**Abstrakt**

The purpose of this thesis is to improve integration between SUDO and SSSD with a focus at improved support of sudo rules stored on a FreeIPA server in native IPA SUDO scheme. It presents design and implementation of native IPA provider for processing these rules at SSSD side. Designed provider eliminates unnecessary overhead of exporting sudo rules from IPA SUDO native schema info legacy SUDO scheme on a FreeIPA server.

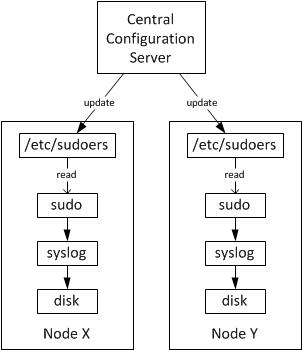
# – Úvod

# – Správá uživatelských práv na linuxových systémech

Sepiš vice možností jakými je možno delegovat práva a potom napiš, že v následujícím textu se budeš zabývat právě SUDO+SSSD+IPA protože je to rozšířené mezi uživateli RHELu.

Jestliže máme velký server a vice adminů starající se o vice služeb, tak nechceme každému dát heslo roota, ale raději by jsme chtěli mít možnost delegovat určitá prává. Tak stejně uživatelů by se sem tam hodily vyšší práva

* 1. **SUDO**
* co to je a co nám to umožňuje dělat
* syntax sudo pravidel + obrázek s příkladem (příklad stejného pravidla jak by vypadalo v ldapu a pak v IPA)
* šíření sudo pravidel mezi více počítačů je problém (obrázek: jeden administrator má nastarost spoustu strojů, kdy každý má vlasní sudoers soubor pravidel)
  + možná řešení toho problému
* mnoho společností dnes LDAP používá a celkem se hodí pro uložení sudo pravidel
* distribuce pravidel s pomocí LDAPu

****

* rozdíl mezi lokalním sudoers a sudoers v LDAPu (LDAP negarantuje pořadí v jakém vrací záznamy ani atributy)
* stejný příklad sudo pravidla jak by vypadalo v LDAPu
  1. **FreeIPA**
* co to je a krátce co to všechno umí
* popsat IPA SUDO Schéma
  + každé záznam i kontejner v sudo kontejneru má operační atribut **entryUSN**, včetně sudo kontejneru samotného
* musíš vymezit oblast: IPA umí 100 věcí, ale nás bude v rámci této práce zajímat pouze sudo pravidla
* problem spojené s tím, když mám sudoers v LDAPu
  + problem s překrýváním uživatelů
  + schema je dané a nedá se měnit
  + nepropojenost uživatelů s pravidly (příklad s tím mazáním pravidel)
* výhody když mám sudoers v LDAPu
  + webgui pro správu pravidel (sudo+ldap => manuální správa pravidel přes konfigurační soubory)
  + granularita
* přiklad sudo pravidla v novém IPA formatu (stejný příklad jako v sekci sudo)
  1. **SSSD z uživatelského hlediska**
* co to je a krátce co to všechno umí
* vymezení oblast, kterou se tato práce bude zabývat
* nevýhody, které má řešení stahování pravidel přes sudo ldap plugin
  + síť
  + cachování
* obrázek (user -> sudo -> SSSD -> IPA)
* sssd volby pro sssd.conf
  + ldap\_sudo\_use\_host\_filter …
* ss

**Refreshes**

**Smart refresh**

**Full refresh**

Provede smazání všech pravidel z cache a stažení všech pravidel z LDAP serveru. Tento typ je prováděn pouze v některých případech, protože v případě mnoha pravidel generuje velký síťový provoz. Provádí se pouze při spuštění SSSD nebo při detekci změny pravidel na serveru.

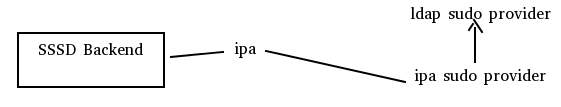
**Rules refresh**

Pokaždé, když je spuštěno sudo, je také spuštěn rules refresh, který zajistí, že uživatel nedostane větší oprávnění než je definováno. Tento refresh znovu stáhne všechna pravidla, aplikovatelná na uživatele, který sudo spoustil, která exspirovala\footnote{Doba po které pravidla v cache exspirují je možno specifikovat v sssd.conf pomocí volby}. Jestliže se některé pravidlo na serveru nenachází, pak se provede full refresh.

Všechny typy refresh znázorňuje následující schéma a detailně jsou rozebírana v sekci refresh…

# – SSSD

* tato kapitola popisuje vnitřní architekturu SSSD se zaměřením na SUDO respondera a providera
* popisuje základní koncepty knihoven talloc a tevent na kterých SSSD staví
  1. **Talloc**
* základní concept hierarchického alokátoru
* nahrazuje malloc
  1. **Tevent**
* událostmi řízené paradigm programování
* vysvětlit základní concept událostí, requests, subrequest, asynchronní funkce
* používá talloc
* zmínit že obaluje DBus a OpenLDAP
  1. **Dereference u LDAPv3**
  2. **Architektura SSSD**
* z jakých komponent se SSSD skládá (monitor, backends, responders, provideres)
* schéma architektury
  1. **Tok dat**
* tok dat do SUDO -> SUDO Responder -> Backend -> LDAP Provider -> IPA a zpět
  1. **IPA SUDO Provider**
* Nejprve popsat LDAP provider a pak říct že nativní ipa sudo provider není?
* když stahuju pravidla normálně z LDAP adresáře tak se použije tento provider, ale když je chci stahovat z IPA, tak se na IPA serveru musí ty pravidla překládáat přes kompat plugin do SUDOers kontejnéru a to přináší režii, protože musíme překládávat všechny pravidla
* SSSD neumí zpracovat pravidla IPA formátu
* momentálně žádný nativní IPA SUDO Provider neexistuje a IPA SUDO Provider využívá LDAP SUDO Provider
* neumožňuje to využít všech vlastností nového IPA SUDO schemata (ipaSudoOpt)
* pokud se export pravidel přesune do SSSD, tak se nemusí exportovat všechny pravidla, ale pouze ty aplikovatelná na konkrétního hosta



* popsat funkci compat palaginu + obrázek
  1. **LDAP SUDO Provider**
* monitor creates backend for every domain
* nastavení search base a search bases array
* nějaké základní schéma a pak až podrobněji popsat jednotlivé části
  + 1. **Inicializace**
* detailní popis se schématy
* vytvoření mapy (detailní popis později)
* nastavení plánování refresh
* zmínit, že se při každém spuštění provádí FULL REFRESH
  1. **Full, Smart and Rules refresh (pro každý typ vlastní sub sekci?)**
* obecné informace v user sekci u SSSD v kapitole 2
* jak se vyvolávají
* jak se plánují
* jak se dají časy ovlivnit v sssd.conf
* jaké LDAP filtry používají
* zmínit že všechny využívají to asynchronní provádění od sdap\_sudo\_refresh (v providers/ldap/sdap\_async\_sudo.c)
  1. **Asychnronní stažení a uložení pravidel**
* hlavní motor LDAP SUDO Provideru, který využívají všechny typy refresh
* detailní popis se schématy
  1. **Nativní mapa sudo pravidel**
* detailní popis + schema

# – Nativní IPA SUDO Provider

1. **Návrh**

* nové LDAP search filtry a proč jsem je vybral
  + ( refer to LDAP filters in RFC! https://tools.ietf.org/html/rfc2254#ref-1)

1. **Implementace**
2. **Testování**

* bench marky jestli je to rychlejší než LDAP SUDO Provider?
* performance testy, od lidí, kteří používají IPA s velkou databází

# – Zhodnocení

1. **odstavec**

* co se mi podařilo naimplementovat a otestovat
* co na to komunita sssd
* věci nad rámec zadání jako patche nebo dokumentace, která neexistovala

1. **odstavec**

* další věci na kterých bych se dalo zapracovat