FreeIPA a SSSD

Pokročilá správa uživatelů v Linuxu

Red Hat Czech s.r.o.

Jakub Hrozek Jan Zelený Pavel Zůna

21. října 2010

redhat.

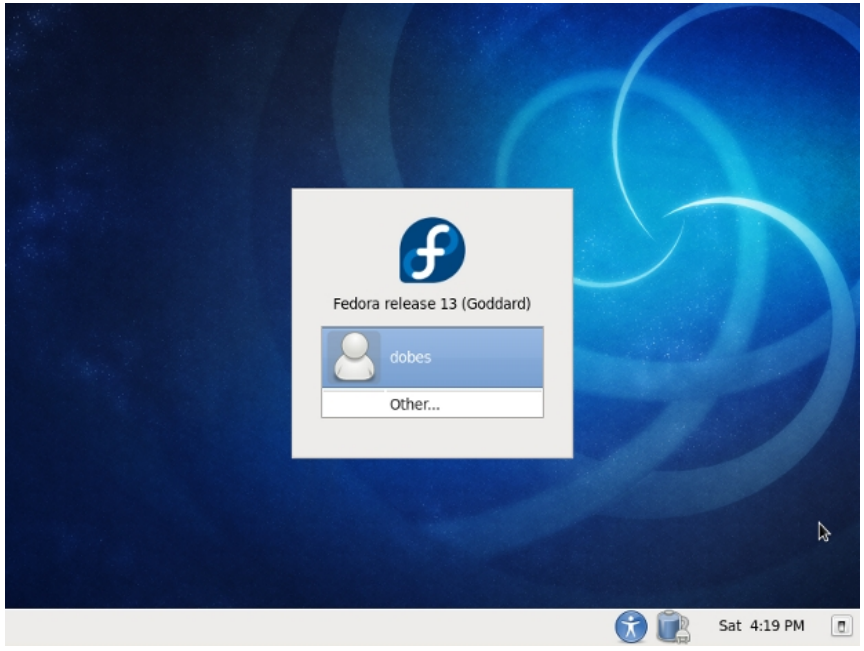
Section 1

Přihlašování uživatelů v Linuxu

redhat

Přihlášení uživatele

- Jak zjistit seznam všech uživatelů v systému?
- Jak zjistit podrobnosti o konkrétním uživateli?
  - domovský adresář, seznam skupin, ...
- Jak uživatele příhlásit



redhat.

Přihlašování uživatelů obecně

- GDM, ssh, login, ...
- obecně se přihlášení skládá z více kroků
  - získání totožnosti - identifikace
  - ověření totožností uživatele - autentizace
  - ověření, zda uživatel má právo vykonat požadovanou činnost - autorizace
  - zpřístupnění služby

redhat.

Historický vývoj – získávání informací

1. vše v souborech
   - uživatelé v `/etc/passwd`, názvy strojů v `/etc/hosts`, ...
   - aplikace mohou přímo přistupovat k souborům
2. programové rozhraní poskytované knihovnou `libc`
3. postupně bylo třeba získávat informace i z jiných databází
   - uživatelé v LDAPu, názvy strojů v DNS, ...
   - staré verze Unixových systémů měly pořadí databází zakompilováno

redhat.

Historický vývoj – autentizace

1. teoreticky je možné, aby si program např. sám porovnal hash hesel se záznamem v `/etc/shadow`, ale:
   - musel by mít oprávnění soubor číst
   - každý program by musel toto implementovat (bezpečnost!)
   - použitelné jen pro autentizaci heslem v souboru
     - co když nepoužíváme hesla? (fingerprint, . . .)
     - co když hesla nejsou v souboru?
2. v Unixových systémech se typicky používá systém PAM
   - podobně jako Name Service Switch je modulární
   - pro různé autentizační mechanismy moduly formou knihoven

redhat.

Name Service Switch

- prostředek poskytující programům přístup ke zdrojům informací
- modulární - přístup k jednotlivým databázím pomocí samostatných knihoven
  - k dispozici knihovny pro soubory, LDAP, NIS a další
- různé databáze pro ruzné druhy informací
  - uživatelé, skupiny, stroje, ...
- konfigurační soubor `/etc/nsswitch.conf`
  - určuje jaké moduly se mají použít
  - specifikuje jejich pořadí

redhat.

PAM - Pluggable Authentication Modules

- poskytuje API pro aplikace, které jej chtějí využívat
- může provádět následující činnosti

account - Ověření účtu (např. expirace)
auth - Autentizace uživatele (např. kontrola hesla)
session - Nastavení prostředí služby
password - Správa hesel, jejich změna, kontrola kvality

redhat.

PAM - Pluggable Authentication Modules

- velké množství dostupných modulů
- možnost detailního nastavení přístupových pravidel
  - autentizace pomocí `/etc/shadow`, LDAPu, Kerbera
  - kontrola kvality hesel, kontrola systémového času
  - ...
- konfigurační soubory v adresáři `/etc/pam.d`

redhat.

Shrnutí

- Pro přihlášení uživatele do systému je třeba:

  Zjistit informace - voláním knihovny libc, která přistupuje k informacím přes komponentu Name Service Switch

  Provést přihlášení - typicky pomocí autentizačních modulů PAM

redhat.

Section 2

Centralizované databáze uživatelů

redhat.

Lokální účty ve větší organizaci

- teoreticky je možné distribuovat soubory
  - v praxi nastává problém se synchronizací
- výhodnější řešení: centralizace informací
- v praxi několik běžně používaných řešení
  - UNIX/Linux – LDAP, LDAP + Kerberos, NIS
  - Windows – Active Directory (LDAP + Kerberos)

redhat.

LDAP

- databáze se stromovou strukturou
- lze použít:
  - ukládání uživatelů a skupin
  - adresář pro e-mailové klienty
  - jakákoliv data se stromovou strukturou
- implementace: OpenLDAP, Active Directory, 389DS, ...

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.

Konfigurace klientské stanice pro LDAP

- pomocí modulů NSS a PAM

NSS - `nss_ldap`

PAM - `pam_ldap`

parametry serveru - `/etc/ldap.conf`

redhat.

Konfigurace klientské stanice pro LDAP - parametry serveru

- konfigurační soubor `/etc/ldap.conf`

/etc/ldap.conf

```
host ldaps://ldap.example.com:636
base dc=example,dc=com
ssl start_tls
ssl on
```

redhat.

Konfigurace klientské stanice pro LDAP - NSS

- konfigurační soubor `/etc/nsswitch.conf`

/etc/nsswitch.conf

```
passwd:     files ldap
shadow:     files
group:      files ldap
```

redhat.

Konfigurace klientské stanice pro LDAP - PAM

- konfigurační soubory `/etc/pam.d/system-auth` a `/etc/pam.d/password-auth`
- v praxi se často nastavuje pomocí GUI/CLI nástrojů
- na ukázku pouze `auth` modul

/etc/pam.d/system-auth

```
auth required    pam_env.so
auth sufficient  pam_unix.so nullok try_first_pass
auth requisite   pam_succeed_if.so uid >= 500 quiet
auth sufficient  pam_ldap.so use_first_pass
auth required    pam_deny.so
```

redhat.

Problémy modulů `nss_ldap` a `pam_ldap`

- jak specifikovat více LDAP serverů pokud jeden z nich vypadne?
- jak specifikovat více LDAP serverů jako více zdrojů informací?
- co se stane, pokud není LDAP server dostupný?
  - nedostupná síť, laptop ve vlaku, nedostupná korporátní VPN

redhat.

Problémy modulů `nss_ldap` a `pam_ldap`

- řešení je několik:
  - `ldapsearch | awk > /etc/passwd` v cronu :-)
  - lokální LDAP server synchronizující data
  - projekt `nsscache`
- ovšem replikují *celý* adresář
  - potenciálně desítky tisíc záznamů
  - u všech uloženy i hashe hesel apod.
- také neřeší více serverů apod.

Section 3

SSSD

redhat.

System Security Services Daemon

- `http://fedorahosted.org/sssd`
- systémový démon, který umožňuje přístup k adresářovým a autentizačním službám
- komunikuje s operačním systémem pomocí vlastních modulů NSS a PAM
- vyvíjen od září 2008

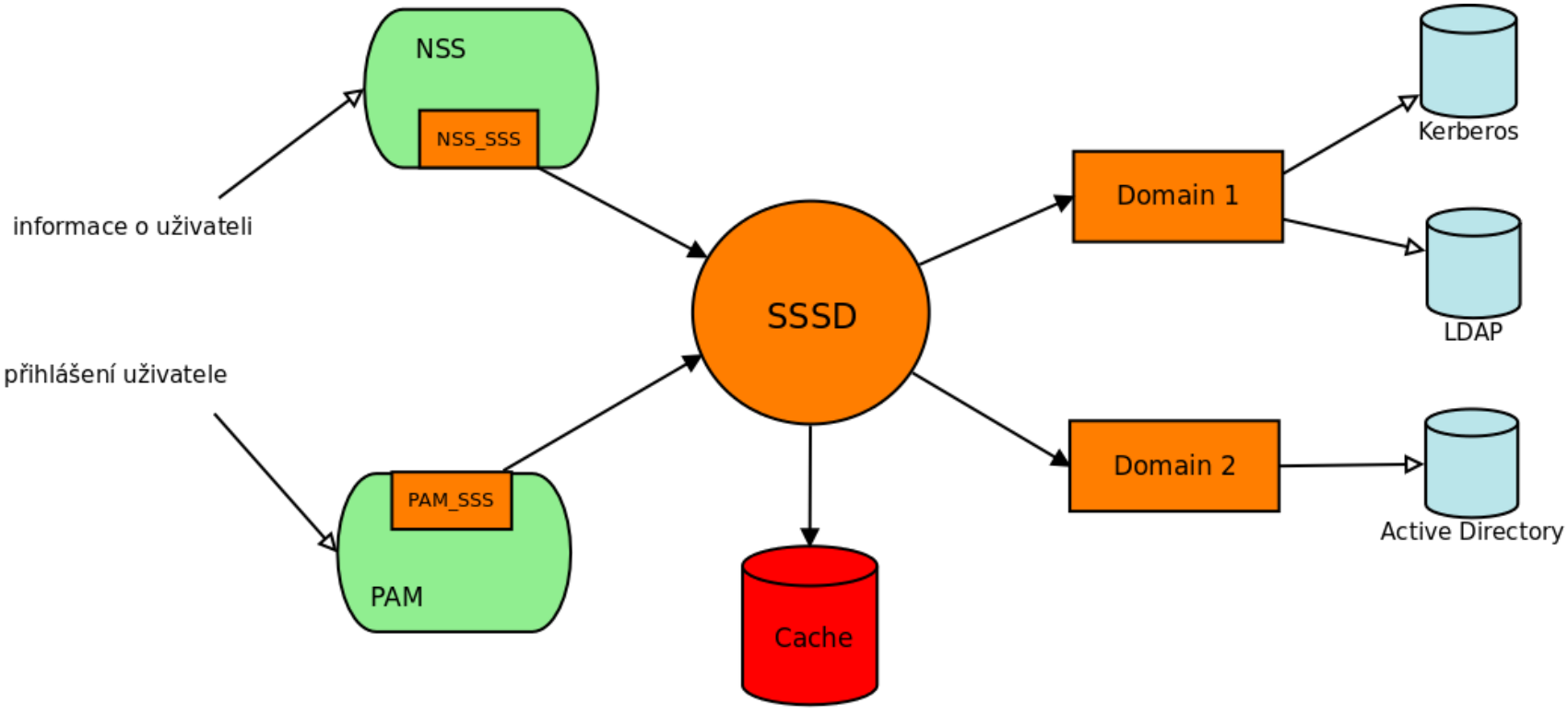
redhat.

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.

Architektura SSSD



redhat.

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`
  - každá doména jako samostatný proces, který zajišťuje komunikaci se serverem
- procesy služeb komunikují s monitorem pomocí protokolu DBus

redhat.

Konfigurace SSSD - PAM a NSS

- konfigurace je velmi podobná nativním modulům pro LDAP
- v podstate stačí jen záměna `s/ldap/sss/`

/etc/nsswitch.conf

```
passwd:     files sss
shadow:     files
group:      files sss
```

redhat.

Konfigurace démona SSSD

- konfigurační soubor `/etc/sssd/sssd.conf`

/etc/sssd/sssd.conf

```
[sssd]
domains = LDAP.EXAMPLE.COM

[domain/LDAP.EXAMPLE.COM]
id_provider = ldap
ldap_uri = ldaps://ldap.example.com
ldap_search_base = ou=accounts,dc=example,dc=com
cache_credentials = true
```

redhat.

Stav SSSD

- poslední vydaná verze je 1.4.0
- binární balíčky k dispozici ve Fedoře, RHEL6, Ubuntu, OpenSuse, Gentoo, Debianu
- v současnosti podporuje SSSD několik typů serverů
  - LDAP
  - Kerberos
  - FreeIPA
  - Active Directory (jako kombinaci LDAP+Kerberos)

redhat.

Budoucí vývoj SSSD

- přístup k pravidlům sudo uloženým v LDAP serveru
- ukládání SSH klíčů v LDAPu a přístup k nim
- poskytování lokálních uživatelů
- možnost vytváření externích back endů
  - i proprietárních - např. RSA servery, Active Directory
- do vývoje je možné se zapojit i formou bakalářských nebo diplomových prací

Section 4

Závěr

redhat.

Workshop

- Možnost v praxi si vyzkoušet SSSD, FreeIPA
- středa 3.11. 15-17 hodin na Gotexu
- je možné domluvit i jiný termín
- přihlášení e-mailem `jhrozek@redhat.com`

redhat.

Bakalářky, diplomky

- příklady témat:
  - autentizační API pro webové aplikace a SSSD
  - sada ukázkových aplikací pomocí knihovny `tevent`
  - analýza výkonnosti 389 Directory Serveru
  - podpora novějšího protokolu `kpasswd` pro server FreeIPA
  - podpora OpenLDAP pluginů v 389 Directory Serveru
- dotazy na workshopu nebo mailem `jhrozek@redhat.com`

redhat.

Děkuji za pozornost

- Otázky?

The end.

Thanks for listening.