Zdokonalení integrace SSSD a SUDO

Michal Šrubař
xsruba03@stud.fit.vutbr.cz

Možná struktura textu

- Smysl BP.
- Uživatelé, root, jak dát běžným uživatelům vyšší práva
- Sudo, su, alternativy
- Proč sudo?
- Proč sudo v LDAPu? (alternativy jak a kam ukládát sudo pravidla, např. puppet)
  - Složitost konfigurace a správy (všechno v textu, není GUI, které FreeIPA má)
  - Firma s mnoha zaměstnanci chce centrálně spravovat informace a politiky o svých uživatelích (chtěla by mít vše na jednom místě a né informace v ldap, sudo pravidla v LDAPu ale nebylo by to nijak propojeno, konfiguráky v puppetu, atd...)
  - sudo pravidla nejsou nijak propojena s ostatními informacemi, které mohou a často jsou v LDAPu uloženy (uživatelé, skupiny, atd)
- Problémy a nedostatky defaultního LDAP shématu, které SUDO používá
  - na uživatele se odkazuje pouze přes řetězec jména, není tam žádná provázanost s počítačem ze kterého dany uživatel je
  - pokud LDAP spravuje i uživatele, a je tam stejný uživatel jako na lokální mašině, tak tam vzniká nějaký problém s překrytím těch uživatelů
  - mezi uživateli a sudo pravidly neexistuje vazba, pokud odstraním uživatele, tak mně zůstane pravidlo s neexistujícím uživatelem
- Projekt FreeIPA
- Proč sudo ve FreeIPA (?granularita?)
- Proč má IPA vlastní SUDO LDAP schema a jaké výhody přináší
  - umožňuje např. povolit/zakázat pravidlo
- Jak to funguje teď
  - definice pravidla
  - jak se uloží v LDAPu
  - co tam bude jinak oproti tomu než bych to uložil do LDAPu s legacy schematem
  - konverze do legacy schématu když k tomu přistoupím přes SSSD
  - cachování
- Proč musí IPA nové schéma přeložit do legacy schematu než jej pošle SSSD
- Jaké problémy to přináší
- Jaké úpravy je nutné provést
  - u sudo bude třeba přenést něco z /lib do /usr (z ticketu: pe_task, cron)
- Vyzdvihnout všechny přednosti

Hlavní problém, který moje BP řeší

FreeIPA používá pro uložení SUDO pravidel v LDAPu svoje schéma, které přináší mnoho vylepšení. **SSSD** ovšem toto schéma neumí zpracovat (FreeIPA nejprve používala legacy schema pro uložení a pak navrhla nové). FreeIPA musí nové schéma přeložit do legacy schématu, které sssd umí zpracovat. Převodem se ovšem ztrácí mnoho informací, které potom způsobují problémy a brzí to tak využití celého potenciálu.

Jelikož SSSD neumí to FreeIPA schéma, tak se musí dodatečně stahovat mnoho informací, což u rozsáhlé databáze způsobuje značné zpomalení. Úkolem není navrhnout nové LDAP schéma pro SUDO, ale upravit SSSD daemon a SUDO tak, aby podporovaly LDAP schéma, které používá IPA.

Hodně zjednodušeně bude výsledkem správný dotaz na LDAP adresář na IPA serveru, který pro daného klienta stáhne všechno potřebné.

1 Administrace linuxového systému

Na většině dnešních linuxových a Unix-like[1] operačních systémech provádí správu systému speciální uživatel zvaný **root**. Někdy také označován jako **superuser**. Tento uživatel má přístup ke všem souborům a může spouštět všechny příkazy operačního systému[2]. Ostatní uživatele systému toto právo nemají, až na tyto vyjímky:

- uživatel zná heslo uživatele root
- uživatel použije program, který mu dočasně poskytne práva uživatele root

1.1 su (Substitute User)

Tento program umožňuje libovolnému uživateli stát se dočasně jiným uživatelem. Vě většině případů je jiný uživatel právě uživatel root. To znamená, že program su může dát libovolnému uživateli, který zná heslo uživatele root, plnou kontrolu nad operačním systémem.

1.2 sudo (Super User DO)

Sudo umožňuje uživateli provést jeden příkaz jako jiný uživatel. Bezpečností politiky, které definují kteří uživatelé mohou spouštět jaké příkazy se nazývají **sudo pravidla**. Tyto pravidla jsou uloženy v souboru */etc/sudoers*. Sudo pravidla by měla být upravována výhradně pomocí utility **visudo**, která zároveň provádí kontrolu syntaxe souboru */etc/sudoers*.

1.2.1 Mezi hlavní výhody SUDO

Jedná se dva naprosto odlišné přístupy k tomu jak získat oprávnění uživatele root.

- sudo umožňuje limitovat přístup zatímco su může uživateli dát plnou kontrolu nad systémem
- uživatel nemusí znát heslo uživatele root
- použití sudo může být monitorováno
- je možné definovat, kteří uživatelé mohou provádět jaké úlohy

1.3 Sudo a pluginy

Sudo Plugin API[3] umožňuje vytvoření vlastního modulu, který bude definovat vlastní správu politik. To jaké pluginy bude sudo používat je možné konfigurovat pomocí souboru */etc/sudo.conf*.

1.4 Distribuce sudo pravidel mezi více počítači

Každý systém, na kterém chci využívat SUDO, musí mít soubor obsahující sudo pravidla. Sudo ovšem nemá nativní způsob jak tyto pravidla šířit mezi více systémy, alčkoliv existuje několik způsobů jako toho dosáhnout:

[1] http://en.wikipedia.org/wiki/Unix-like
[2] http://www.linfo.org/root.html
[3] http://www.sudo.ws/sudo_plugin.man.html

1.4.1 Manuální distribuce

Administrátor spravující více systémů může může sudo pravidla šířit mezi více systémy pomocí nástrojů jako je cron, scp, rsync, atd. Tento způsob je ovšem velmi pracný.

1.4.2 Centrálním uložiště

Je možné využít nástrojů, které automaticky sledují a distribuují soubory mezi vice systémy. Mezi tyto nástroje patří např. Puppet[4]

1.4.3 LDAP adresář

Ve většině firemních prostředí se dnes používá adresářových služeb k synchronizaci uživatelů, skupin a dalších sdílených informací. Sudo pravidla mohou být na tomto serveru také uložena. Přistoupit k nim je možné pomocí protokolu LDAP[5]. Při použití adresářového serveru je možné sudo pravidla centrálně spravovat a globálně k nim přistupovat. Sudo ovšem takto nativně nepracuje proto je potřeba plugin. Sudo má plugin pro použití s openLDAP. Schéma v jakém jsou sudo pravidla na LDAP serveru uložena je pevně specifikováno a přináší následující nevýhody:

1. problém s tím překrýváním lokálních uživatelů
2. další

Pokud chce administrátor tento způsob správy politik využít, pak musí dané schéma dodržet i se všemi jeho nevýhodami.

1.5 Why is SUDO in LDAP better solution?

LDAP is characterized as a "write-once-read-many-times" service. It's eminently suitable for maintaining data which are not changed very often. Sudo rules are set once by system's administrator but accessed by users many times. Administrator will also want to edit the rules but not as often as client will access it.

Directories are faster that databases because they don't require consistency as much as relational or transactional databases. It doesn't use transactions, locking or roll-backs[6].

1.6 What is meant by LDAP server?

Technically, LDAP is just a protocol that defines the method by which directory data is accessed. It also defines and describes how data is represented in the directory service.

2 FreeIPA

FreeIPA používá vlastní schéma a proto musela napsat i vlastní plugin sss.

Výhody použití FreeIPA pro správu sudo pravidel - u sudo+openldap musím vytvořit schéma a ručně jej přidat mezi ostatní schémata + přidat o tom záznam do /etc/sldap.conf

[4] http://puppetlabs.com/puppet/what-is-puppet
[5] Lightweight Directory Access Protocol, which is an application protocol for querying and modifying directory services.
[6] www.zytrax.com/books/ldap/ch2/