



FreeIPA

Red Hat Czech Open House

1 Centralizovaná správa uživatelů

2 FreeIPA

3 SSSD

4 Identity Management v Brně



Section 1

Centralizovaná správa uživatelů

Správa uživatelů ve větší organizaci

- na osobním stroji lokální uživatelé
 - `/etc/passwd`, `/etc/shadow`
- větší organizace potřebují účty spravovat centrálně
 - snadná instalace a správa
 - centralizované rozhraní
 - delegace práv (SUDO, selfservice, ...)

Obecné centralizované řešení

- databáze pro ukládání uživatelů, strojů
 - LDAP - replikace, distribuce
- přihlašování, single sign on
 - Kerberos
- správa strojů, služeb
 - DNS, Certificate Authority

LDAP, Kerberos

- LDAP
 - databáze se stromovou strukturou
 - ukládání uživatelů a skupin, adresář pro e-mailové klienty
 - implementace: OpenLDAP, Active Directory, 389DS, ...
- Kerberos
 - protokol pro autentizaci
 - single sign-on, uživatel obdrží *ticket* z *Key Distribution Center* a ten používá pro přihlašování

Příklad uživatele v LDAPu

uživatel v /etc/passwd

```
jakub:x:500:500:Jakub Hrozek:/home/jakub:/bin/bash
```

uživatel v LDAPu

```
dn: cn=jakub,ou=People,dc=redhat,dc=com
objectClass: posixAccount
objectClass: inetOrgPerson
uid: jakub
uidNumber: 500
gidNumber: 500
homeDirectory: /home/jakub
gecos: Jakub Hrozek
loginShell: /bin/bash
cn: jakub
```

Obecné centralizované řešení

- Open Source komponenty existují a používají se
- složitá integrace, špatná abstrakce
 - administrátor chce *přidat uživatele*, ne *vytvořit záznam v LDAPu*
- hotová řešení většinou proprietární
 - MS Active Directory
 - Novell eDirectory



Section 2

FreeIPA

FreeIPA

- Free Identity, Policy, Audit
 - Identity - správa uživatelů, strojů, služeb, DNS
 - Policy - kvalita hesel, SUDO, HBAC
 - Audit - TBD
- cílem je jednoduchá instalace a správa
- existující Open Source komponenty
 - LDAP - 389DS
 - Kerberos - MIT Kerberos
 - DNS - Bind
 - CA - Red Hat Certificate Server
- FreeIPA 2.0 - Fedora 15, RHEL 6.1

Příklad použití FreeIPA (v2)

Instalace

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

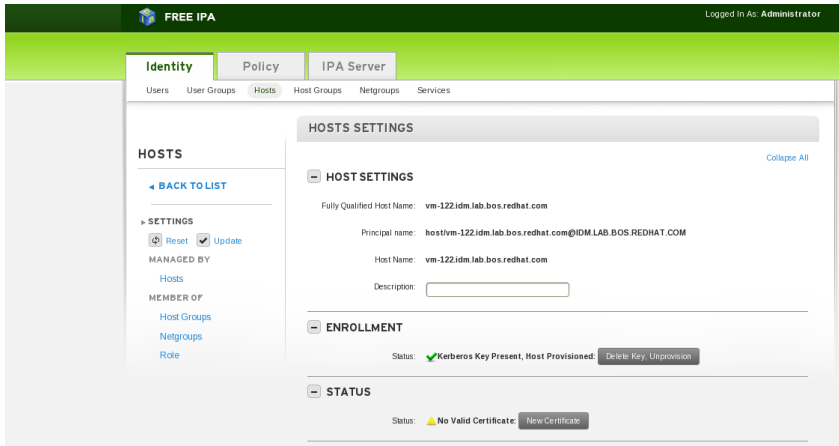
Administrace - přidání uživatele

```
# kinit admin
```

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

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

FreeIPA WebUI



The screenshot displays the FreeIPA WebUI interface. At the top, there is a green header with the "FREE IPA" logo on the left and "Logged In As: Administrator" on the right. Below the header, there are three main tabs: "Identity", "Policy", and "IPA Server". Under the "Identity" tab, there are sub-tabs for "Users", "User Groups", "Hosts", "Host Groups", "Netgroups", and "Services". The "Hosts" sub-tab is currently selected.

The main content area is divided into two sections. On the left, there is a sidebar with the following options:

- HOSTS**
- [BACK TO LIST](#)
- SETTINGS**
- Reset Update
- MANAGED BY**
- [Hosts](#)
- MEMBER OF**
- [Host Groups](#)
- [Netgroups](#)
- [Role](#)

The right section is titled "HOSTS SETTINGS" and contains the following information:

- HOST SETTINGS** (with a "Collapse All" link)
- Fully Qualified Host Name: **vm-122.idm.lab.bos.redhat.com**
- Principal name: **host/vm-122.idm.lab.bos.redhat.com@IDM.LAB.BOS.REDHAT.COM**
- Host Name: **vm-122.idm.lab.bos.redhat.com**
- Description:
- ENROLLMENT**
- Status: **✓ Kerberos Key Present, Host Provisioned:**
- STATUS**
- Status: **▲ No Valid Certificate:**

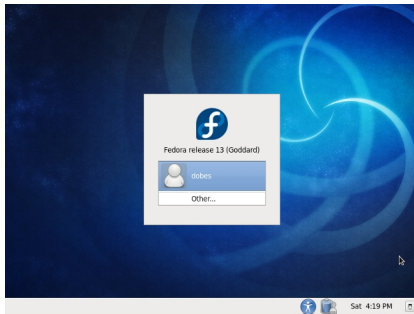


Section 3

SSSD

SSSD

- klientská část centralizovaného řešení
- unixový démon, který běží na každém stroji v síti
- poskytuje informace o uživateli z centrální databáze
- umožňuje uživateli se přihlásit



SSSD

- binární balíčky k dispozici ve Fedoře, RHEL6, Ubuntu, OpenSuse, Gentoo, Debianu
- v současnosti podporuje SSSD několik typů serverů
 - LDAP
 - LDAP+Kerberos
 - FreeIPA
 - Active Directory (jako kombinaci LDAP+Kerberos)

Výhody SSSD

- podporuje více "domén"
 - oddělené servery poskytující různá data
- podpora více serverů pro jednu doménu
 - redundance
- detekce nedostupnosti a opětovné dostupnosti serveru
- cachování informací o uživateli, případně hesel
 - do cache se ukládají pouze opravdu použitá data
 - není třeba kvůli každému dotazu zatěžovat server
 - funguje i při nedostupném serveru
 - záznamy v cache mohou postupně expirovat
 - pro přihlášení se vždy snaží komunikovat se serverem (oproti pam_ccache)
- pro některé druhy serverů specializované funkce



Section 4

Identity Management v Brně

FreeIPA v Brně

- 4 stálí vývojáři + intern
 - jedno volné místo
- zbytek týmu v USA, Německu
- možnost spolupráce formou studentských prací

Zapojte se do vývoje

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

Děkuji za pozornost

- Otázky?