FreeIPA

Red Hat Czech Open House

Section 1

Centralizovaná správa uživatelů

redhat.

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, . . .)

redhat.

Obecné centralizované řešení

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

redhat.

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

redhat

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
```

redhat.

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

redhat.

FreeIPA

- Free Identity, Policy, Audit
  - Identity - správá 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

redhat.

Příklad použití FreeIPA (v2)

Instalace

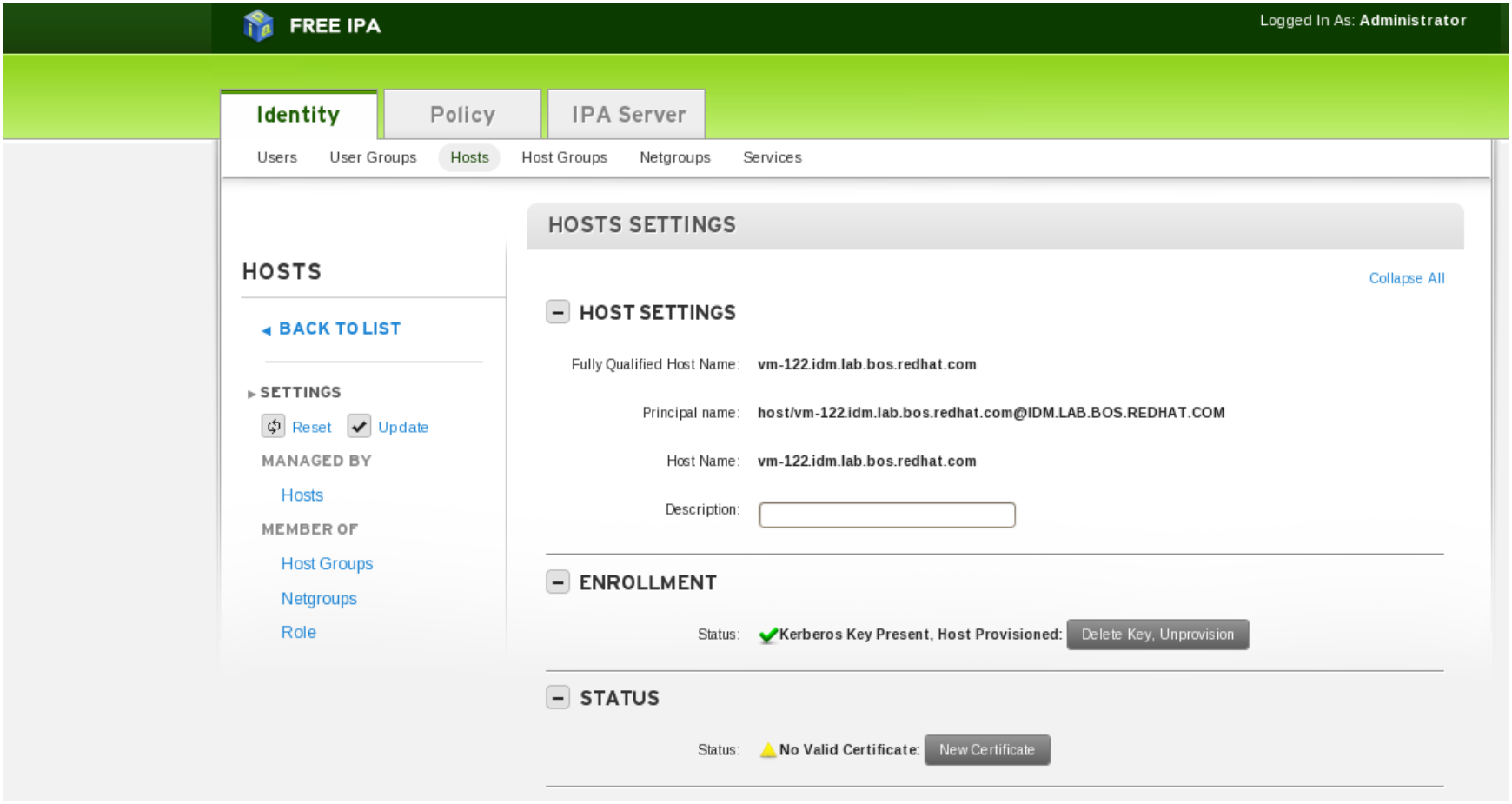
```
# ipa-server-install
```

Administrace - přidání uživatele

```
# kinit admin
Password for admin@EXAMPLE.COM:
# ipa user-add -f John -l Doe jdoe
```

redhat.

FreeIPA WebUI



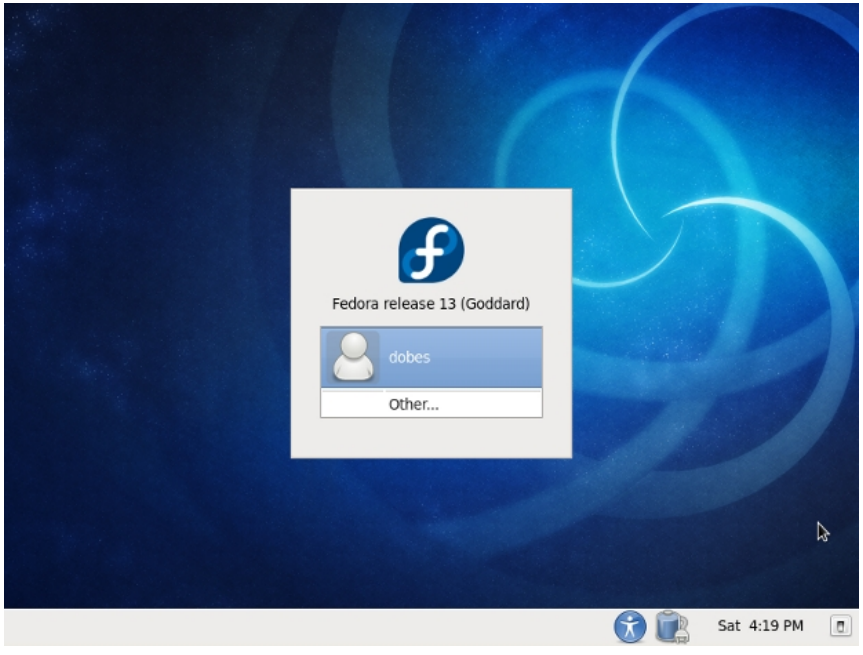
Section 3

SSSD

redhat.

SSSD

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



redhat.

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)

redhat.

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 uživatelích, 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

redhat.

Section 4

Identity Management v Brně

redhat.

FreeIPA v Brně

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

redhat.

Zapojte se do vývoje

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

redhat.

Děkuji za pozornost

- Otázky?