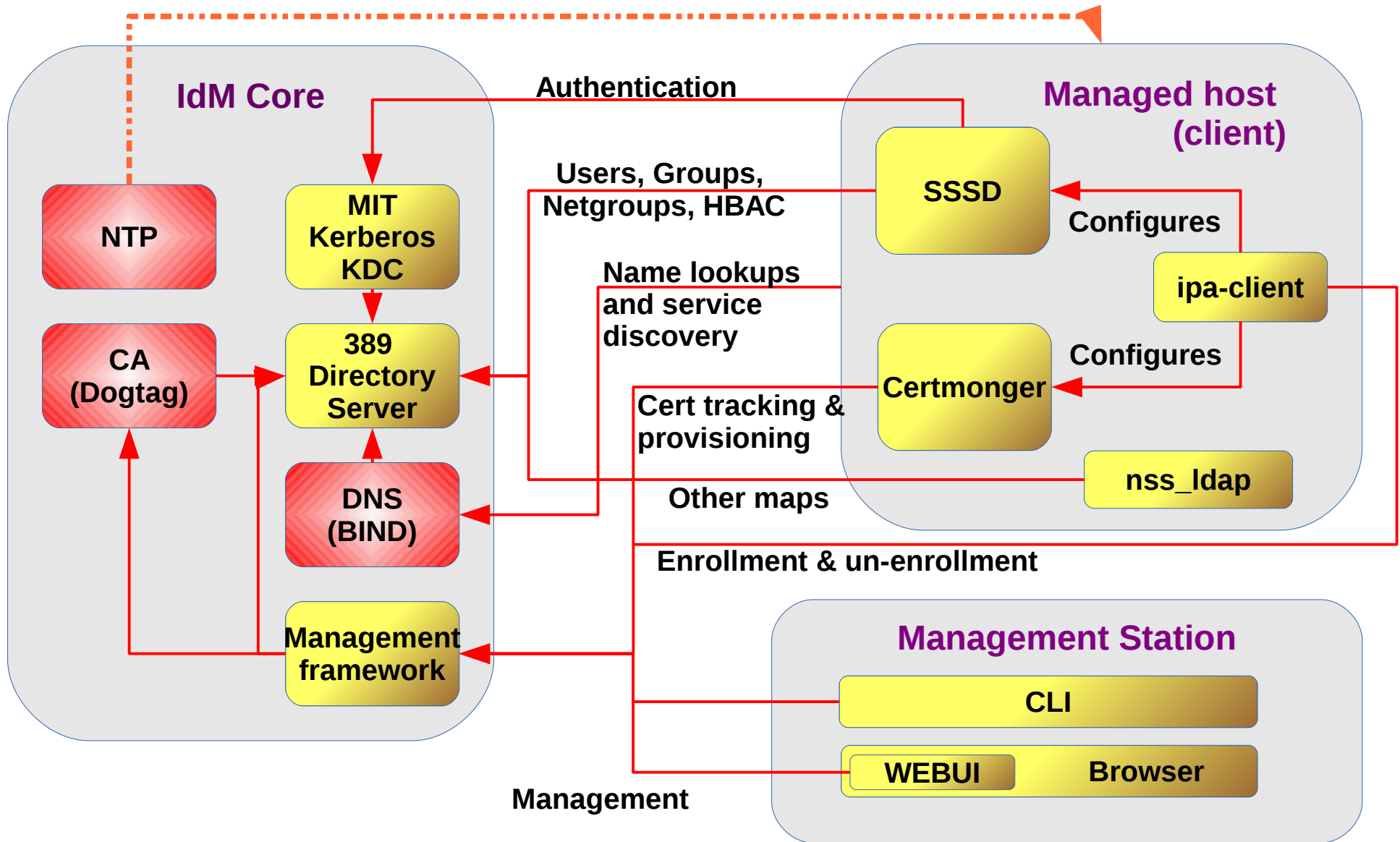
Architecture – high level



Architecture – SSSD



Architecture – detail



Roadmap

Roadmap – short term efforts

- DNSSEC
- CA certificate renewal
- Backup and restore scripts
- Updated web UI
- Improved permissions; fine-grained read access
- Integration with Red Hat Support Portal
- Available in SSSD 1.12.* and FreeIPA 4.1.*
 - Being considered for RHEL 7.1

Roadmap – longer term efforts

- **Enforce stronger authentication** for select services
 - Kerberos CAMMAC / Authentication Indicator
- Kerberos authentication for **mobile** devices
- DNSSEC improvements
- SSSD **Smart Card** login
- Customisable X.509 **certificate profiles**
- **User certificate** provisioning
- *Password Vault*: secure key and secret store
 - FreeIPA front-end to Dogtag *Key Recovery Manager*

Integration efforts

- CloudForms
- **Docker**: SSSD and FreeIPA in containers
- OpenStack (IaaS)
 - Keystone (authorisation)
 - Barbican (secret store)
 - Designate (DNS)
- **OpenShift** Origin (PaaS)
- Calamari (Ceph management platform)
- **<your project>?** Start the conversation!

Adoption

- **GNOME Infrastructure** is now powered by FreeIPA
 - Blog post: <http://is.gd/ISFwSy>
- Other projects or communities with proliferation of identity silos?
 - FreeIPA might help. Let's talk!
- Demo: <http://www.freeipa.org/page/Demo>



Conclusion

- FreeIPA is advanced, *open source*, enterprise IdM
- Ease of deployment and administration
 - Reduce cost of management
- Active Directory integration
 - Avoid duplication; cost-effective IdM infrastructure
- Integrate with FreeIPA
- Adopt FreeIPA?

Resources

- FreeIPA: <http://www.freeipa.org/>
 - http://www.freeipa.org/page/Web_App_Authentication
 - Mailing lists:
 - freeipa-interest@redhat.com (announcements; low traffic)
 - freeipa-users@redhat.com (general help and discussion)
 - freeipa-devel@redhat.com (development discussion and patches)
 - IRC: #freeipa on Freenode
 - Blogs: <http://planet.freeipa.org/>
- SSSD: <https://fedorahosted.org/sss/>
 - Lists: sssd-users@redhat.com ; sssd-devel@redhat.com

Attribution and license

- Architecture diagrams by Dmitri Pal, Martin Kosek
- AD trust diagram © 2012 Red Hat, Inc. (GFDL)
- Copyright 2015 Red Hat, Inc.

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit

<http://creativecommons.org/licenses/by/4.0/>.

Questions?