



# FreeIPA a SSSD

## Správa uživatelů pomocí Free Software

LinuxAlt 2009

Jakub Hrozek

Martin Nagy

30. listopadu 2009

**1 Úvod**

**2 FreeIPA**

**3 SSSD**



# Section 1

## Úvod

## Správa uživatelů a systémů

- definice problému:
  - jakým způsobem můžeme spravovat uživatele a s nimi spojené politiky v síti s mnoha počítači?
  - jak můžeme spravovat stroje v síti, úroveň důvěry mezi nimi, pravidla omezující přihlašování uživatelů podle uživatele, skupiny nebo třeba data a času?
- koncept řešení:
  - ukládat informace o uživateli, strojích, přihlašovací údaje atp. v centralizovaném systému s jednotným uživatelským rozhraním
  - řešení by mělo poskytovat Single-Sign-On nebo alespoň Single Password
  - musí být co nejjednodušší na instalaci a správu
- ve FreeIPA konkrétně:
  - Kerberos (a jeho závislosti: NTP, DNS)
  - LDAP
  - Certificate Authority



## Section 2

# FreeIPA

# FreeIPA



- jednodušší instalace a prvotní nastavení
- snadná správa uživatelů, strojů, skupin, ...
- poskytuje single sign-on.
- centralizované úložiště informací v LDAPu včetně replikace
- skrývá implementační detaily LDAPu, DNS, Kerbera
- certificate Server

# Komponenty FreeIPA

- 389 Directory Server
  - dříve "Fedora Directory Server"
  - dobrá podpora multi master replikace
- MIT Kerberos
- Apache HTTP server
- BIND DNS server
- NTP server
- Red Hat Certificate Server

# Kerberos

- protokol pro autentizaci
- single sign-on, uživatel obdrží *ticket* z *Key Distribution Center* a ten používá pro přihlašování
- klienti musí mít se serverem synchronizovaný čas (nejčastěji pomocí NTP)
- pro ukládání informací se často používá LDAP
- klienti mohou automaticky najít servery pomocí DNS dotazů



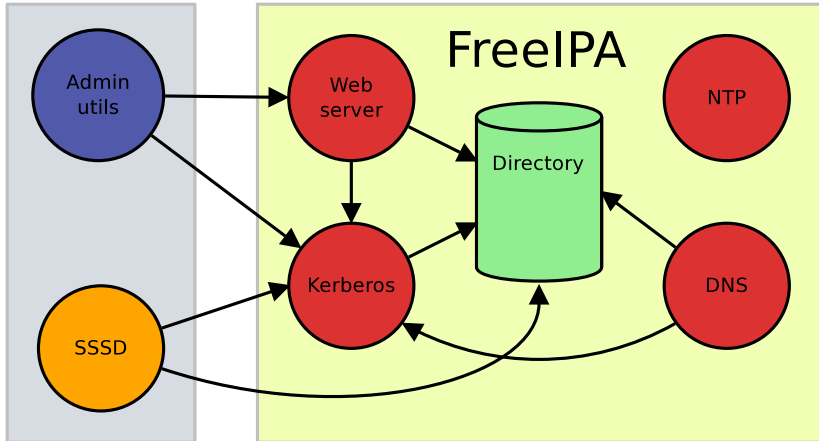
# LDAP

- lightweight Directory Access Protocol
- protokol pro ukládání a přístup k datům na adresářovém serveru
- optimalizován pro čtení
- objekty jsou v adresáři uloženy ve stromové struktuře
- dobrá granularita pro správu přístupových pravidel k jednotlivým podstromům
- Multi-Master replikace
- připojení se k LDAP serveru se může použít jako autentikace (absence podpory Kerbera)

## Problémy s použitím řešení nad LDAP+Kerberos

- administrátor musí spravovat několik netriviálních technologií
- sami si mohou spravovat svoje informace jen technicky velmi zdatní uživatelé
  - změna telefonního čísla - ldapmodify
- špatná abstrakce - administrátor nechce *přidat záznam do LDAPu*, ale jednoduše *vytvořit uživatele*

# Architektura FreeIPA



## Příklad použití FreeIPA (v2)

### Instalace

```
# ipa-server-install
```

### Administrace - přidání uživatele

```
# kinit admin
```

```
Password for admin@EXAMPLE.COM:
```

```
# ipa user-add -f John -l Doe jdoe
```

### Instalace repliky

```
server# ipa-replica-prepare replica.example.com
```

```
Packaging replica information into
```

```
/var/lib/ipa/replica-info-replica.example.com
```

```
server# scp replica-info-replica.example.com.gpg \  
root@replica:~/
```

```
replica# ipa-replica-install \  
replica-info-replica.example.com.gpg
```

## Příklad použití FreeIPA (v2)

### Uživatel

- instalace klienta:

```
# ipa-client-install
```

- změna uživatelova shellu:

```
$ kinit jdoe
```

```
Password for jdoe@EXAMPLE.COM:
```

```
$ ipa user-mod -s /bin/tcsh
```



## Add User

### Identity Details

Add User

Job Title:

First Name:

Last Name:

Full Name:

[Remove](#)

[Add Full Name](#)

Display Name:

Initials:

### Account Details

Account Status:

Login:

Password:

Confirm Password:

UID: Generated by server

GID: Generated by server

Home Directory: Generated by server

### Tasks

[Add User](#)

[Find Users](#)

[Add Group](#)

[Find Groups](#)

[Add Service Principal](#)

[Find Service Principal](#)

[Manage Policy](#)

[Self Service](#)

[Delegations](#)

# Stav vývoje FreeIPA

- FreeIPA verze 1
  - jen identita uživatelů (ne strojů)
  - kombinace LDAPu a Kerbera
  - ovládání z příkazové řádky a pomocí webového rozhraní
- FreeIPA verze 2
  - vyvíjena, 28. října vydána alfa verze
  - rozšiřitelný systém pluginů
  - identita strojů, integrace s DNS
  - přístupová pravidla (HBAC)
  - integrace certifikační autority

# Stav vývoje FreeIPA

- FreeIPA verze 3
  - ve fázi návrhu
  - integrace s Active Directory s využitím Samba 4



## Add a new User

AutoMount

DNS

Services

### Identity Details

Title

First Name

Last Name

Login

Email

Phone

Address

### Account Details

Password

Confirm Password

Error: the passwords do not match

Account Status  ▼

Allow SSH  ▼



# Section 3

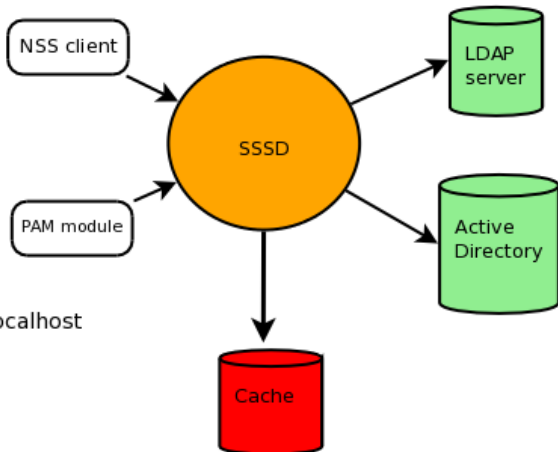
## **SSSD**

## SSSD - více než jen FreeIPA klient

- <http://fedorahosted.org/sss>
- systémový démon
- umožňuje přístup k síťovým službám poskytujícím autentikaci a informace o uživateli
- pokročilejší databáze k ukládání lokálních uživatelů a jejich dat, rozšiřitelné schéma
- komunikuje se systémem pomocí PAM a NSS modulu
- vyvíjen od září 2009

# Architektura SSSD

getent passwd foo

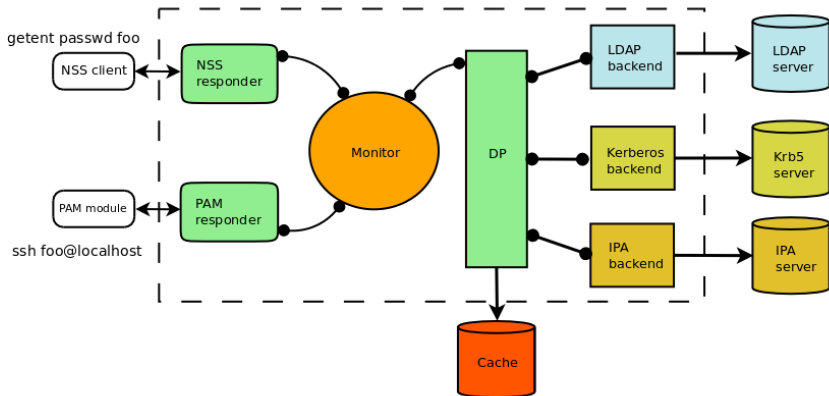


ssh foo@localhost

## Architektura SSSD

- monitor - centrální proces sledující ostatní procesy, spouští nebo restartuje je dle potřeby
- specializované služby běží ve vlastních procesech
  - NSS responder odpovídá na dotazy na identitu uživatelů z NSS modulu `nss_sss`
  - PAM responder zajišťuje PAM konverzaci přes modul `pam_sss`
- procesy služeb komunikují s monitorem přes DBus

# Architektura SSSD



## Lokální databáze

- měla by doplnit či úplně nahradit `/etc/passwd`, `/etc/shadow`
- databáze má formát podobný LDAPu
  - sofistikované vyhledávání
  - rozšiřitelná - avatar, rozložení klávesnice, desktopové prostředí
  - LDB, <http://ldb.samba.org>
- SSSD obsahuje utility na správu lokálních uživatelů podobné `shadow-utils`
  - `sss_useradd`, `sss_userdel`, ...
- skupiny se mohou vnořovat (autorizace)
- koncept "Magic Private Groups" - uživatelské skupiny se fyzicky nevytváří, ale jsou vráceny, jednotný namespace, ID space

## Vzdálené databáze

- LDAP, Kerberos, IPA, AD, ...
- SSSD zajišuje cachování informací o uživatelích
  - není třeba kvůli každému dotazu zatěžovat server
  - jak pozitivní tak negativní cache
- offline autentikace
  - offline cachování informací o uživatelích i přístupových údajů
  - uživatele laptopů, přenosných zařízení
- pro některé backendy specializované služby, např. pro IPA:
  - Host Based Access Control
  - automatické vyhledání serverů (verze 1.0)
  - výběr serveru podle lokace (verze 1.0?)



## Vývoj SSSD

- poslední vydaná verze je 0.7.1
  - backend pro LDAP, Kerberos, IPA
  - cachování informací o uživateli a přihlašovacích údajů
  - lokální databáze uživatelů s nástroji na její správu
  - bindingy pro Python určené na správu uživatelů
- probíhá vývoj verze 1.0RC (druhá polovina listopadu)
  - vylepšení IPA backendu - pravidla pro kontrolu přístupu
  - server failover - přechod na jiný server pokud je preferovaný nedostupný
  - server discovery, location discovery - vyhledání serveru podle domény, IP adresy
- verze 1.0 do konce roku - stabilizace 1.0RC
- binární balíčky jsou k dispozici pro Fedoru, Ubuntu (zastaralé), průběžně kompilujeme i na Suse

## Konfigurace klienta - LDAP/Kerberos, IPA

### Příklad konfigurace domén

```
[domains]
domains = foo.example.com,bar.example.com

[domain/foo.example.com]
id_provider = ldap
ldap_uri = ldapi://ldap.example.com
ldap_user_search_base = ou=users,dc=example,dc=com
auth_module = krb5
krb5KDCIP = 192.168.1.1
krb5REALM = EXAMPLE.COM

[domain/bar.example.com]
id_provider = ipa
ipa_server = ipaserver.example.com
```

## Příklad: konfigurace klienta Active Directory, IPA

### Příklad konfigurace domén (budoucí verze)

```
domains = local,ipa.example.com,ad.example.com
```

```
[domain/local]
```

```
domain-type=local
```

```
[domain/ad.example.com]
```

```
id_provider=ad
```

```
server=ad.example.com
```

```
[domain/ipa.example.com]
```

```
id_provider=ipa
```

```
ipa_domain=example.com
```

## Zapojte se do vývoje

- home page - [www.freeipa.org](http://www.freeipa.org)
  - dokumentace, tarbally, zdrojový kód
- <http://fedorahosted.org/sssds>
  - HOWTO, bugtracker
  - v tarballu manuálové stránky, komentovaný `sssds.conf`
- komunikace
  - IRC - FreeNode, kanál #freeipa
  - konference
    - `freeipa-{devel,users,interest}@redhat.com`,
    - `sssds-devel@lists.fedorahosted.org`
- hack on FreeIPA
  - <http://freeipa.org/page/Contribute>

# Děkuji za pozornost

- Otázky?



# The end.

Thanks for listening.