Identity and Directories with FreeIPA

Simo Sorce
Sr. Principal Sw. Eng., Red Hat
2015/01/21

What is FreeIPA ?

FreeIPA is a Directory and Authentication Server

aka a Domain Controller

Primarily targets at Linux servers.

“IPA” stands for Identity, Policy and Audit

FreeIPA project

The FreeIPA project can be defined as a meta-project.

It integrates existing Open Source components into a cohesive and harmonized solution.

The goal of the FreeIPA project is to provide an easy to use and install but powerful *Identity Management* solution for Linux environments.

Identity Management ?

Identity Management

“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

Identity Management - Basics

Identities

When talking about identities in FreeIPA we think equally of users, hosts and services.

Identity implies concepts such as *naming*, *credentials*, *privileges*, identification is key to establish relations with other objects.

Authentication

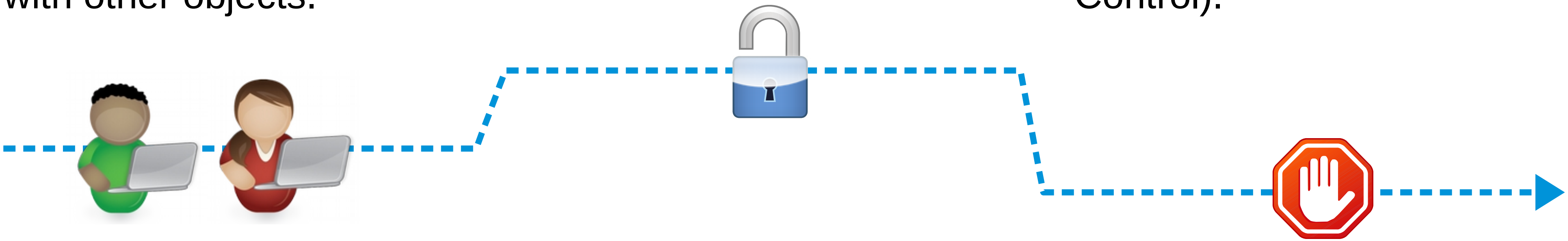
Authentication is the act of identifying one actor to another.

In FreeIPA both users and machines own credentials and can authenticate (to) each other.

Access Control

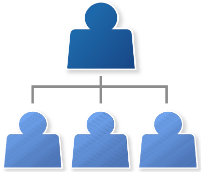
The end goal is to be able to apply access policies and enforce access privileges.

FreeIPA implements a number of standard access controls as well as new ones (like Host Based Access Control).

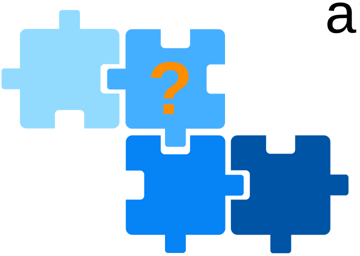


Why should I care for Identity Management ?

Every networked machine needs accounts and authentication services.



From small startups to big enterprises, from cloud deployments to on-premise, every system admin or devop environment faces the problem of managing users, admins, systems, their credentials and keys, and control and coordinate access.



Purpose built Identity Management systems reduce errors, and improve productivity of both admins and users by simplifying management.

Identities and Directories

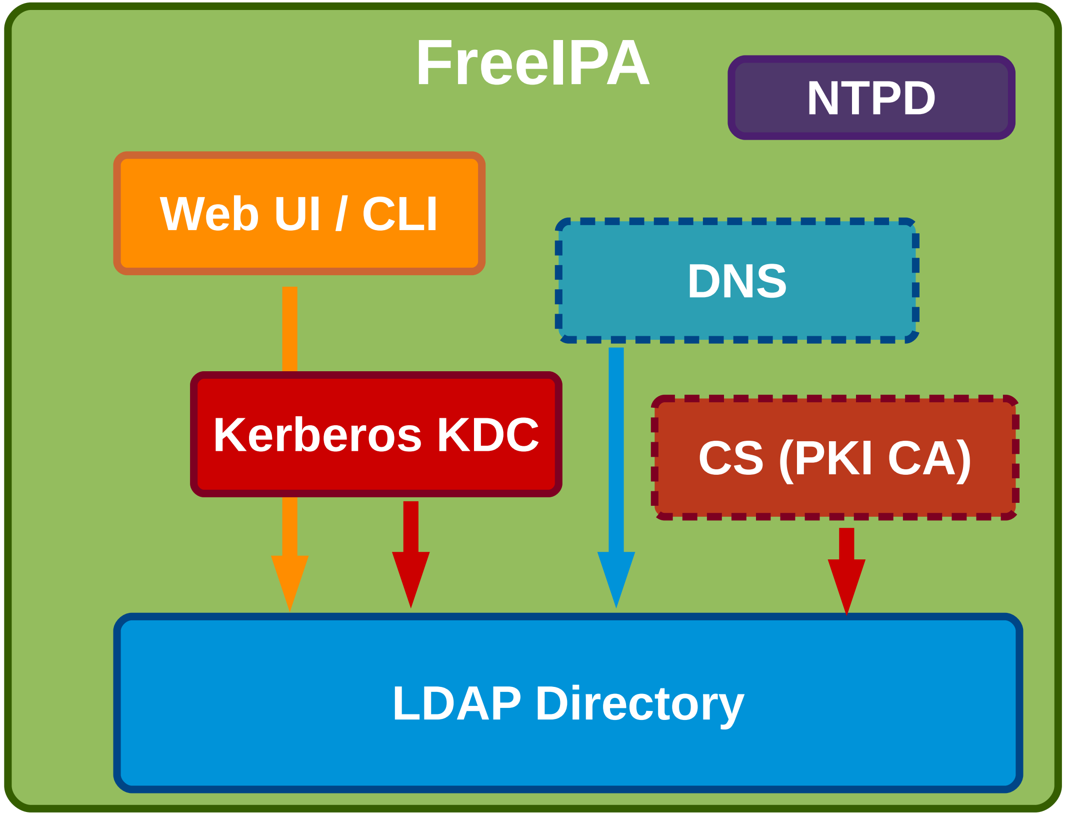
Just a directory ?

A directory is necessary but not sufficient.

A modern system includes dedicated authentication services, policies and a way to manage all these components.

Naming is also important over networks;
if you can't resolve names you can't effectively use modern security and crypto services.

FreeIPA Components



Core:

- 389ds LDAP Server
- MIT Krb5 KDC
- HTTP APIs / Web UI
- Python IPA framework
- NTPD server

Optional:

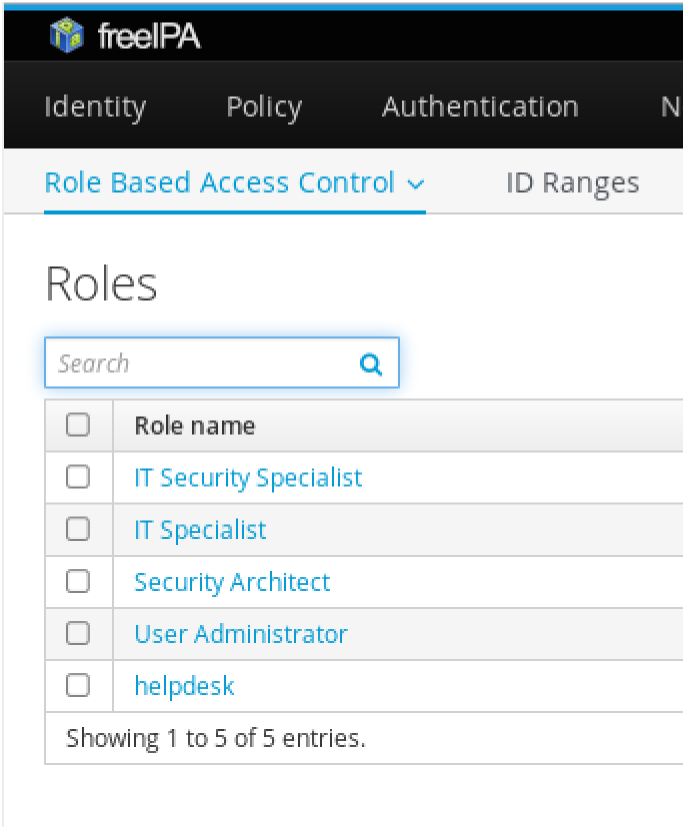
- BIND9 DNS Server
- Dogtag Certificate System

Holistic approach

Not just a bag of parts.

Conceal complexity with consistent management interfaces.

All the functions are available both via a pleasing Web UI and a powerful CLI all based on the same API.



Roles

□	Role name
□	IT Security Specialist
□	IT Specialist
□	Security Architect
□	User Administrator
□	helpdesk

Showing 1 to 5 of 5 entries.

So, what can it do for you ?

Manage identities

Full identity life-cycle management for:

- Users
- Hosts
- Services

Nested user groups

Nested host groups

Private user groups

External users and groups

Auto-membership

Netgroups

Automount maps

User self-service

Policy & Security

Extensive security policy management capabilities:

- Host Based Access Control
- Centralized Sudo Policies
- Groups based password policies

- Two Factor Authentication via Hard or Soft-token (TOTP/HOTP)
- SSH Keys management
  - Both host and user public keys

Role-based, fine-grained delegation of administrative privileges.

Hosts SSL Certificates management including revocation and automatic renewal via integrated CA and client tools

Secure DNS updates (GSS-TSIG)

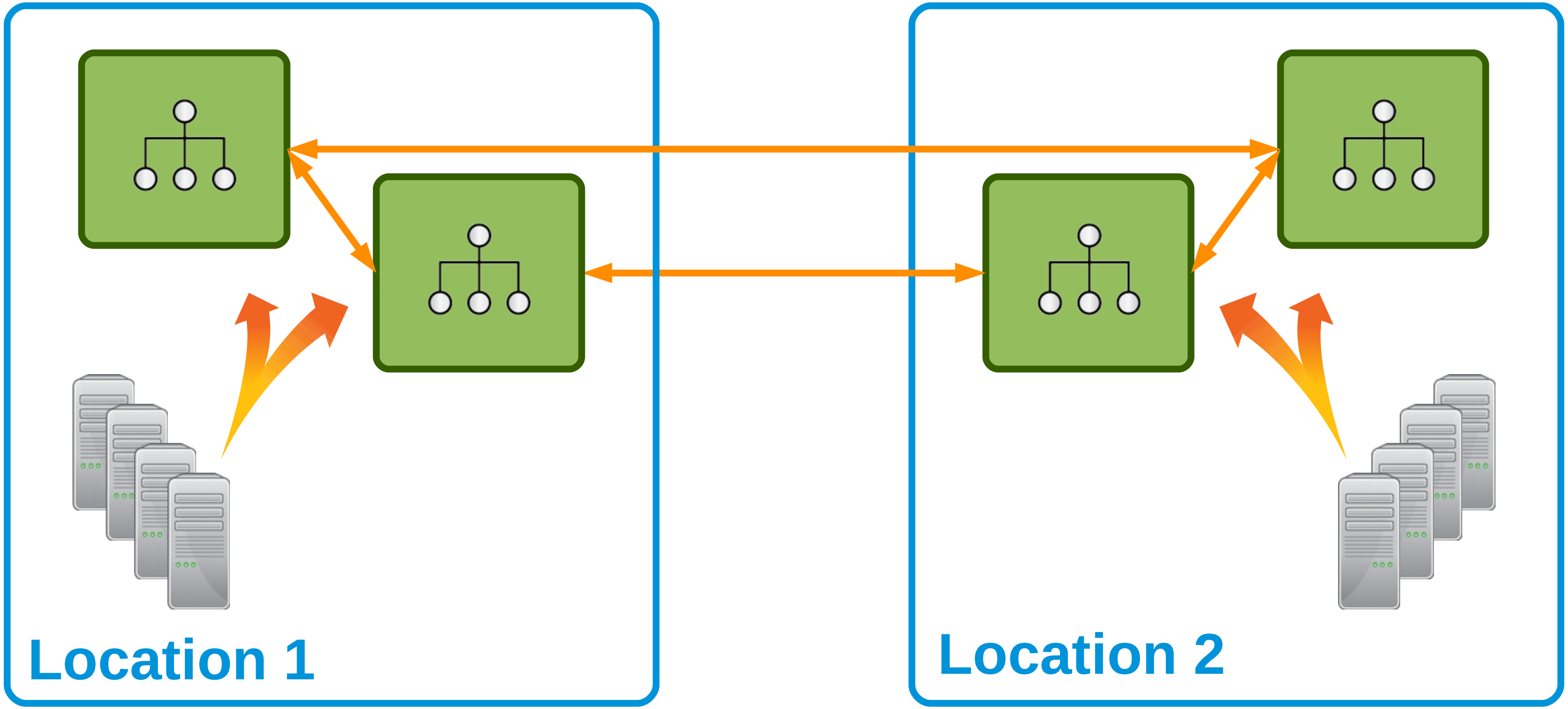
SELinux User Mapping

Simple and powerful setup tools

Install scripts are used to configure both servers and clients

ipa-server-install	first server instance
ipa-replica-install	additional freeipa servers
ipa-client-install	quick client domain join and setup
ipa-advise tool	help admins with configuration advice
ipa tool	command line administrative interface

Scalable



Integration tools

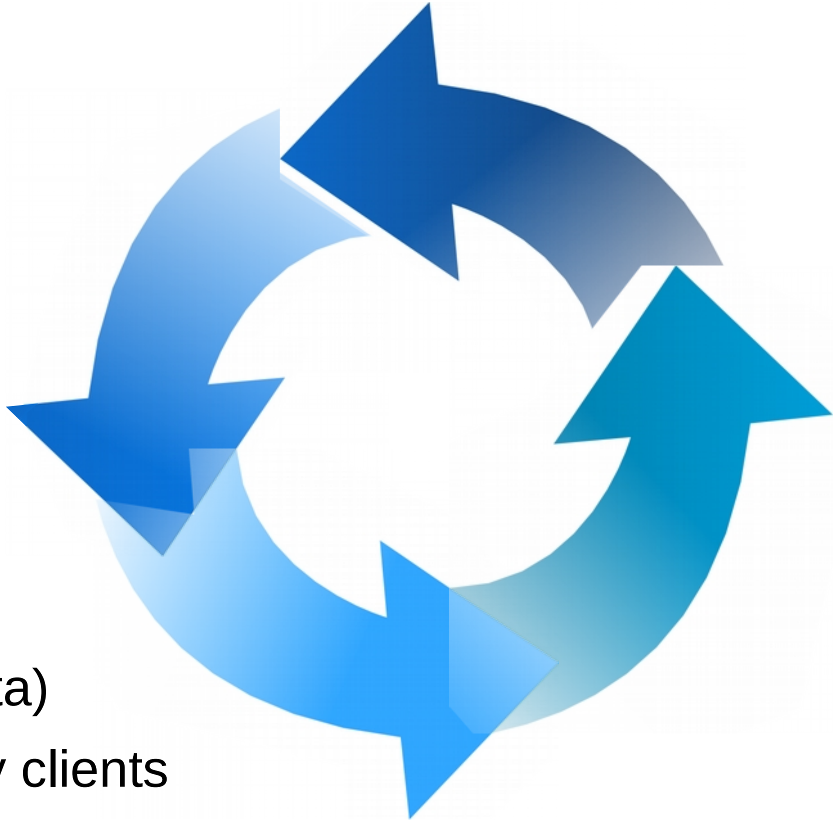
Directory migration

- *ipa migrate-ds* tool
- Including password migration

Legacy clients compatibility:

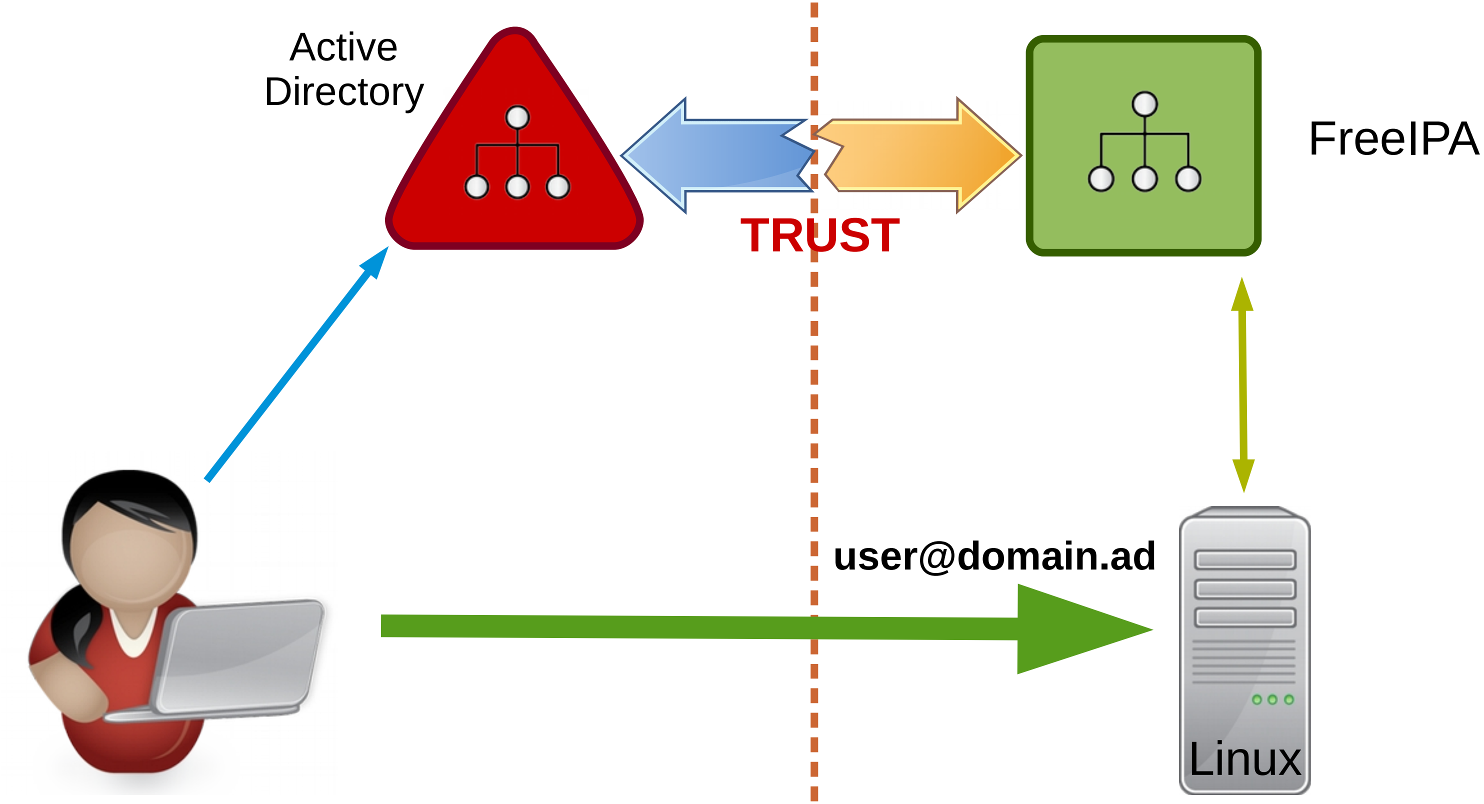
- Internal NIS server (translates from LDAP data)
- LDAP “compat” tree for legacy RFC2307-only clients

Active Directory Integration via cross-forest trust or sync



Trust ?

Active Directory Integration (Trust)



Active Directory Cross-Forest Trust Features

Authentication to FreeIPA clients

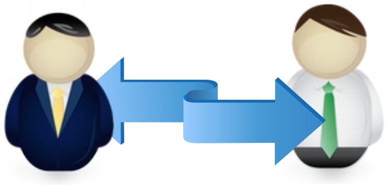
- Password based PAM login
- GSSAPI/Krb5 single sign on to services
  - SSH, HTTP/Negotiate, etc..

External membership in FreeIPA groups

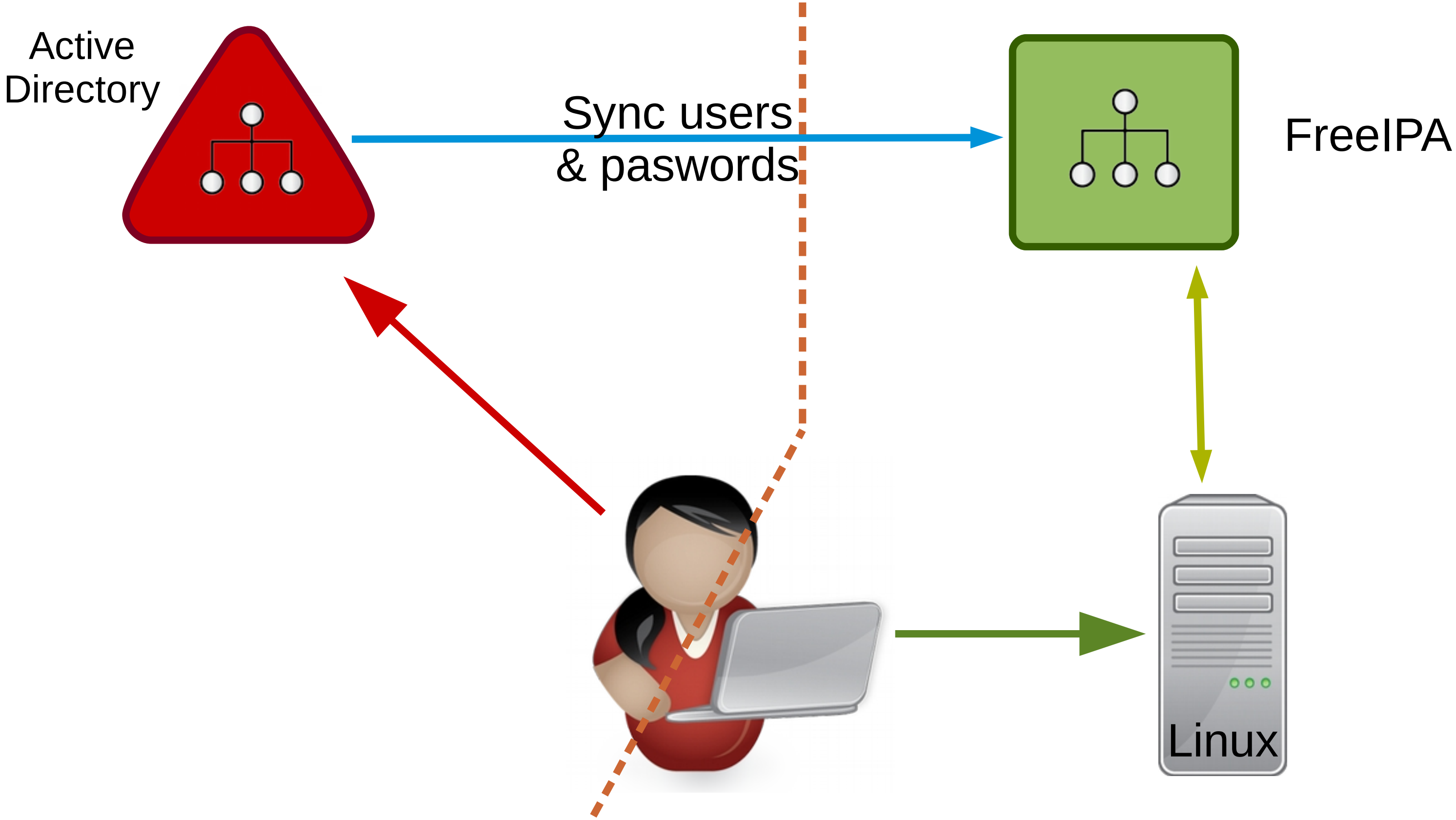
- Including (indirect) membership in posix groups for file and other access control

Multiple Posix ID mapping choices

- Autogenerated IDs
- RFC2307 IDs from AD
- ID Views
  - legacy clients
  - migrations



Active Directory Integration (Sync)



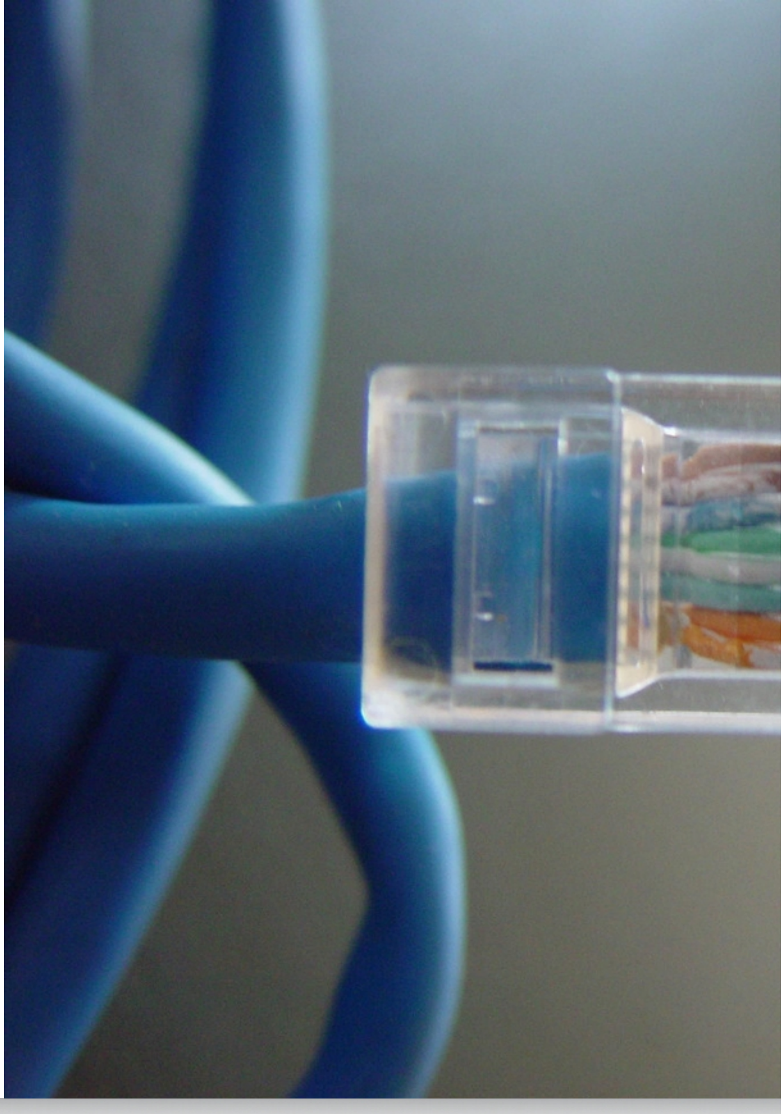
Clients

Clients

The 'official' FreeIPA client is SSSD (System Security Services Daemon).

SSSD replaces legacy clients like pam_ldap/nss_ldap/pam_krb5 (they are also still fully supported as clients, but they do not offer all the advanced features of SSSD).

Certmonger is the client tool used to fetch and automatically renew certificates.



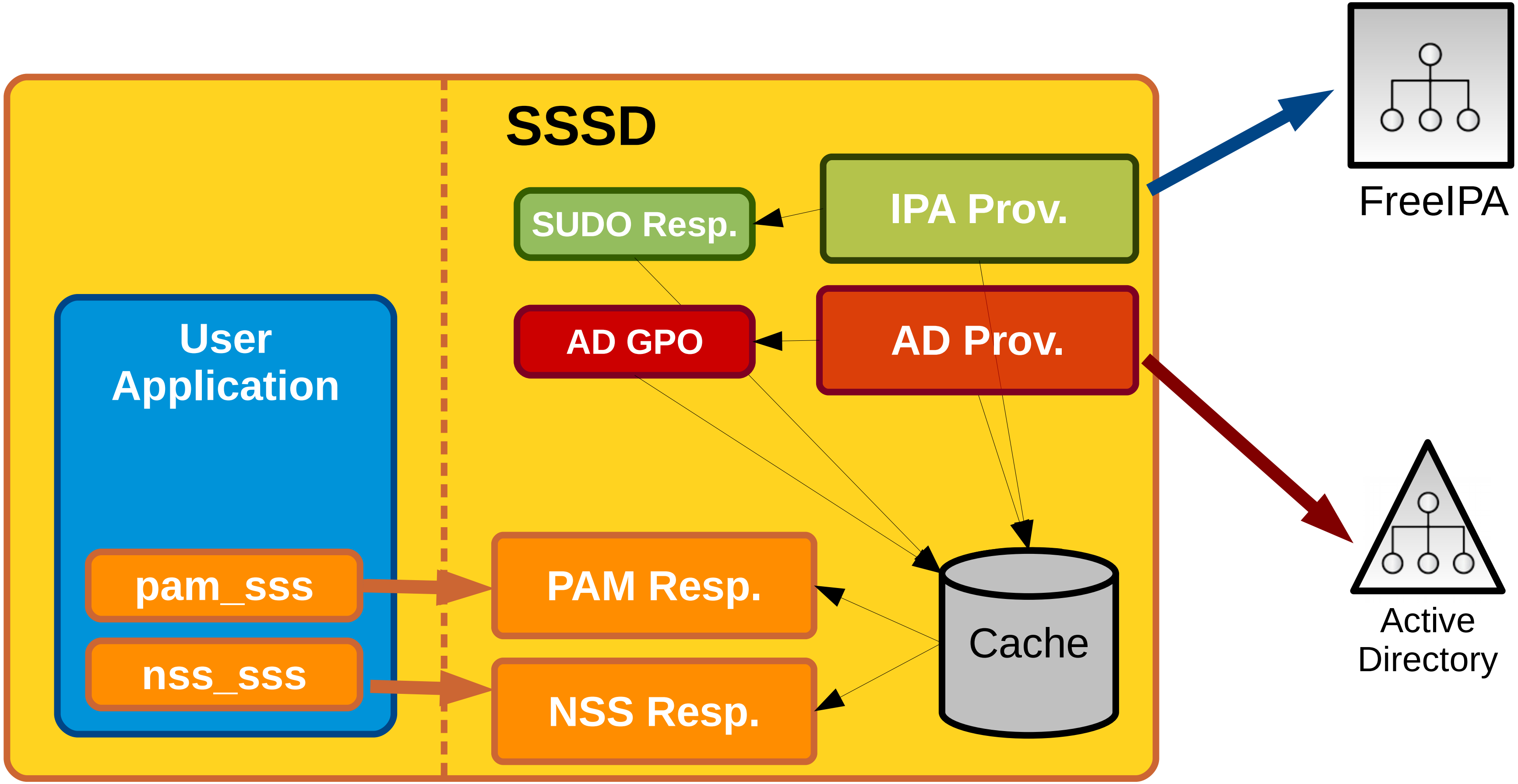
SSSD

SSSD is the recommended client agent for FreeIPA.

But SSSD is more than that, it is a generic agent to connect to identity information and authentication services.

SSSD is in fact a pluggable service that provides connectors for multiple identity systems (even at the same time) and organizes identity information sources into "domains":

- FreeIPA Domains
- Active Directory Domains
- Plain LDAP servers
- ...


SSSD
SUDO Resp.
IPA Prov.
FreeIPA
User Application
AD GPO
AD Prov.
pam_sss
nss_sss
PAM Resp.
NSS Resp.
Cache
Active Directory

Key SSSD Features

Smart caching of identity information

- Automatically refreshed as needed

Offline identity and authentication support via caching:

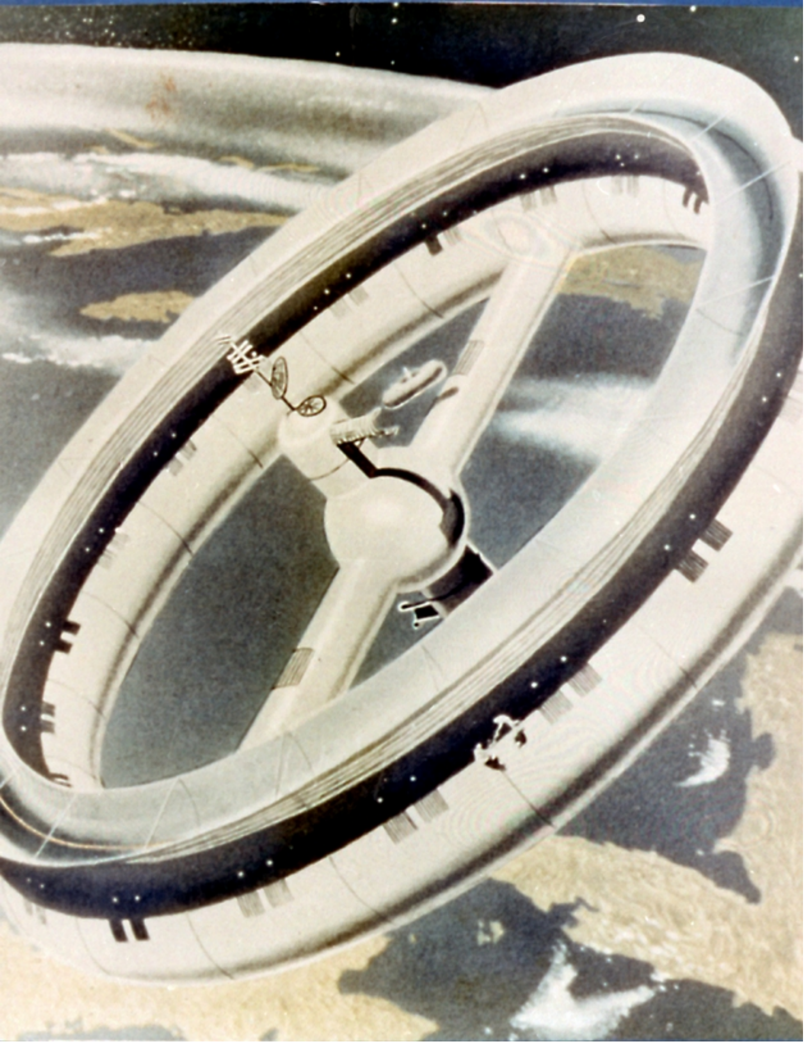
- network interruptions, server maintenance windows, good for laptops

Better client behavior:

- Keeps access credentials private
- Saves load on the servers thanks to caching and connection pooling.

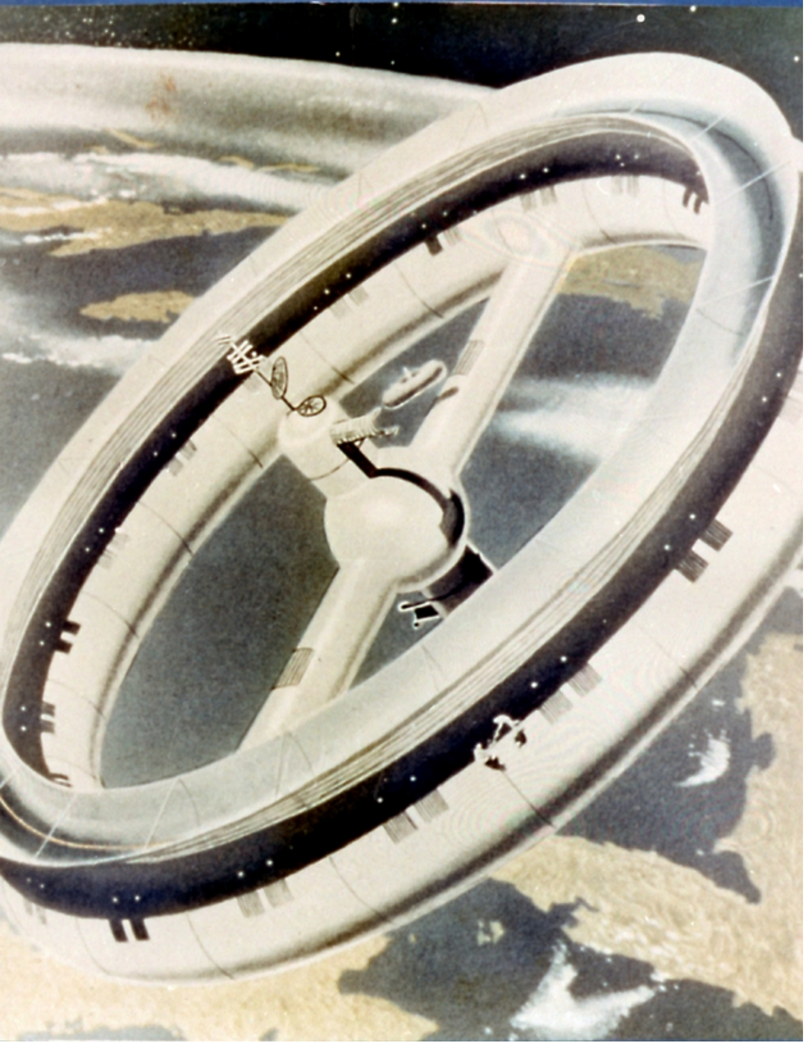
Advanced FreeIPA / AD features

Let's take a look at FreeIPA



Future features

- Enterprise user life-cycle
  - User provisioning into staging area and admin controlled activation, recover of deleted users
- DNSSEC support
  - Automatic zone signing and key rotation
- Ipsilon Identity Provider (spinoff project)
  - Web authentication and Federation
    - SAML, OpenID, OpenID Connect, Persona, etc...



Future features - continued

- Password vault
  - Allow users or services to store passwords and other secrets in the directory and retrieve them anywhere using a master password
  - With optional escrow for admins
- Security domains
  - Scope limited sub-CAs
    - VPN Certs
    - Puppet Certs ....

Clearly the best thing since sliced bread!

FreeIPA Server available in:

- RHEL / CentOS / Fedora
- Debian (unstable)
- Ubuntu (15.04)

SSSD Client available in pretty much all distros and even FreeBSD

Cures admin-blues in minutes! As seen on TV!

Questions ?

Learn more

http://freeipa.org

http://fedorahosted.org/sssd

IRC – FreeNode: #freeipa, #sssd

Try it out

Demo site: http://ipa.demo1.freeipa.org

FreeOTP: https://fedorahosted.org/freeotp

Docker Images: http://www.freeipa.org/page/Docker