



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

ZDOKONALENÍ INTEGRACE SSSD A SUDO

IMPROVED INTEGRATION OF SSSD AND SUDO

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

MICHAL ŠRUBAŘ

VEDOUCÍ PRÁCE

SUPERVISOR

Prof. Ing. TOMÁŠ VOJNAR, Ph.D.

BRNO 2014

Abstrakt

Smyslem této bakalářské práce je zlepšení integrace mezi SUDO a SSSD se zaměřením na vylepšení podpory SUDO pravidel uložených na serveru FreeIPA. Zabývá se popisem LDAP SUDO provideru a přináší návrh a implementaci IPA SUDO provideru. Navržený provider eliminuje nadbytečnou režii překládání SUDO pravidel z IPA SUDO schématu do nativního LDAP SUDO schématu na straně FreeIPA serveru.

Abstract

The purpose of this thesis is to improve integration between SUDO and SSSD with a focus on improved support of SUDO rules stored on an FreeIPA server in the native IPA SUDO scheme. It presents documentation of LDAP SUDO provider and also the design and implementation of the native IPA SUDO provider. Designed provider eliminates unnecessary overhead of exporting SUDO rules from IPA SUDO schema info native LDAP SUDO scheme on an FreeIPA server.

Klíčová slova

sudo, nativní LDAP SUDO schéma, IPA SUDO schéma, FreeIPA, SSSD, LDAP SUDO provider, IPA SUDO provider

Keywords

sudo, native LDAP SUDO schema, IPA SUDO schema, FreeIPA, SSSD, LDAP SUDO Provider, IPA SUDO Provider

Citace

Michal Šrubař: Zdokonalení integrace SSSD a SUDO, bakalářská práce, Brno, FIT VUT v Brně, 2014

Zdokonalení integrace SSSD a SUDO

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením pana ...

.....

Michal Šrubař
17. května 2014

Poděkování

Rád bych poděkoval profesoru Vojnarovi za veškerou poskytnutou pomoc. Dále mému technickému vedoucímu Jakubu Hrozkovi za trpělivost a vedení. Poděkování patří také komunitám projektů SSSD a FreeIPA za trpělivé zodpovídání veškerých dotazů a to zejména Pavlu Březinovi.

© Michal Šrubař, 2014.

Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Obsah

1	Úvod	3
2	Správa bezpečnostních politik identit	4
2.1	Sudo	4
2.1.1	Distribuce sudo pravidel	5
2.1.2	Nativní LDAP sudo schéma	6
2.1.3	Integrace identit a politik	7
2.2	FreeIPA	8
2.2.1	IPA sudo schéma	10
2.2.2	Definice sudo pravidel	12
2.3	System Security Services Daemon	12
2.3.1	Aktualizace sudo pravidel v cache paměti	13
3	SSSD a SUDO provider	15
3.1	Knihovny třetích stran	15
3.2	Architektura SSSD	17
3.3	SSSD z pohledu programu sudo	18
3.3.1	SDAP dotaz a mapování atributů	19
3.4	LDAP SUDO Provider	21
3.4.1	Inicializace	23
3.4.2	Plánování aktualizací	23
3.4.3	Aktualizace sudo pravidel	23
3.4.4	Asynchronní modul	26
3.4.5	Uložení sudo pravidel do sysdb	28
3.4.6	LDAP SUDO Handler	28
3.5	IPA SUDO provider	28
4	Nativní IPA SUDO Provider	31
4.1	Návrh	31
4.1.1	Sudo pravidla aplikovatelná na klienta	31
4.1.2	Stážení sudo pravidel	32
4.1.3	Překlad pravidel	35
4.1.4	Využitelnost LDAP pluginu	38
4.2	Implementace	38
4.3	Testování	40
4.3.1	Metodika	40
5	Závěr	41

Kapitola 1

Úvod

Tato bakalářská práce popisuje správu bezpečnostních politik identit s pomocí použití programu sudo. Popisuje problémy, na které může administrátor narazit při nasazení tohoto řešení v doménovém prostředí. Představuje možná řešení těchto problémů použitím technologií FreeIPA a SSSD, které jsou používány v Redhat Enterprise prostředích. Toto řešení ovšem disponuje určitými nedostatky, které tato práce odkrývá. Smyslem této práce je tedy tyto nedostatky identifikovat, navrhnout jejich řešení a tyto řešení implementovat.

Cílem tedy není diskutovat nad možnostmi a technologiemi, které je možné pro správu politik identit použít. Také nemá sloužit jako návod pro konfiguraci výše zmíněných technologií pro řešení daného problému.

Od čtenáře je ovšem očekávána uživatelská znalost programu sudo, základních konceptů online adresářů a LDAP protokolu.

Struktura této práce je rozdělena do pěti kapitol. První kapitola popisuje obsah této práce. V kapitole 1 jsou popsány problémy, které vznikají při centralizované správě identit a jejich bezpečnostních politik za pomoci programu sudo. Diskutuje také nad možným řešením v podobě použití serveru FreeIPA a démonu SSSD.

Třetí kapitola se blíže zabývá démonem SSSD. Popisuje jeho architekturu a činnost z pohledu programu sudo a dokumentuje činnost pluginů ipa a ldap, které SUDO provider používá pro zpracování sudo pravidel na straně klienta. Tento popis byl sestaven na základě experimentování a čtení zdrojových kódů projektu SSSD. Sekce 3.5 poté detailně popisuje hlavní nedostatek v démonu SSSD, na který se tato práce zaměřuje.

Tento popis posloužil pro sestavení návrhu a implementaci, který tento nedostatek odstraňuje. Návrhem, implementací a testováním navrženého řešení se zabývá kapitola 4.

Poslední kapitola poté zhodnocuje dosažené výsledky a diskutuje nad možnostmi pokračování v této práci.

Tato práce dále používá následující konvence:

1. Všechny důležité pojmy jsou vysázeny **tučným písmem**.
2. Nové pojmy jsou vysázeny *kurzivou*.
3. Hodnoty atributu ipaUniqueID byly záměrně zkráceny kvůli velikosti textu a obrázků.
4. Všechny názvy souborů, jejich obsahy, klíčových slova jazyka C nebo jména identifikátorů jsou vysázeny **strojovým písmem**.

Kapitola 2

Správa bezpečnostních politik identit

Tato kapitola popisuje možnost správy bezpečnostních politik identit pomocí programu `sudo`. Popisuje možné problémy, které mohou nastat při distribuci pravidel, kterými se program `sudo` řídí a dále LDAP schéma, které `sudo` používá pro uložení těchto pravidel v LDAP adresářích. Zabývá se nedostatkem, kterými toto schéma disponuje z pohledu domény a představuje schéma projektu FreeIPA, které se tyto nedostatky snaží řešit. Dále popisuje klientského démona SSSD, který je nezbytný pro využití tohoto schématu s programem `sudo`.

2.1 Sudo

Pomocí programu `sudo` má administrátor možnost delegovat oprávnění správce ostatním uživatelům bez nutnosti sdílení hesla správce. Umožňuje uživateli operačního systému spustit jeden příkaz jako jiný uživatel. Ve většině případů je tímto uživatelem právě správce linuxového systému, tj. uživatel `root`. Tedy uživatel, který má nejvyšší oprávnění. Jestliže uživatel vyvolá nějaký příkaz za pomoci programu `sudo`, pak není vyzván k zadání hesla správce systému, ale k zadání hesla daného uživatele. [1, Sekce 4.4.3.2] Bezpečnostní politiky, kterými se `sudo` řídí, se nazývají `sudo` pravidla. Někdy také označovaná jako *sudoers*. Tyto pravidla se zapisují v následujícím formátu:

```
user host_list = ( user_list ) command_list
```

- `user` – specifikuje uživatele nebo skupinu na kterou bude pravidlo aplikováno
- `host_list` – reprezentuje seznam koncových systému
- `user_list` – (nepovinné) specifikuje pod kterým uživatelem má být příkaz proveden
- `command_list` – seznam povolených/zakázaných příkazů

Jestliže chce správce počítače s doménovým jménem `client.example.cz` dát například uživateli „`xsruba03`“ oprávnění spouštět příkaz `/sbin/fdisk` s právy uživatele `root`, pak musí definovat následující pravidlo:

```
xsruba03 client.example.cz = /sbin/fdisk
```

Sudo pravidla se definují v souboru `/etc/sudoers`. Tento soubor by měl být editován pouze pomocí nástroje **visudo**, který provádí automatickou kontrolu syntaxe. Ve výchozím nastavení se v tomto souboru nachází jediné pravidlo definující práva uživatele root.

```
root ALL = ( ALL ) ALL
```

Toto pravidlo dává uživateli root oprávnění spustit jakýkoliv příkaz, jako jakýkoliv uživatel na kterémkoliv systému, kde je toto pravidlo definováno.

2.1.1 Distribuce sudo pravidel

V rozsáhlejších sítích má administrátor na starost více než jednu koncovou stanici. Každou stanici může použít více než jeden uživatel, který může potřebovat provést úlohu, pro kterou potřebuje vyšší oprávnění. Proto by chtěl správce distribuovat sudo pravidla mezi více počítačů. Sudo ovšem nemá nativní způsob jak tyto pravidla distribuovat mezi více počítačů [2, Kapitola 20]. Spravovat tyto pravidla ručně na všech počítačích, které administrátor spravuje, by bylo ovšem velice pracné a časově náročné. Otázkou tedy zůstává jak tyto pravidla šířit mezi více počítačů. Existuje několik způsobů jak toho docílit.

1. Ručně distribuovat tyto pravidla mezi více systému za použití standardních linuxových nástrojů jako jsou *cron*, *scp*, *rsync*, Tento přístup by ovšem mohl být časově náročný a také by nemusel být spolehlivý.
2. Použít speciální nástroje jako je například *Puppet*¹, který sleduje a automaticky šíří konfigurační soubory.
3. Uložit sudo pravidla do centralizované databáze.

LDAP adresáře² mohou uchovávat různé typy informací a jsou tak používány organizacemi a institucemi k ukládání informací o jejich zaměstnancích, uživateli nebo zařízeních jejich počítačových sítí. Jsou charakterizovány jako „jednou-zapsat-a-mnohokrát-číst“³ služba. Jsou optimalizovány pro rychlé čtení a vyhledávání, protože předpokládají, že budou uchovávat informace, které nebudou příliš často modifikovány. [3] Sudo pravidla jsou většinou jednou definována správcem systému a mnohokrát použita uživateli. Uložení sudo pravidel do LDAP adresáře je tedy velice výhodné a nabízí následující výhody:

1. Jestliže jsou sudo pravidla centralizována, pak se správce systému nemusí starat o jejich distribuci. Spravuje pouze jediný soubor se sudo pravidly.
2. Vyhledávání sudo pravidla v LDAP adresáři je rychlejší. Při použití lokálních sudoers⁴ musí sudo přečíst celý sudoer soubor. Při uložení pravidel v LDAP adresáři je potřeba pouze několik LDAP dotazů. [4]
3. Jestliže udělá správce v sudoers souboru chybu, pak se program sudo nespustí. Do LDAP adresáře není možné uložit data, která nesplňují syntaxi daného LDAP sudo schématu. Správná syntaxe je tedy zaručena. Ovšem stále je možné udělat chybu v uživatelském jménu, příkazu nebo názvu koncového systému.

¹<http://puppetlabs.com>

²Adresář, ke kterému se přistupuje pomocí LDAP protokolu.

³write-once-read-many-times

⁴tj. když jsou sudo pravidla definována v lokální `/etc/sudoers` souboru

2.1.2 Nativní LDAP sudo schéma

Sudo má vlastní podporu pro uložení sudo pravidel do LDAP adresáře. Definuje také schéma, které je nutno dodržet. Třída `sudoRole`, která specifikuje sudo pravidlo vypadá následovně:

```
objectclass (
  1.3.6.1.4.1.15953.9.2.1
  NAME 'sudoRole' SUP top STRUCTURAL
  DESC 'Sudoer Entries'
  MUST ( cn )
  MAY ( sudoUser $ sudoHost $ sudoCommand $ sudoRunAs $
        sudoRunAsUser $ sudoRunAsGroup $ sudoOption $
        sudoNotBefore $ sudoNotAfter $ sudoOrder $ description
  )
)
```

Atribut `sudoUser` specifikuje uživatele na kterého bude pravidlo aplikováno. Uživatele je možno specifikovat několika způsoby, které popisuje tabulka 2.1. Sudo pravidlo je také možné aplikovat na veškeré uživatele, čehož je možno docílit použitím hodnoty `ALL`.

Možná hodnota atributu	Příklad
uživatelské jméno	<code>xsruba03</code>
<code>uid</code> ⁵	<code>#9843</code>
skupina uživatelů	<code>%3bit</code>
<code>gid</code> ⁶	<code>%#43</code>
unixová síťová skupina	<code>+admins</code>
non-unixová síťová skupina	<code>%:finance_dp</code>
všichni uživatelé	<code>ALL</code>

Tabulka 2.1: Popis možných hodnot atributu `sudoUser`.

Jestliže víme na koho bude pravidlo aplikováno, musíme dále specifikovat na kterých systémech bude toho pravidlo platné. To specifikuje atribut `sudoHost`, jehož možné hodnoty uvádí tabulka 2.2.

Možná hodnota atributu	Příklad
jméno počítače	<code>client.example.cz</code>
IP adresa	<code>fe80::8a9f:faff:fe0c:b989</code>
adresa sítě	<code>192.168.1.0/24</code>
síťová skupina	<code>+servers</code>
kterýkoliv počítač	<code>ALL</code>

Tabulka 2.2: Popis možných hodnot atributu `sudoHost`.

Posledním atributem, jehož možné hodnoty popisuje tabulka 2.3, pro sestavení sudo pravidla je atribut `sudoCommand`. Ten specifikuje, který unixový příkaz má uživatel povolen/zakázán spouštět. Je také možné specifikovat konkrétní parametry daného příkazu.

Možná hodnota atributu	Popis
povolený příkazzakázaný příkaz	blkid /dev/sda1
zakázaný příkaz	!blkid
všechny příkazy	ALL

Tabulka 2.3: Tabulka popisující možné hodnoty atributu sudoCommand.

Sudo příkaz je také možné spustit jako jiný uživatel než root. Specifikovat uživatele popř. skupinu pod kterou bude uživatel moct daný příkaz provést specifikují atributy `sudoRunAsUser` a `sudoRunAsGroup`. Ve starších verzích programu sudo byl také používán atribut `sudoRunAs`. Ten už se dnes ovšem nedoporučuje používat a považuje se jako „zavržený“⁷.

K sudo pravidlu je také možné specifikovat různé volby, které například určují jak bude vypadat řetězec, který požádá uživatele o zadání hesla. Specifikovat zda bude heslo vůbec požadováno a mnoho dalších. Všechny tyto volby je možné definovat pomocí atributu `sudoOption` [5, Sekce SUDOERS OPTIONS].

Schéma také definuje atributy `sudoNotBefore` a `sudoNotAfter`, které je možno použít pro časově závislá pravidla. Jelikož dále diskutovaný FreeIPA server řeší vypršení platnosti pravidel jiným způsobem, viz. USN plugin v sekci 2.2.1, nebudeme se těmito atributy dále zabývat.

Posledním definovaným atributem je atribut `sudoOrder`. Ten představuje číselnou hodnotu, která je použita v situaci, kdy bude možno aplikovat více než jedno pravidlo. Vždy bude vybrán záznam s větší hodnotou tohoto atributu. To odráží chování „poslední shody“ lokálního sudoers souboru. Předpokládejme, že soubor `/etc/sudoers` obsahuje pouze následující dvě pravidla:

```
xsruba03 ALL=NOPASSWD: /sbin/blkid /dev/sda1
xsruba03 ALL=NOPASSWD: !/sbin/blkid /dev/sda1
```

V tomto případě uživatel „xsruba03“ nebude mít oprávnění spustit příkaz `blkid`. Jestliže ovšem prohodíme tyto pravidla, pak uživatel **bude mít** oprávnění tento příkaz spustit. Pořadí, v kterém jsou sudo pravidla definována, má tedy výrazný vliv na chování programu sudo. LDAP protokol ovšem negarantuje pořadí ve kterém jsou přijaty jednotlivé záznamy, tj. sudo pravidla [6][3, Kapitola 3, Sekce Maintaining Order]. Vychází to z předpokladu, že jak záznamy, tak jednotlivé atributy jsou definovány jako množina. Proto bylo nutné definovat atribut pomocí kterého je možné řadit jednotlivá pravidla.

Záznam ekvivalentního suda pravidla, pro pravidlo 2.1, by v LDAP adresáři vypadal tak, jak jej popisuje obrázek 2.1.

Detailní popis nativního LDAP SUDO schématu je možné nalézt v manuálových stránkách `sudoers.ldap` nebo v oficiálním manuálu [4].

2.1.3 Integrace identit a politik

Pod pojmem *identita* je možno si představit objekt, u kterého nás zajímá jeho jednoznačná identifikace. V linuxovém prostředí tedy typicky například uživatel. Většina administrátorů

⁷deprecated

Záznam sudo pravidla na LDAP serveru

```
dn: cn=rule1,ou=SUDOers,$DC
cn: rule1
description: Simple rule allowing user xsruba03 to run fdisk command.
sudoUser xsruba03
sudoHost client.example.cz
sudoCommand /sbin/fdisk
```

Obrázek 2.1: Příklad záznamu sudo v LDAP adresáři.

spravujících prostředí o desítkách a více uživatelů chce spravovat identity centrálně. LDAP adresáře jsou pro tento účel tedy velice využívány. Například ve Windows prostředích je dnes rozšířeno řešení *Active Directory* nebo *FreeIPA* v linuxových prostředích. Na tyto servery je tedy možné nativní LDAP sudo schéma nahrát a začít tak sudo pravidla spravovat centrálně. Přístup ke správě identit a bezpečnostních politik pomocí LDAP adresáře a nativního sudo schématu má ovšem několik nevýhod:

- Nativní LDAP sudo schéma je pevně dané a není možné jej modifikovat. Záznamy, které neodpovídají tomuto schématu sudo neumí zpracovat.
- Pravidla je možno definovat pouze pomocí příkazového řádku, popř. pomocí souborů v LDIF⁸ formátu.
- V případě, že se uživatel ocitne bez připojení k serveru, který uchovává sudo pravidla, pak není možné sudo použít (případně lze pracovat pouze s lokálními pravidly definovanými v souboru `/etc/sudoers`).
- Při špatné konfiguraci NSS⁹ může dojít k překrytí uživatele z LDAP adresáře s lokálním uživatelem.

Jako největší nevýhodu lze ovšem považovat nulovou integraci mezi existujícími identitami v adresáři a bezpečnostními politikami. Jestliže se administrátor rozhodne spravovat jak identity tak bezpečnostní politiky těchto identit centrálně, pak by chtěl aby tyto entity byly vzájemně propojeny. Toho ovšem není možné dosáhnout s použitím nativního LDAP sudo schématu. Při použití nativního schématu, se při definici sudo pravidel není možné odkazovat na již administrátorem vytvořené identity¹⁰. Toto je jeden z problémů, které se snaží řešit projekt FreeIPA, kterým se zabývá následující sekce.

2.2 FreeIPA

Kvůli efektivitě a jednoduché správě se IT administrátoři snaží spravovat identity centrálně a spojovat identity s autentizačními a autorizačními politikami. V linuxových prostředích existuje mnoho protokolů pro různé služby, které například definují doménu (NIS¹¹, Kerberos), LDAP¹² pro uchování dat nebo sudo pro správu přístupu. Žádné z těchto služeb ovšem

⁸LDAP Data Interchange Format

⁹Name Service Switch

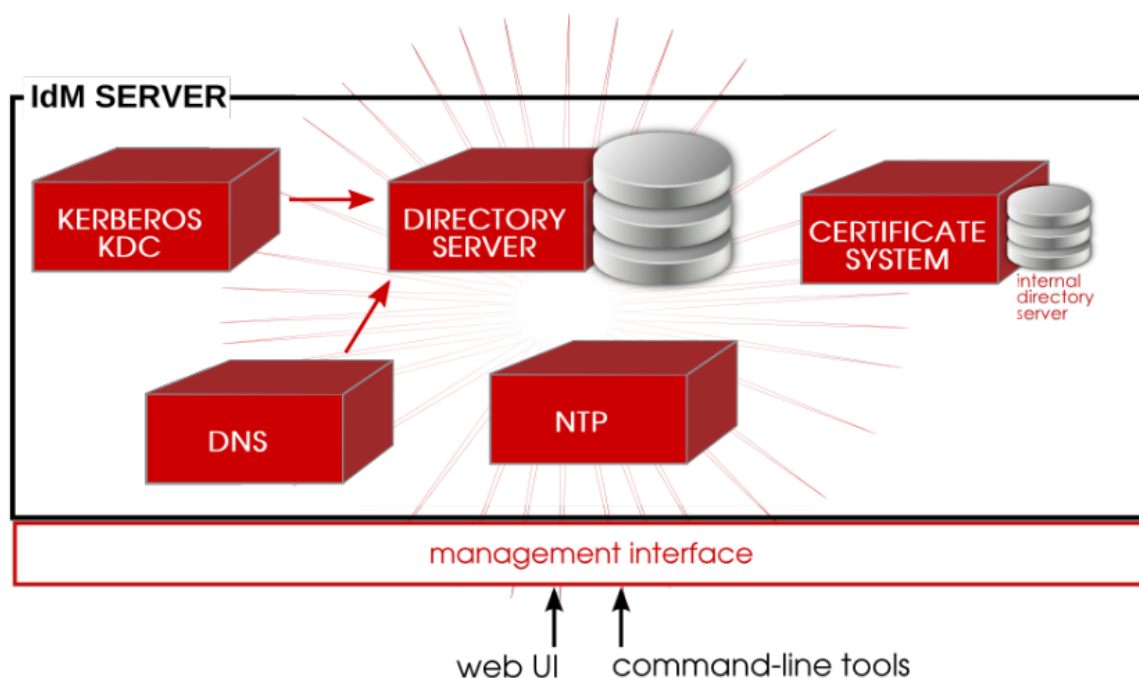
¹⁰například uživatele nebo počítače

¹¹Network Information Service

¹²Lightweight Directory Access Protocol

nejdou nijak propojeny a zároveň všechny musí být spravovány lokálně. Administrátor tedy musí mít potřebné znalosti všech těchto služeb a protokolů aby je dokázal správně používat a dané služby spravovat.

FreeIPA¹³ je projekt, který se zaměřuje na správu identit a jejich politik. Je postaven nad existujícími nativními linuxovými aplikacemi a standardizovanými protokoly. Definuje doménu ve které se vyskytují servery, klienti a vzájemně mezi sebou sdílí centrálně spravované služby jako jsou například Kerberos nebo DNS¹⁴. Je tedy možné říci, že je to v podstatě doménový kontrolér pro linuxové a unixové stanice. Poskytuje jakousi obálku nad standardizovanými síťovými službami jako jsou PAM, LDAP, Kerberos, DNS, NTP nebo certifikační služby. Jeho hlavní úlohou je tedy spravovat všechny tyto služby na jednom místě. IPA navíc umožňuje synchronizaci dat s Active Directory. Neumí ovšem Windows klienty spravovat.



Obrázek 2.2: FreeIPA sjednocuje standardní služby.

Jako úložiště veškerých dat IPA používá LDAP adresář¹⁵. Pro autentizaci je použit protokol Kerberos, který využívá symetrickou kryptografii pro generování *tiketů*, které jsou používány namísto klasických hesel. Jako certifikační autoritu, která zajišťuje vystavování certifikátů serverům, replikám nebo klientům, IPA používá *Dogtag Certificate System*. Služby jako Kerberos jsou závislé na doménových jménech a časových razítkách. Proto IPA slouží také jako DNS a NTP¹⁶ server. [2, Kapitola 1]

Pro cíle této bakalářské práce nás dále bude zajímat pouze správa sudo politik. Tedy jakým způsobem IPA server sudo pravidla uchovává a jak jsou zpracovány na straně klienta.

¹³Free Identity, Policy and Audit, zkráceně IPA

¹⁴Domain Name System

¹⁵The 389 Directory Server, <http://directory.fedoraproject.org>

¹⁶Network Time Protocol

2.2.1 IPA sudo schéma

Sekce 2.1.3 popisovala problémy, které mohou nastat při použití nativního LDAP sudo schématu z pohledu domény. Toto schéma sice může být nahráno na IPA server, ale neposkytuje žádné propojení s již existujícími objekty dané domény. Z těchto důvodů se vývojáři projektu FreeIPA rozhodli vytvořit vlastní schéma pro uchovávání sudo pravidel. Toto schéma umožňuje lepší integraci s již existujícími objekty s konkrétními pravidly. Umožňuje také daleko flexibilnější a jednodušší konfiguraci. Uživatel již tedy není dále specifikován pouze jako řetězec znaků, ale jako odkaz na již existující identitu dané domény.

Schéma definuje novou třídu pro sudo pravidla, jejichž definice vypadá následovně:

```
## Object class for SUDO rules
objectClasses: (
    2.16.840.1.113730.3.8.8.1
    NAME 'ipaSudoRule'
    SUP ipaAssociation
    STRUCTURAL
    MAY ( externalUser $ externalHost $ hostMask $ memberAllowCmd $
        memberDenyCmd $ cmdCategory $ ipaSudoOpt $ ipaSudoRunAs $
        ipaSudoRunAsExtUser $ ipaSudoRunAsUserCategory $
        ipaSudoRunAsGroup $ ipaSudoRunAsExtGroup $
        ipaSudoRunAsGroupCategory $ sudoNotBefore $
        sudoNotAfter $ sudoOrder
    )
    X-ORIGIN 'IPA v2'
)

objectClasses: (
    2.16.840.1.113730.3.8.4.6
    NAME 'ipaAssociation'
    ABSTRACT
    MUST ( ipaUniqueID $ cn )
    MAY ( memberUser $ userCategory $ memberHost $ hostCategory $
        ipaEnabledFlag $ description
    )
    X-ORIGIN 'IPA v2'
)
```

Třída `ipaSudoRule` dědí atributy třídy `ipaAssociation`. Každý záznam, popisující konkrétní sudo pravidlo, obsahuje jedinečné ID (`ipaUniqueID`), své jméno (`cn`) a dále může obsahovat atributy specifikující samotné pravidlo.

Obecně v záznamech sudo pravidel na IPA serveru platí, že `member*` atributy¹⁷ obsahují DN¹⁸ již existujících objektů IPA domény, zatímco `external*`¹⁹ atributy specifikují objekty, které jsou definovány mimo tuto doménu. Speciální případy, kdy je například sudo pravidlo aplikovatelné na kteréhokoliv uživatele nebo počítač specifikují `*Category`²⁰ atributy.

¹⁷tj. například `memberUser`, `memberAllowCmd`, ...

¹⁸Distinguished Name

¹⁹tj. například `externalUser`, `externalHost`, ...

²⁰tj. například `userCategory`, `cmdCategory`, ...

Uživatele, na kterého bude pravidlo aplikovatelné, je možné specifikovat pomocí tří atributů. Příklady hodnot těchto atributů popisuje tabulka 2.4. Jak je možné odvodit z prvního řádku této tabulky, záznamy uživatelů IPA domény se nacházejí v kontejneru `cn=users,cn=accounts,$DC`. Pomocí `externalUser` atributu je také možné vytvořit sudo pravidlo aplikovatelné na uživatele, který není členem IPA domény. Tento uživatel ovšem musí být členem jiné domény²¹ a mezi touto a IPA doménou musí být vytvořena vzájemná důvěra, tzv. *trust*. Popis, jak toto propojení mezi doménami funguje nebo jak jej vytvořit, je ovšem nad rámec této bakalářské práce.

Jméno atributu	Hodnota atributu
<code>memberUser</code>	<code>uid=xsruba03,cn=users,cn=accounts,\$DC</code> ²²
<code>userCategory</code>	<code>all</code>
<code>externalUser</code>	<code>xsruba04</code>

Tabulka 2.4: Atributy specifikující uživatele sudo pravidla.

Identitu, pod kterou bude příkaz spuštěn je možné specifikovat pomocí `ipaSudoRunAs*` atributů. Zde je možné specifikovat jak konkrétní identitu, tak i skupinu identit.

Stejným způsobem je poté pomocí atributů `memberHost`, `hostCategory` a `externalHost` definován počítač na který bude pravidlo aplikováno. Zde je navíc definován atribut `hostMask` pomocí kterého je možné specifikovat počítač, popř. skupinu počítačů, pomocí IP adresy nebo adresy sítě. Tento atribut ovšem v praxi není využíván.

Poslední množinou, kterou je nutno specifikovat pro vytvoření kompletního pravidla, jsou příkazy. Zde popsané schéma přináší novou vlastnost a tou jsou **skupiny příkazů**. Jak záznamy příkazů, tak záznamy skupin příkazů jsou v samostatných kontejnerech. Jsou také definovány pomocí jiných tříd. Atributy a příklad jejich možných hodnot popisuje tabulka 2.5. Záznamy pro sudo příkazy se nacházejí v kontejneru `cn=sudocmds,cn=sudo,$DC`.

Jméno atributu	Hodnota atributu
<code>memberAllowCmd</code>	<code>cn=dics,cn=sudocmdgroups,cn=sudo,\$DC</code>
<code>memberDenyCmd</code>	<code>ipaUniqueID=41e9a39c,cn=sudocmds,cn=sudo,\$DC</code>
<code>cmdCategory</code>	<code>all</code>

Tabulka 2.5: Atributy specifikující sudo příkaz.

Kromě skupin příkazů přináší nové schéma další výhodu a to povolování/zakazování pravidel. Jestliže administrátor spravuje sudo pravidla pomocí LDAP serveru a nativního LDAP sudo schématu. Pak pravidla, která jsou v adresáři definována budou vždy použita. Pokud by chtěl administrátor, například z důvodu testování, nějaké pravidlo dočasně zakázat, musel by jej z adresáře odstranit. Třída `ipaAssociation` definuje atribut `ipaEnableFlag`. Pomocí tohoto atributu je možné libovolné pravidlo dočasně povolit nebo zakázat bez nutnosti jeho odstranění z adresáře. Záznam ekvivalentního suda pravidla pro pravidla 2.1 a 2.1 v novém IPA sudo schématu popisuje obrázek 2.3.

Každý záznam na IPA serveru má také **operační** atribut `entryUSN`²³. Hodnotu tohoto atributu aktualizuje USN plugin při každé změně daného záznamu. Tento plugin tedy po-

²¹ například doména spravována pomocí Active Directory

²³ Entry Update Sequence Number

Záznam sudo pravidla na IPA serveru

```
dn: ipaUniqueID=e6917a9c,cn=sudorules,cn=sudo,$DC
cn: rule1
ipaEnabledFlag: TRUE
ipaUniqueID: e6917a9c
description: Simple rule allowing user xsruba03 to run fdisk command.
memberUser: uid=xsruba03,cn=users,cn=accounts,$DC
memberHost: fqdn=client.example.cz,cn=computers,cn=accounts,$DC
memberAllowCmd: ipaUniqueID=41e9a39c,cn=sudocmds,cn=sudo,$DC
```

Záznam sudo příkazu pro dané pravidlo

```
dn: ipaUniqueID=41e9a39c,cn=sudocmds,cn=sudo,$DC
description: Manipulate disk partiton table.
sudoCmd: /sbin/fdisk
ipaUniqueID: 41e9a39c
memberOf: cn=dics,cn=sudocmdgroups,cn=sudo,dc=example,$DC
```

Obrázek 2.3: Příklad záznamu sudo pravidla na IPA serveru.

skytuje způsob, který umožňuje informovat IPA klienty o **modifikaci** jakéhokoliv záznamu [7, Sekce 3.4].

LDAP schémata, která používá FreeIPA server je možné nalézt v adresáři `/etc/dirsrv/slapd-instance_name/`. Detailní popis tříd a atributů pro definici sudo pravidel na IPA serveru je možné nalézt v souboru `65sudo.ldif`. Schémata, která používá FreeIPA server je možné najít také na příloženém CD, viz. Příloha A.

2.2.2 Definice sudo pravidel

Další výhodou, kterou přináší FreeIPA je snadnější definice pravidel. Sudo pravidla na IPA serveru je možné definovat dvěma způsoby. Jednak pomocí **webového rozhraní** nebo pomocí utilit příkazového řádku `ipa sudorule*`. Podrobnější popis s příklady jak definovat pravidla ve webovém rozhraní nebo pomocí příkazového řádku je možné nalézt například v oficiální dokumentaci²⁴. Při správě pravidel v LDAP adresáři bylo nutné pravidla vytvářet textově a ručně je do adresáře přidávat. Webové rozhraní zde tedy administrátorovi velice zjednodušuje práci.

2.3 System Security Services Daemon

SSSD se skládá z několika komponent (démonů), které zajišťují přístup ke vzdáleným adresářům a autentizačním mechanismům jako jsou LDAP, Kerberos nebo FreeIPA skrze framework, který poskytuje cachování a offline podporu.

Předpokládejme následující případ, kdy se uživatel připojuje do firemní sítě, kde jsou centrálně spravovány identity. Jestliže je klient připojen k síti, pak se při přihlášení ověří jeho identita pomocí vzdáleného serveru. Dostane-li se klient do situace kdy není připojen k síti, tak nastává problém, protože se klient nebude moci přihlásit. V takových případech to klient musel řešit separátním účtem, který mu umožnil přístup do systému. SSSD umožňuje

²⁴Red Hat Enterprise Linux 6 Identity Management Guide

cachovat informace o identitách a jejich autorizaci. Pokud se klient bude chtít přihlásit bez připojení k síti, pak jeho identita není ověřena vůči vzdálenému serveru, ale oproti informacím uloženým v cache SSSD. [8, Sekce 8.2]

SSSD také podporuje více domén, což znamená, že může být počítač připojen k více doménám zároveň. Ovšem pro cíle této bakalářské práce nás dále bude SSSD zajímat pouze z pohledu programu sudo. Tedy jakým způsobem SSSD tyto pravidla zpracovává než jsou předány programu sudo.

Jestliže se administrátor rozhodne spravovat sudo politiky pomocí IPA serveru, pak u všech klientů musí být démon SSSD dostupný. Použití SSSD pro přístup k sudo politikám, uložených na vzdáleném serveru, má oproti přístupu pomocí ldap pluginu²⁵ následující hlavní výhody:

- **offline podpora** - SSSD si ukládá všechna přijatá pravidla do své cache paměti na disku. Jestliže dojde k odpojení klienta od sítě, pak může stále používat tyto uložená pravidla.
- **lepší výkon** - každé zavolání sudo utility způsobí jeden nebo více LDAP dotazů na server, kde jsou daná pravidla uložena. V kombinaci s pomalou sítí nebo zatíženým serverem to může znamenat značné zpomalení v případech, kdy uživatel potřebuje použít program sudo vícekrát za sebou. SSSD si uloží pravidla do cache paměti a při spuštění programu sudo se pravidla hledají nejprve v cache paměti. Další zpomalením u ldap pluginu může být situace, kdy používá sudo více uživatelů najednou. V takovém případě se vytváří několik LDAP spojení. Zatímco SSSD používá pouze jediné spojení s LDAP serverem

SSSD také podporuje nativní LDAP sudo schéma. Je tedy možné jej nastavit, tak aby získával sudo pravidla z LDAP serveru. V takovém případě získá uživatel jednak offline podporu, ale také cachování těchto pravidel. Konfigurace SSSD pro tento účel je popsána v manuálové stránce `sssd-sudo` a některé konfigurační volby také v `sssd-ldap`.

2.3.1 Aktualizace sudo pravidel v cache paměti

SSSD provádí následující tři typy aktualizací sudo pravidel ve své cache paměti:

Průběžné aktualizace

Periodicky stahují pravidla, která jsou na serveru nově přidány nebo byly od poslední aktualizace modifikovány. V manuálových stránkách a v kódu SSSD je možné tento typ aktualizace vyhledat jako „*smart refresh*“.

Úplná aktualizace

Provede smazání všech pravidel z cache paměti a stažení všech pravidel ze serveru. Tento typ aktualizace se neprovádí velmi často, protože při velkém množství pravidel generuje velký síťový provoz. Provádí se tedy pouze při spuštění SSSD nebo při detekci změny pravidel na serveru. V manuálových stránkách a v kódu SSSD je možné tento typ aktualizace najít jako „*full refresh*“.

²⁵ Jedná se o plugin, který dodává sudo. Nezaměňovat tedy s ldap pluginem, který používá SUDO provider démona SSSD.

Aktualizace pravidel

Je provedena při každém spuštění programu sudo. Zajistí aby uživatel nedostal větší oprávnění než je definováno. Tento typ aktualizace stáhne ze serveru pouze ty pravidla, která v cache paměti nadále nejsou platná²⁶. Jestliže se některé pravidlo na serveru nenachází, indikuje to změnu na serveru a je provedena úplná aktualizace pravidel. V manuálních stránkách a v kódu SSSD je možné tento typ aktualizace najít jako „*rules refresh*“.

²⁶Čas po kterém pravidla v cache paměti stanou neplatná je možno nastavit v `sssd.conf` pomocí volby `entry_cache_sudo_timeout`, viz. manuálová stránka `sssd.conf`

Kapitola 3

SSSD a SUDO provider

Tato kapitola popisuje vnitřní architekturu démona SSSD se zaměřením na sudo providera a pluginy, které má k dispozici. Tento popis byl sestaven na základě experimentování a čtení zdrojových kódů. Popis byl nezbytný pro úplné pochopení způsobu, jakým SSSD sudo pravidla zpracovává. V poslední sekci je také popsán hlavní problém, kterým se tato práce zabývá.

3.1 Knihovny třetích stran

SSSD používá pro alokaci dynamické paměti hierarchický alokátor *talloc*^[9] namísto standardního systémového volání *malloc*. Nepoužívá imperativní ani OOP¹ paradigma, ale událostmi řízené paradigma² programování.

U imperativního nebo OOP paradigmatu programování se při provádění programu postupuje od shora dolů. To ovšem u událostmi řízeného paradigmatu neplatí. Programy reagují na události a tyto události poté určují, která část programu bude vykonávána. Takový program se poté nachází ve dvou stavech:

1. čeká na událost
2. provádí obsluhu události

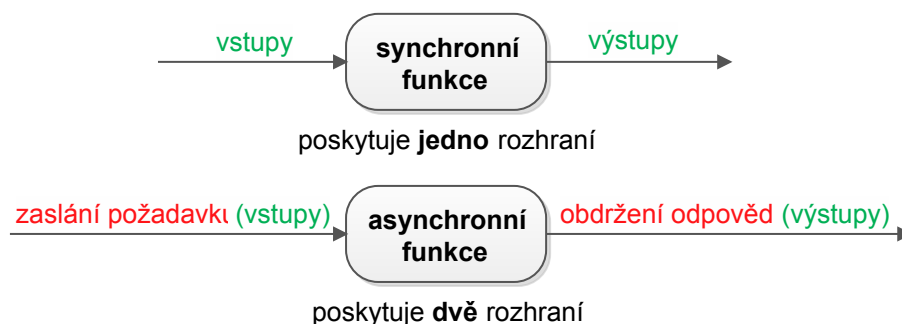
Knihovna *tevent*^[10] realizuje tyto události za pomoci asynchronních funkcí. Synchronní funkce poskytují programátorovi pouze jedno rozhraní, přes které je možno specifikovat vstupní parametry funkce a získat výsledek dané funkce. Naproti tomu asynchronní funkce poskytují rozhraní dvě. Jedno pro předání parametrů funkci a získání výsledků a druhé pro zaslání samotného požadavku a uvědomění programátora o dokončení této asynchronní události. Funkce, která je zavolána jako výsledek o dokončení události se nazývá tzv. *callback*.^[10]

Knihovna *tevent* implementuje tyto asynchronní funkce pomocí tzv. *tevent requests*. Jejich grafické znázornění popisuje schéma 3.2. S tím je také spojena následující konvence:

- S událostí jsou spojeny privátní data, které mají příponu `_state`.
- Funkce, která provádí asynchronní volání má příponu `_send`.

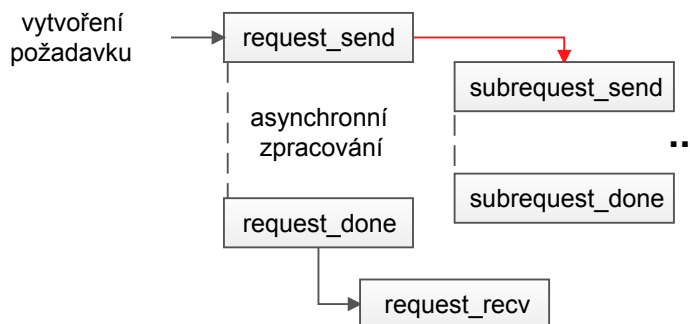
¹Object-oriented programming

²Event-driven Programming Paradigm



Obrázek 3.1: Rozhraní synchronních a asynchronních funkcí.

- Funkce, která bude vyvolána v okamžiku dokončení události má příponu `_done`
 - V této funkci je možné získat výsledky asynchronní operace pomocí volání funkce s příponou `*_recv`.



Obrázek 3.2: Příklad grafického zobrazení asynchronní funkce.

Nejprve je danou událost nutno vytvořit a spojit s ní privátní data. Knihovna `tevent` pro alokaci dynamické paměti používá rovněž knihovnu `talloc`. Asynchronní funkci je možné zavolat pomocí rozhraní „`request_send`“³. Poté probíhá asynchronní provádění programu. V okamžiku kdy bude událost označena jako dokončená, vyvolá se její callback tj. funkce „`request_done`“. V této funkci je možné zpracovat výsledky dané události a následně ji odstranit. Volání asynchronních funkcí je možné do sebe také zanořovat. Jedna asynchronní operace tak může volat jinou atd.

Knihovna `tevent` je také využívána ve spojení s knihovnami `OpenLDAP`⁴ a `DBus`⁵, které obaluje aby bylo možné využít jejich vlastností. Tyto knihovny jsou poté v `SSSD` označovány jako `SDAP` a `SBUS`.

³funkci je možné pojmenovat např. `ldap_query_send`

⁴www.openldap.org

⁵dbus.freedesktop.org

3.2 Architektura SSSD

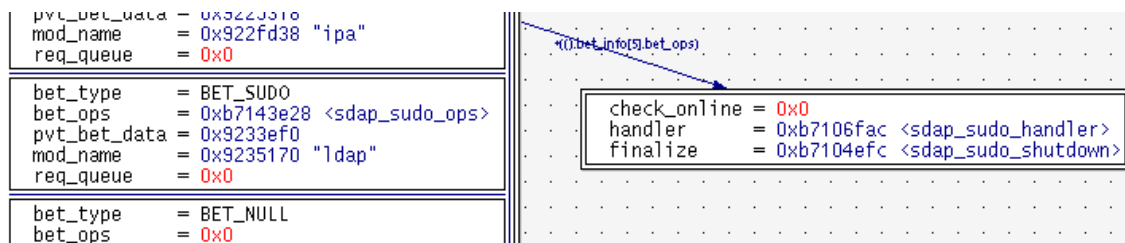
SSSD se skládá z několika komponent (démonů). Hlavním procesem je zde *Monitor*, který je otcem všech ostatních procesů. Stará se o to, aby ostatní procesy zůstaly aktivní, detekuje síťové změny a informuje o nich ostatní procesy.

Další komponentou jsou tzv. *respondeři*. Jsou to procesy, které přijímají požadavky od klientských aplikací⁶ a vracejí odpovědi na tyto požadavky. Smyslem těchto procesů je vrátit, za pomoci cache paměti, co nejrychleji odpověď na dotaz, který jim klientská aplikace zaslala. Proto by měly provádět co nejméně algoritmičky náročných operací a v podstatě pouze číst a předávat data z cache paměti SSSD. Komunikují tedy pouze s cache pamětí nebo poskytovali dat, ale nikdy nekomunikují se vzdáleným serverem. V následujícím textu bude pro každý takový proces používán výraz **responder**.

Veškerou práci spojenou s komunikací se vzdáleným serverem, zpracování výsledků a jejich uložení do cache paměti by měl zajistit konkrétní *provider*. Který provider bude použit pro kterou službu je možné nastavit v konfiguračním souboru `sssd.conf`. Například `id_provider` specifikuje, který provider SSSD použije pro zjišťování informací o identitách. Informace o sudo pravidlech poté poskytuje sudo provider. Každý provider může používat jiný plugin. Například provider identit může použít *ldap plugin* pro přístup k identitám uloženým v LDAP adresáři, *ad plugin* pro identity spravované serverem *Active Directory*. Pro sudo providera je možné použít pluginy *ldap* a *ipa*. Informaci o tom, které pluginy jsou konkrétními providery podporovány, je možné nalézt v manuálové stránce `sssd.conf`. Jestliže mluvíme o LDAP SUDO providerovi, pak máme namysli *ldap plugin*, pomocí kterého přistupuje SUDO provider k sudo politikám na vzdáleném serveru.

S pomocí SSSD může být jedna stanice připojena do více domén zároveň. Pro každou doménu je vytvořen samostatný proces, který danou doménu reprezentuje. Takový proces je nazýván *backend*. Backend používá providery pro komunikaci se vzdálenými servery.

Každý backend má ve svém kontextu⁷ ukazatel na pole `bet_info`, které obsahuje informace o providerech, které daný backend používá. Každá položka tohoto pole je tvořena strukturou `bet_info`. Ta obsahuje např. jméno pluginu, který se má pro daný provider použít, ukazatel na privátní data nebo ukazatel na strukturu `bet_ops`, kde se nachází ukazatel na funkci, kterou volají respondeři, pokud chtějí danému providerovi zaslat nějaký požadavek. Jméno této funkce má v SSSD obecně příponu **handler**⁸ a takto bude označována i v následujícím textu. Položku pole `bet_info` pro LDAP SUDO providera zobrazuje obrázek 3.3.



Obrázek 3.3: Položka pole `bet_info` pro SUDO.

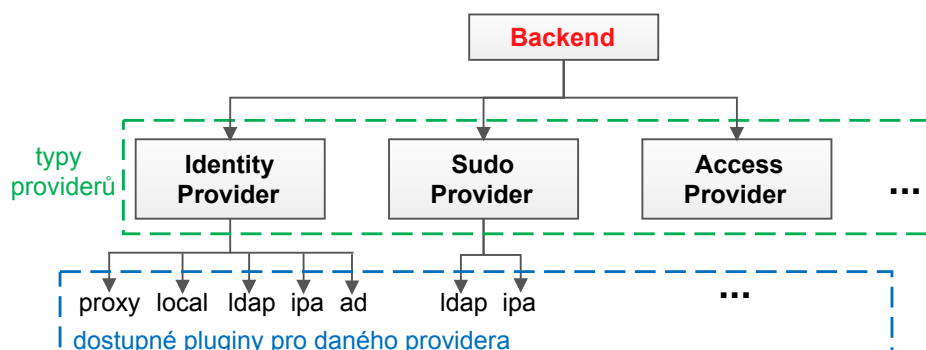
Každý backend také používá svou cache paměť, která je tvořena LDB databází. Do této

⁶např. `sudo`, `id`, `getent`, `ls`, ...

⁷`struct be_ctx`

⁸například `sdap_sudo_handler` je SUDO handler pro LDAP SUDO providera

paměti zapisuje pouze daný backend a responderi z ní mohou data pouze číst. Tato cache paměť se také označuje jako *sysdb*.



Obrázek 3.4: Typy providerů a jejich pluginů.

3.3 SSSD z pohledu programu sudo

Předpokládejme, že jak informace o identitách, tak jejich autentizaci a bezpečnostních politikách jsou uloženy na vzdáleném serveru, ke kterému přistupujeme pomocí démonu SSSD. Běžný uživatel chce zobrazit obsah souboru `/etc/shadow`. K tomu ovšem potřebuje vyšší oprávnění a proto se rozhodne použít program sudo. Tuto situaci demonstruje obrázek 3.5.

Po spuštění programu sudo se nejprve zjistí informace o uživateli, který program sudo vyvolal. Knihovna NSS pošle požadavek o informacích NSS responderu, tj. procesu `sssd_nss`. Ten nejprve zjistí zda se informace o daném uživateli nenacházejí v cache paměti. Jestliže ne, pak požádá backend dané domény o aktualizaci cache paměti. Tuto aktualizaci provede nakonfigurovaný provider identit⁹. Poté musí proběhnout autentizace uživatele. Tu zajistí stejným způsobem PAM¹⁰ responder.

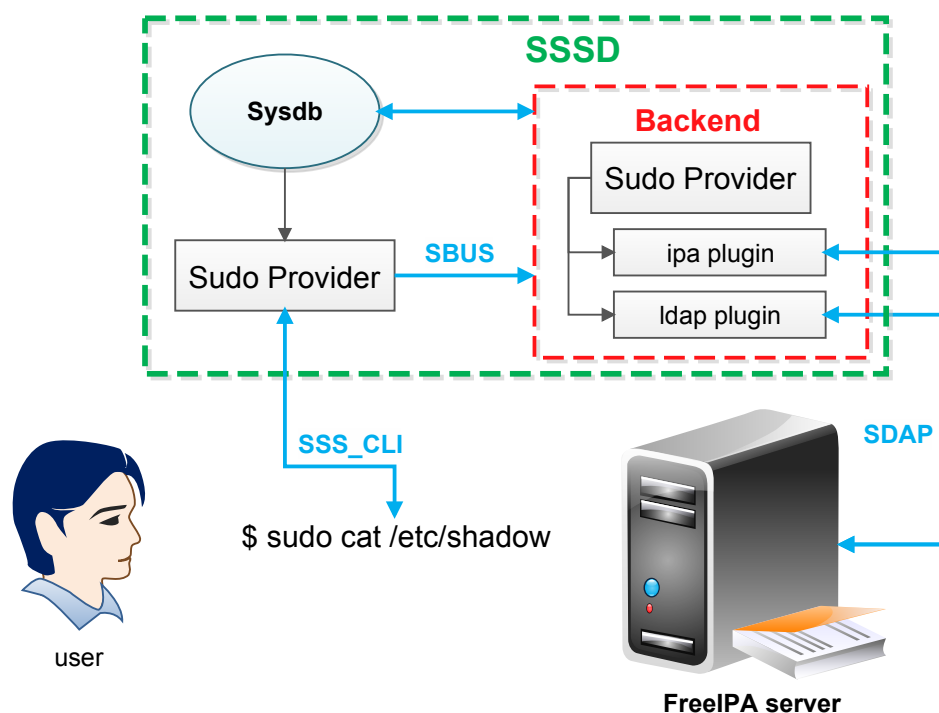
Jestliže autentizace uživatele proběhla úspěšně, pak přichází na řadu sudo responder. Ten hledá nejprve požadované pravidlo v cache paměti. Jestliže se dané pravidlo v `sysdb` nachází a je stále validní, pak nastává tzv. *cache hit*. V tomto případě je pravidlo vráceno programu sudo.

Jestliže hledané pravidlo v cache paměti není validní, pak je provedena jeho aktualizace, tj. ověření zda se na serveru stále nachází. Proběhne také aktualizace všech ostatních pravidel, která již nejsou nadále validní. Aktualizaci `sysdb` provádí sudo provider, který zajistí vyhledání potřebných pravidel na vzdáleném serveru, jejich zpracování a uložení zpět do `sysdb`. Po aktualizaci se SUDO responder opět dotáže cache paměti pro požadované pravidlo.

Jestliže při prvním dotazu do cache paměti není požadované pravidlo nalezeno, pak neprobíhá jeho další vyhledání na vzdáleném serveru. Pokud se ovšem dané pravidlo na serveru opravdu nachází, pak je nutné restartovat démona SSSD nebo počkat na provedení některé z průběžných aktualizací, které jsou průběžně plánovány. Tuto funkcionalitu blíže popisuje sekce 3.4.2.

⁹identification provider, volba `id_provider` v `sssd.conf`

¹⁰Pluggable authentication module



Obrázek 3.5: Architektura SSSD.

3.3.1 SDAP dotaz a mapování atributů

Jestliže se administrátor rozhodne uložit sudo pravidla do LDAP adresáře, tj. ne na server FreeIPA, musí dodržet sudem definované schéma, které bylo popsáno v sekci 2.1.2. Tedy přesná jména atributů a formát hodnot. Pravidla v jiném formátu sudo zpracovat neumí¹¹. S pomocí SSSD je možné ovlivnit alespoň názvy atributů pod kterými jsou sudo pravidla uložena. Toho je docíleno za použití map.

Mapy se používají k mapování hodnot voleb z konfiguračního souboru SSSD¹², pro výběr atributů při sestavování LDAP dotazu a pro definování jmen atributů pod kterými budou výsledky dotazů uloženy v sysdb. Výchozí mapy jsou definovány v hlavičkovém souboru `providers/ldap/ldap_opts.h`. Zde je také definována výchozí mapa, kterou LDAP SUDO Provider používá při stahování sudo pravidel z LDAP serveru. Mapy používané při komunikaci s IPA serverem se nacházejí v souboru `providers/ipa/ipa_opts.h`.

Většina map je definována jako pole následujících struktur.

```
struct sdap_attr_map {
    const char *opt_name;
    const char *def_name;
    const char *sys_name;
    char *name;
};
```

¹¹Neumí zpracovat ani pravidla v IPA SUDO schématu, který používá IPA server, viz. Sekce 3.5

¹²Ve výchozím nastavení se nachází v `/etc/sss/sss.conf`

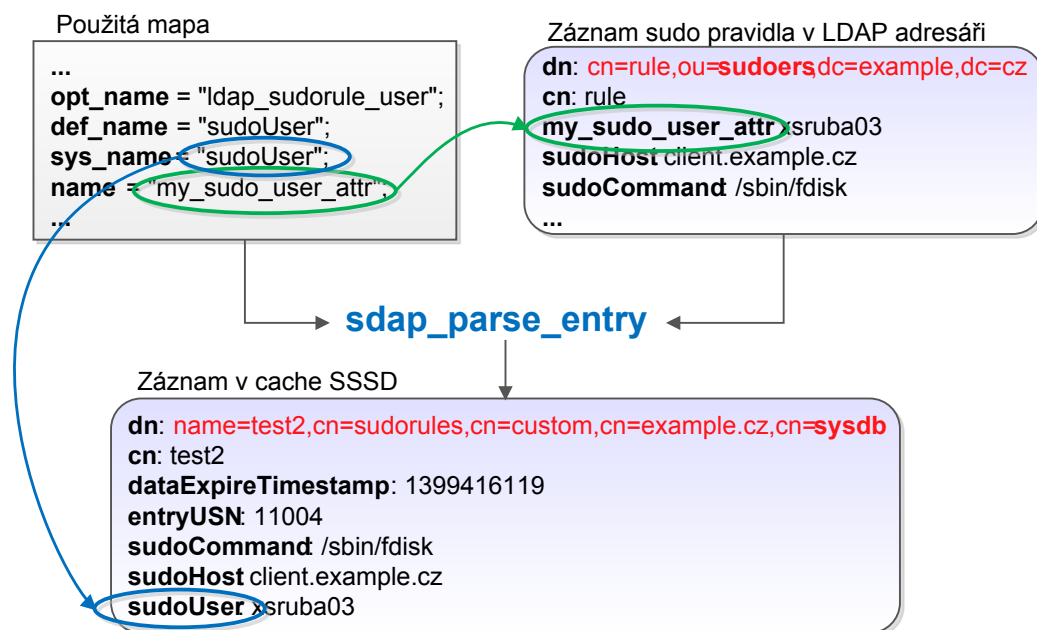
Mapu je možné vytvořit pomocí funkce `sdap_get_map()`. Jako jeden z parametrů je nutné specifikovat výchozí mapu, ze které bude mapa vytvořena. V proměnných `opt_name` jsou uloženy jména voleb z konfiguračního souboru, jejichž hodnoty se uloží do proměnných `name`, pokud byly v `sssd.conf` specifikovány. Jestliže se daná volba v konfiguračním souboru nenachází, pak je pro proměnnou `name` použita výchozí hodnota tj. hodnota proměnné `def_name`, která bude specifikována ve výchozí mapě. Hodnoty proměnných `name` jsou použity při vytváření atributů, které se mají vyhledat při LDAP dotazech. Proměnná `sys_name` je poté použita pro jméno atributu, pod kterým bude uložena hodnota, která se nachází na serveru pod hledaným atributem, v `sysdb`. Ukázka z výchozí mapy kterou používá sudo vypadá následovně:

```
{"ldap_sudorule_user", "sudoUser", "sudoUser", NULL},
```

Z této ukázky je možno odvodit, že jestliže není v `sssd.conf` zadaná volba `ldap_sudorule_user`. Pak bude při sestavování LDAP dotazu na sudo pravidlo požadován atribut `sudoUser` a do `sysdb` bude jeho hodnota rovněž uložena pod jménem atributu `sudoUser`.

Uvažujme následující příklad, který demonstruje schéma 3.6. V `sssd.conf` se nachází následující volba:

```
ldap_sudorule_user = my_sudo_user_attr
```



Obrázek 3.6: Ukázka mapování atributů z `sssd.conf` do `sysdb`.

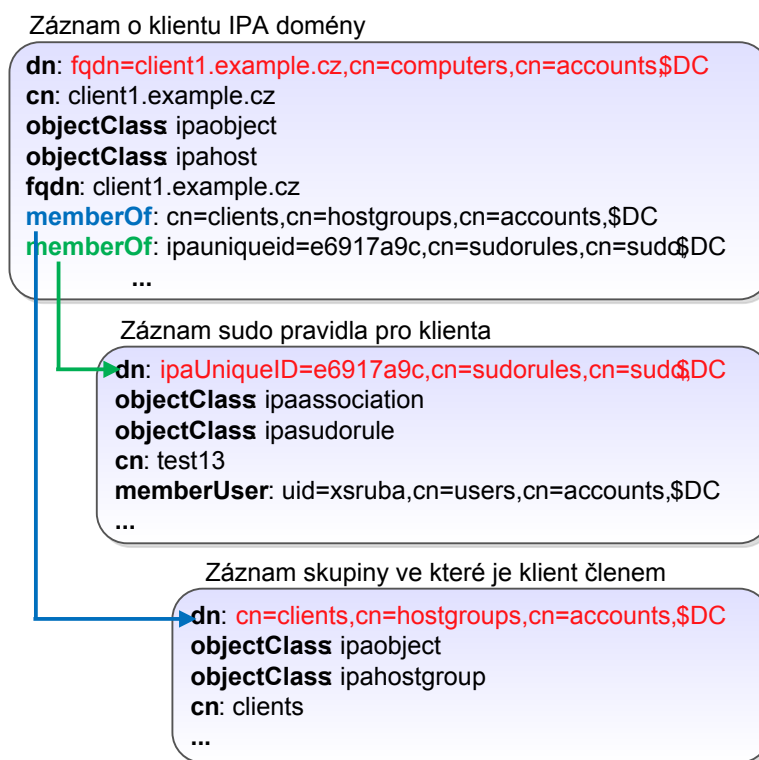
Jméno uživatele, na kterého bude aplikováno sudo pravidlo, bude hledán pod atributem `my_sudo_user_attr` a jeho hodnota bude do `sysdb` uložena pod atribut `sudoUser`.

Asynchronní volání `ldap_search_ext()` samozřejmě neumožňuje žádnou mapu specifikovat. SDAP definuje vlastní asynchronní rozhraní `sdap_get_generic_ext_send()`, které

s těmito mapami pracuje. Toto rozhraní také provádí zpracování výsledků, které vrací funkce knihovny OpenLDAP, a vrací je jako ldb elementy. Zde je nezbytné zmínit, že jako první položkou v mapě musí být **vždy** uvedena třída. Přijaté záznamy, které neodpovídají této třídě nebudou předány jako výsledek! Taktéž v mapě není možné specifikovat více než jednu třídu! Výsledky `ldap_search_ext` a `sdap_get_generic_ext_send`, který je postaven nad OpenLDAP, tedy nemusejí být vždy ekvivalentní.

SDAP ještě nabízí druhé rozhraní a to `sdap_deref_search_send`. Pomocí kterého je možné získat záznam a také všechny záznamy na které je ze záznamu odkazováno pomocí DN. U tohoto dotazu ovšem není možné specifikovat filtr, jelikož mohou provést dereferenci atributů pouze **jednoho** záznamu! Obrázek 3.7 zobrazuje záznamy, které by byly vráceny po zaslání dereferenčního dotazu s těmito parametry:

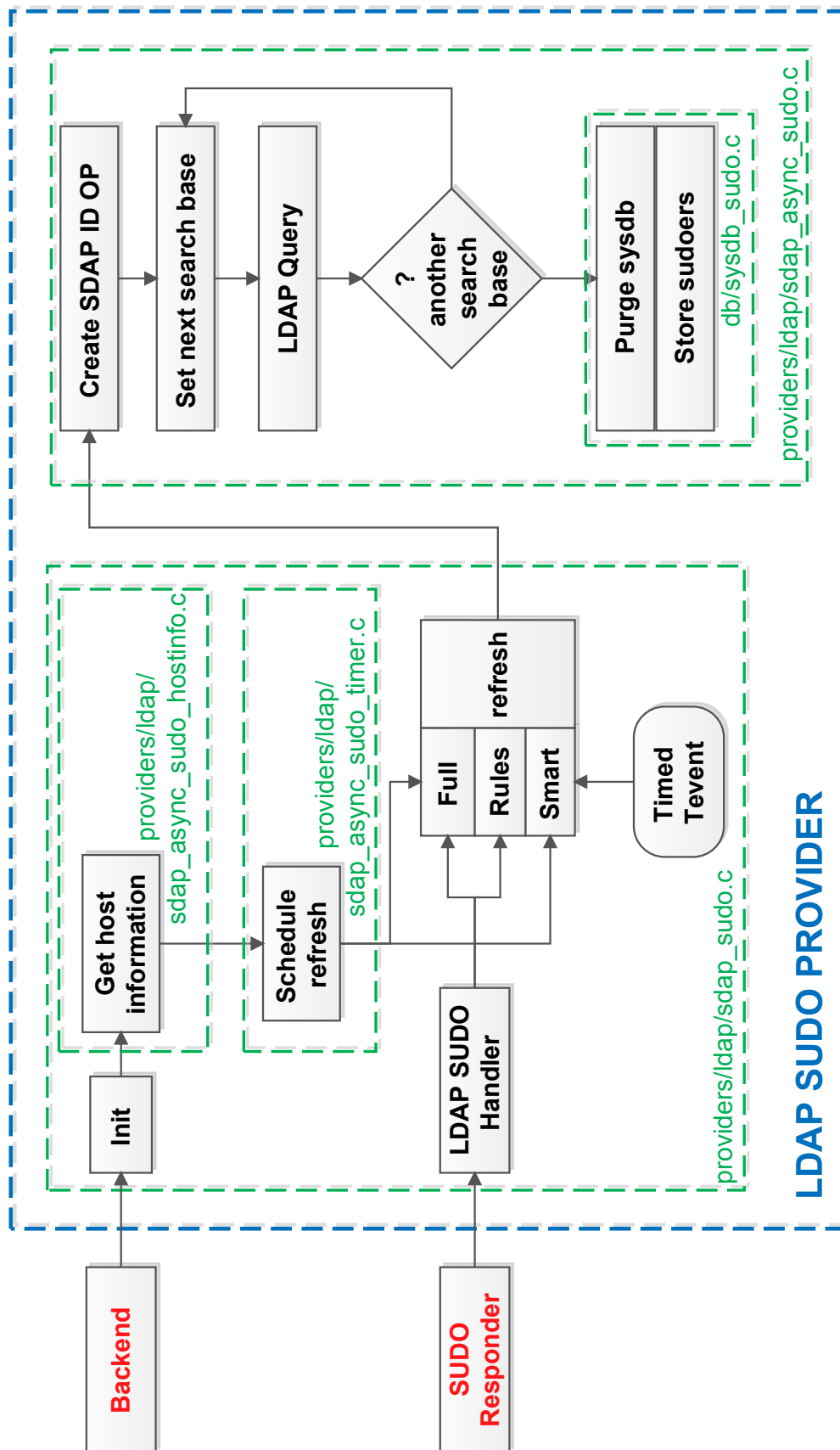
prohledávaná oblast: `fqdn=client1.example.cz,cn=computers,cn=accounts,$DC`
odkazované atributy: `memberOf`



Obrázek 3.7: Ukázka dereferenčního dotazu.

3.4 LDAP SUDO Provider

Tento provider provádí veškerou práci při komunikaci s LDAP serverem na kterém jsou uložena sudo pravidla v nativním LDAP SUDO schématu. Tedy stažení, zpracování a uložení těchto pravidel do sysdb. Skládá se z několika modulů jejichž celkovou funkcionalitu popisuje schéma 3.8.



Obrázek 3.8: Schéma událostí asynchronního modulu `providers/ldap/sdap_async_sudo.c`.

3.4.1 Inicializace

Inicializaci zajišťuje modul `providers/ldap/sdap_sudo.c` a probíhají při ní následující úlohy:

- alokace `sudo_ctx` kontextu, který je zároveň privátními daty LDAP SUDO Providera
- nastavení handleru pro SUDO respodera, tj. vytvoření struktury `bet_ops`
- vytvoření mapy z výchozí `native_sudorule_map` mapy
- získání všech jmen a IP adres daného počítače
- nastavení plánování aktualizací sudo pravidel

Inicializaci provádí funkce `sdap_sudo_init()`. Vytváří se zde sudo mapa, která je použita v SDAP dotazech. Jako výchozí mapa je použita `native_sudorule_map` a při vytváření se také zohledňují volby zadané v konfiguračním souboru SSSD. Ukazatel na vytvořenou mapu je uložen v `id_ctx`¹³. Vytvoření a použití map je blíže popsáno v sekci 3.3.1.

Jména počítače, pro která budou stahována aplikovatelná sudo pravidla, jsou získávána automaticky pomocí systémového volání `gethostname()`. Jestliže je již jméno počítače specifikováno jako FQDN¹⁴. Pak již další vyhledávání neprobíhá. V opačném případě se LDAP plugin pokusí získat FQDN pomocí asynchronního volání `resolv_gethostbyname_send()`. I když jsou IP adresy a jméno počítače získávána automaticky, je možné je specifikovat přímo v `sssd.conf` pod volbami `ldap_sudo_hostnames` a `ldap_sudo_ip`. Jejich hodnoty jsou poté zohledněny při sestavování filtrů pro LDAP dotazy. Použitím těchto voleb je poté možné stahovat i taková sudo pravidla, která nejsou aplikovatelná na klientský počítač¹⁵.

3.4.2 Plánování aktualizací

Součástí inicializace je také nastavení plánování průběžných a úplných aktualizací. Jak často budou tyto aktualizace prováděny je možné ovlivnit v `sssd.conf`¹⁶.

Při spouštění SSSD by mohla nastat situace, kdy stihne uživatel spustit program sudo ještě před provedením aktualizace. V takovém případě by sudo nefungovalo správně, jelikož by se v sysdb nenacházela žádná pravidla.¹⁷ Proto je při každém spuštění SSSD provedena kompletní aktualizace sudo pravidel.

Plánování aktualizací je realizováno pomocí časových událostí knihovny `tevent` a implementační detaily je možné nalézt ve funkci `sdap_sudo_setup_periodical_refresh()`.

3.4.3 Aktualizace sudo pravidel

Všechny tři typy aktualizací využívají modul `providers/ldap/sdap_async_sudo.c`, který provádí samotné stažení a uložení sudo pravidel do sysdb. Funkcionalitu tohoto modulu je možné ovlivnit pomocí parametrů, které jsou mu předány. Parametry mohou být například filtry, které se mají použít. Předpřipravení parametrů pro konkrétní aktualizace provádějí následující funkce:

¹³Kontext providera identit (angl. Context of Identity Provider)

¹⁴Fully Qualified Domain Name

¹⁵Používáno převážně pro testování.

¹⁶Volby `ldap_sudo_full_refresh_interval` a `ldap_sudo_smart_refresh_interval`

¹⁷za předpokladu, že se na serveru nějaká pravidla nacházejí

- `sdap_sudo_full_refresh_send()` pro kompletní aktualizaci
- `sdap_sudo_smart_refresh_send()` pro průběžné aktualizace
- `sdap_sudo_rules_refresh_send()` pro aktualizaci pravidel

Úplná aktualizace

Pro úplnou aktualizaci sudo pravidel je použit následující LDAP filter. Tento i všechny následující filtry se řídí syntaxí specifikovanou LDAP protokolem [11, RFC2254]. Jsou pouze doplněny bílými znaky pro lepší čitelnost.

LDAP filter :

```
( & ( objectClass=sudoRole )
  ( | ( ! ( sudoHost=*)
    ( sudoHost=ALL )
    ( sudoHost=hostname.domain )
    ( sudoHost=hostname )
    ( sudoHost=IPv4 )
    ( sudoHost=IPv4/netmask )
    ( sudoHost=IPv6 )
    ( sudoHost=IPv6/netmask )
    ( sudoHost=+* )
    ( | ( sudoHost=*\\* )
      ( sudoHost=?* )
      ( sudoHost=*\** )
      ( sudoHost=*[*]* )
    )
  )
)
```

SYSDB filter :

```
( objectClass=sudoRule )
```

Tento filtr vyhledá všechna sudo pravidla, která jsou aplikovatelná na klientský počítač. Jméno počítače (`hostname` a `hostname.domain`) a IP adresy jsou získány při inicializaci. Filtr také zachytí všechna pravidla aplikovatelná na jakoukoliv síťovou skupinu počítačů (`(sudoHost=+*)`), protože nemá informaci o tom, ve kterých síťových skupinách se počítač nachází.

Před uložením stažených pravidel jsou nejprve z sysdb odstraněny **všechny** sudo pravidla pomocí filtru (`objectClass=sudoRule`). Až poté je zahájena transakce pro uložení nově stažených pravidel.

Průběžná aktualizace

Pro detekci modifikovaných pravidel se při průběžných aktualizacích využívá USN plugin a jeho `EntryUSN` atribut, viz. USN plugin v sekce 2.2.1.

Předpokládejme příklad kdy je na klientském počítači spuštěno SSSD a tento počítač má následující parametry:

Doménové jméno: `client1.example.cz`
IPv4 adresa: `192.168.0.2`
IPv6 adresa: `fe80::a00:27ff:fe71:1191`

V sysdb již máme stažená nějaká pravidla a nejvyšší hodnota atributu **EntryUSN**, která se mezi pravidly nachází je **9270**. LDAP filtr, který by se použil při průběžné aktualizaci by vypadal následovně:

LDAP filter :

```
(&(&(objectclass=sudoRole)
  (entryUSN>=9270)
  (!(entryUSN=9270))
)
(|(!(sudoHost=*))
  (sudoHost=ALL)
  (sudoHost=client1.example.cz)
  (sudoHost=client1)
  (sudoHost=192.168.0.2)
  (sudoHost=192.168.0.0/24)
  (sudoHost=fe80::a00:27ff:fe71:1191)
  (sudoHost=fe80::/64)
  (sudoHost=+*)
  (|(sudoHost=*\\\\\\*)
    (sudoHost=?*)
    (sudoHost=*\\\\**)
    (sudoHost=*[*]*)
  )
)
)
```

Při průběžných aktualizacích z sysdb nejsou mazána žádná pravidla. Dochází pouze k přidávání pravidel, jestliže se na serveru vyskytují novější pravidla.

Aktualizace pravidel

Jestliže se v sysdb při spuštění programu sudo nachází nějaká pravidla, která již nejsou platná, pak se provede jejich aktualizace. Předpokládejme příklad, kdy v sysdb již nejsou validní pravidla **rule1** a **rule2**. Poté by LDAP a sysdb filtr pro jejich aktualizaci vypadal následovně:

LDAP filter :

```
(&(&(objectClass=sudoRole)
  (|(cn=rule1)
    (cn=rule2)
  )
)
(|(!(sudoHost=*))
  (sudoHost=ALL)
)
```

```

(sudoHost=client1.example.cz)
(sudoHost=client1)
(sudoHost=192.168.0.2)
(sudoHost=192.168.0.0/24)
(sudoHost=fe80::a00:27ff:fea1:b983)
(sudoHost=fe80::/64)
(sudoHost=+*)
(|(sudoHost=*\\\\\\*)
(sudoHost=?*)
(sudoHost=*\\\\**)
(sudoHost=*[*]*)
)
)
)

```

SYSDb filter :

```

(&(objectClass=sudoRule)
(|(cn=test4)
(cn=test5)
)
)

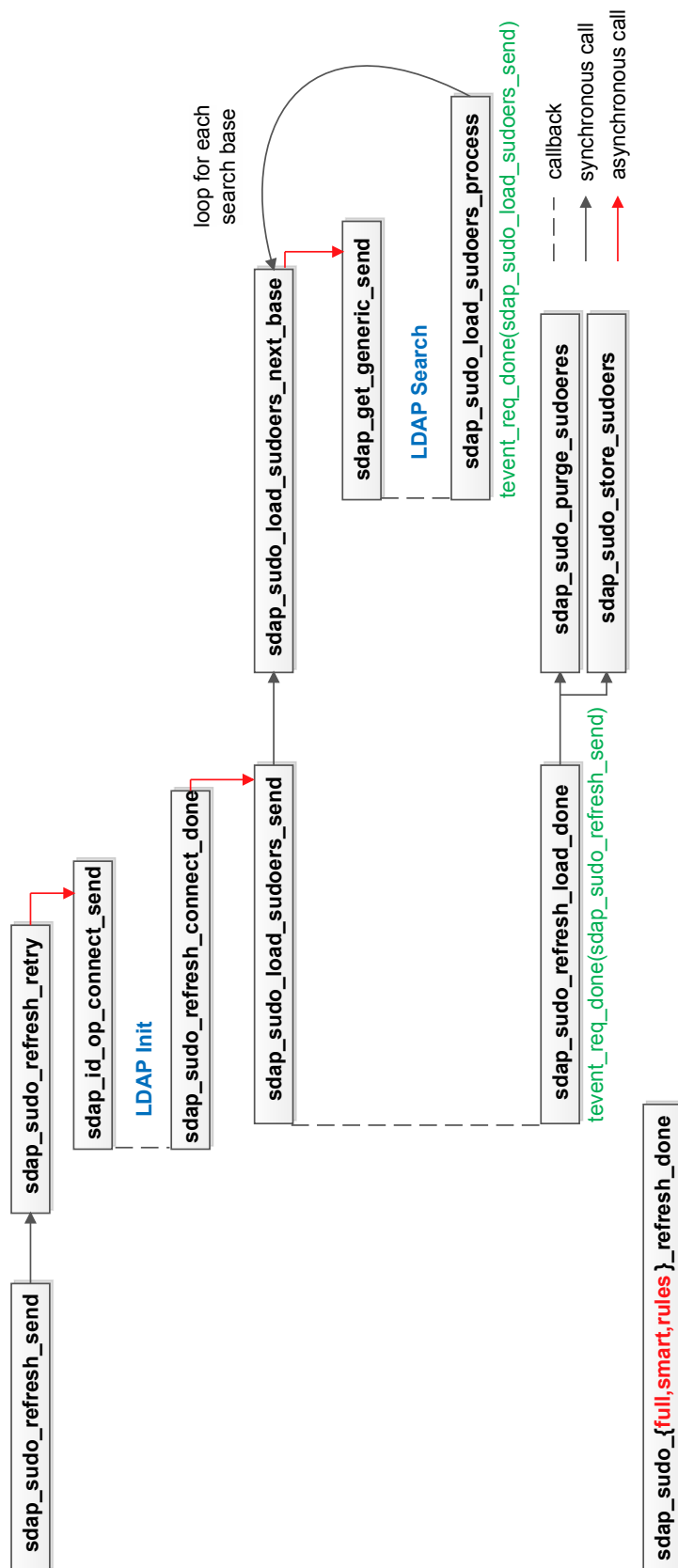
```

Nejprve by se provedlo vyhledání a stažení pravidel z LDAP serveru. Poté by došlo k vymazání pravidel `rule1` `rule2` ze sysdb a následně uložení nově stažených pravidel. Aktualizace pravidel, která jsou stále platná, se neprovede. Neprovede se ani aktualizace právě vyvolaného pravidla, za předpokladu, je stále platné.

3.4.4 Asynchronní modul

Modul `providers/ldap/sdap_async_sudo.c` je nejdůležitější částí LDAP SUDO pluginu, který provádí asynchronní stažení a uložení sudo pravidel do sysdb. Jeho asynchronní činnost popisuje schéma 3.9. Asynchronní funkce toho modulu poté provádějí následující:

- `sdap_sudo_refresh_retry()` – Provádí kontrola zda je klient stále připojen k síti. Jestliže ano, pak proběhne inicializace LDAP spojení.
- `sdap_sudo_load_sudoers_send()` Zde se vytváří pole atributů pro LDAP dotaz.
- `sdap_sudo_load_sudoers_next_base()` Nastavuje aktuální search base, a posílá LDAP dotaz pomocí rozhraní `sdap_get_generic_send()`.
- `sdap_sudo_load_sudoers_process()` – Zajišťuje přijmutí a zpracování pravidel, tj. přidání pravidel k již staženým. Jakmile jsou všechna pravidla stažena, proběhne modifikace sysdb a poté je zahájena transakce při které se nově stažená pravidla uloží do sysdb.



Obrázek 3.9: Schéma událostí asynchronního modulu `providers/ldap/sdap_async_sudo.c`.

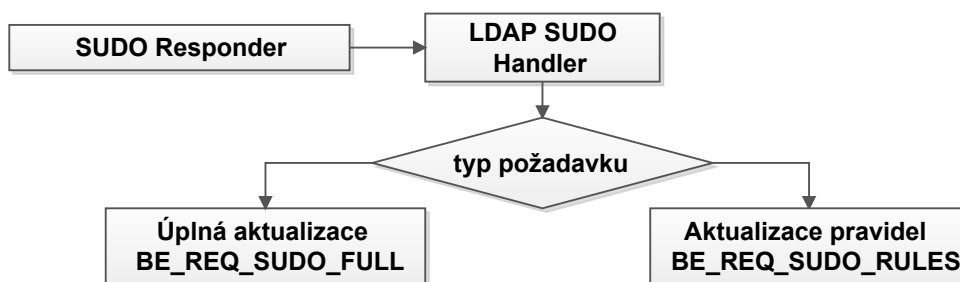
3.4.5 Uložení sudo pravidel do sysdb

Před samotným uložením pravidel jsou v sysdb nejprve vyhledány a následně odstraněny všechny záznamy, které odpovídají SYSDB filtru pro konkrétní typ aktualizace. Při ukládání sudo pravidel se každému pravidlu přidá atribut **dataExpireTimestamp**¹⁸. Jeho hodnota reprezentuje čas, kdy daný záznam stane neplatným. Zároveň je získána nejvyšší hodnota USN, která ovšem není uložena v cache paměti společně s pravidly, ale v kontextu `id_ctx->srv_opts` v proměnné `max_sudo_value`.

3.4.6 LDAP SUDO Handler

Jestliže SUDO responder nenajde daná pravidla v sysdb, pak zašle SBUS požadavek přes SUDO handler danému providerovi. Jestliže SUDO používá LDAP jako provider plugin¹⁹, pak se zavolá handler `sdap_sudo_handler`. Handler se nachází v kontextu backendu, viz. Sekce 3.3. Samotnou definici handleru je možné najít v modulu `sdap_sudo.c`.

LDAP SUDO provideru je přes handler předán typ aktualizace, který po něm SUDO responder žádá a pole pravidel, které chce responder aktualizovat²⁰. SUDO responder může požádat o úplnou aktualizaci nebo o aktualizaci pravidel, která již v sysdb nejsou nadále platná.



Obrázek 3.10: LDAP SUDO Handler.

3.5 IPA SUDO provider

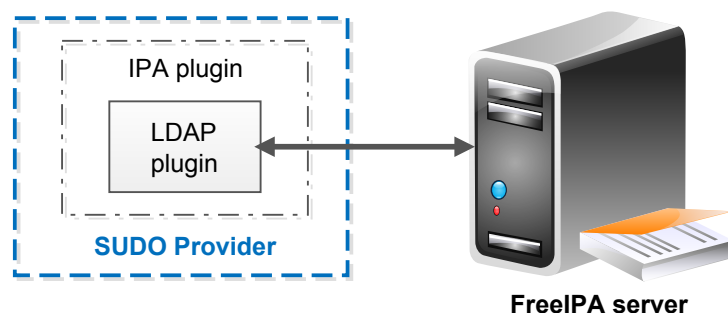
Pro SUDO providera je možné použít také ipa plugin²¹, jestliže jsou sudo pravidla uložena na IPA serveru. Problém ovšem je, že SSSD nedisponuje IPA pluginem pro SUDO providera, který by podporoval IPA SUDO schéma. Současná implementace tohoto pluginu je pouze obálka pro LDAP sudo plugin. Samotný LDAP plugin rovněž nepodporuje IPA SUDO schéma a neumí tedy sudo pravidla v tomto formátu zpracovat. LDAP plugin umí zpracovat pouze pravidla, která odpovídají nativnímu LDAP SUDO schématu.

¹⁸aktuální čas (v době ukládání) + hodnota volby `entry_cache_sudo_timeout`, viz. `man sssd.conf`

¹⁹`sudo_provider=ldap`

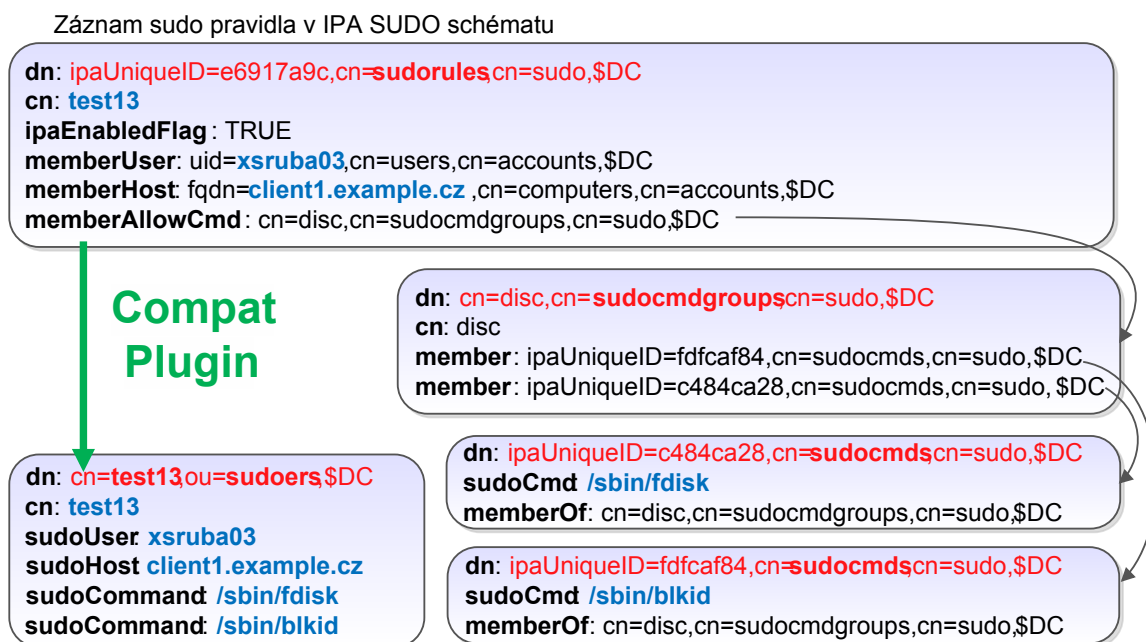
²⁰pole jmen pravidel, tj. pole hodnot `cn` atributů

²¹`sudo_provider=ipa`



Obrázek 3.11: Současná implementace IPA SUDO pluginu.

Pro podporu sudo pravidel v IPA SUDO formátu využívá současná implementace SSSD *compat plugin*. Tento plugin běží na serveru FreeIPA a zajišťuje překlad sudo pravidel z IPA SUDO schématu do LDAP SUDO schématu. Funkcionalitu pluginu demonstruje schéma 3.12. Překlad samotný probíhá při každém vytvoření nebo modifikaci sudo pravidla. Takto přeložená pravidla se poté na serveru nacházejí v kontejneru `ou=SUDOers,$DC`.



Obrázek 3.12: Překlad sudo pravidel provádí na IPA serveru compat plugin.

Sudo pravidla jsou tedy na serveru uložena dvakrát, i když v jiných schématech. Za předpokladu, že by SSSD mělo podporu pro nativní IPA SUDO schéma, byla by odstraněna režie compat pluginu. To znamená, že by nadále nebylo nutné provádět překlad **všech** sudo pravidel. Překlad by byl přenesen ze serveru na klienta. To by znamenalo překlad pouze těch pravidel, která jsou aplikovatelná pro daného klienta.

Tato bakalářská práce si klade za cíl odstranění této režie a implementaci ipa sudo

pluginu, který bude zajišťovat podporu nativního IPA SUDO schématu.

Kapitola 4

Nativní IPA SUDO Provider

Tato kapitola se zabývá diskusí nad řešením hlavních problémů, které je nutno zvážit při návrhu, implementaci a testování nativního IPA SUDO providera. Tento provider poté bude podporovat nativní IPA SUDO schéma používané FreeIPA serverem. Návrh popisuje možné přístupy ke stažení a zpracování sudo pravidel, jejichž výhody a nevýhody byly diskutovány s vývojáři LDAP SUDO providera. Některé specifické detaily také s vývojáři projektu FreeIPA. Sekce implementace popisuje jak a které z těchto přístupů byly vybrány pro implementaci nového providera. V sekci testování je poté popsána metodika a nástroje využití k otestování navržených řešení.

4.1 Návrh

4.1.1 Sudo pravidla aplikovatelná na klienta

Jedním z problémů, které je nutno vyřešit, je správný přístup k tomu jakým způsobem získat kompletní sudo pravidla pro daný počítač. A zároveň nestahovat žádná pravidla ani jiné nepotřebné informace navíc. LDAP SUDO provider při úplné aktualizaci stahuje například i všechna pravidla, která jsou aplikovatelná na libovolnou síťovou skupinu počítačů. Ke stahování pravidel z IPA serveru lze přistoupit následujícími způsoby.

Klient jako člen IPA domény

Každý klientský počítač, který je členem IPA domény, má na IPA serveru záznam v kontejneru `cn=computers,cn=accounts,$DC`. Každý takový záznam obsahuje například atribut `memberOf`, kde se nacházejí odkazy na záznamy skupin počítačů, síťových skupin a sudo nebo HBAC¹ pravidel, kterými je daný počítač členem. Bylo by tedy možné jedním dotazem získat odkazy na sudo pravidla, která jsou aplikovatelná na daný klientský počítač a dalšími dotazy už konkrétní záznamy sudo pravidel. Jestliže bychom chtěli získat DNS² sudo pravidel aplikovatelných na klientský počítač jehož doménové jméno je `client.example.cz`. Poté by LDAP dotaz mohl mít následující parametry:

```
Prohledávaná oblast: fqdn=client.example.cz,cn=computers,cn=accounts,$DC
Filtr:                "(memberOf=ipauniqueid=*cn=sudorules,cn=sudo,$DC)"
Dotazované atributy:  memberOf
```

¹Host-Based Access Control

²Distinguished Names

S tímto přístupem jsou ovšem spojeny dva problémy. V `memberOf` atributu záznamu pro klienta se nenachází sudo pravidla aplikovatelná na kterýkoliv počítač. To znamená pravidla, která mají `hostCategory` atribut. Tyto pravidla by tedy bylo nutné dodatečně stáhnout. Druhým problémem jsou skupiny počítačů. Jestliže je sudo pravidlo aplikovatelné na nějakou skupinu počítačů a klient je zároveň členem této skupiny. Pak je sudo pravidlo na daného klienta aplikovatelné. Odkaz na toto pravidlo se ovšem nenachází v záznamu daného počítače, ale v záznamu dané skupiny. Odkazy na tyto pravidla by bylo nutné získat pomocí dereference odkazů na dané skupiny počítačů.

Specifikace klientského počítače

Je možné využít stejný přístup, který používá současná implementace LDAP SUDO providera. Pro výběr sudo pravidla aplikovatelného na konkrétní počítač v IPA doméně jsou použity tři atributy.

- `memberHost`
- `externalHost`
- `hostCategory`

Za předpokladu, že je sudo pravidlo na IPA server přidáno korektně, tj. pomocí webového rozhraní nebo utilit `ipa-sudorule-add-*`. Pak atribut `memberHost` bude vždy obsahovat plně specifikované doménové jméno počítače. Nebo název skupiny počítačů. Jestliže je pravidlo aplikovatelné na libovolný počítač, pak bude mít atribut `hostCategory` hodnotu `all` a jiné atributy specifikující počítač se již v záznamu pravidla neobjeví. Parametry LDAP dotazu pomocí kterého bychom získali záznamy všech pravidel aplikovatelných pro klientský počítač s doménovým jménem `client.example.cz` mohou vypadat následovně:

```
Prohledávána oblast:  cn=sudorules,cn=sudo,dc=example,dc=cz
Filtr:                 "(|(memberHost=client.example.cz)(hostCategory=all))"
Dotazované atributy:   memberOf
```

Problémem tohoto přístupu je fakt, že SUDO provider nemá informaci o tom, ve kterých skupinách počítačů se daný počítač nachází. Tato informace je dostupná pouze na IPA serveru. Tento problém by bylo možné odstranit dvěma způsoby:

1. Stažením sudo pravidel aplikovatelných pro libovolnou skupinu počítačů. V případě rozsáhlé databáze pravidel a mnoho skupin počítačů by to ovšem mohlo způsobit značný síťový provoz navíc.
2. Nejprve získat seznam všech skupin, kterými je daný klient členem a až poté sestavit LDAP dotaz pro stažení sudo pravidel.

4.1.2 Stažení sudo pravidel

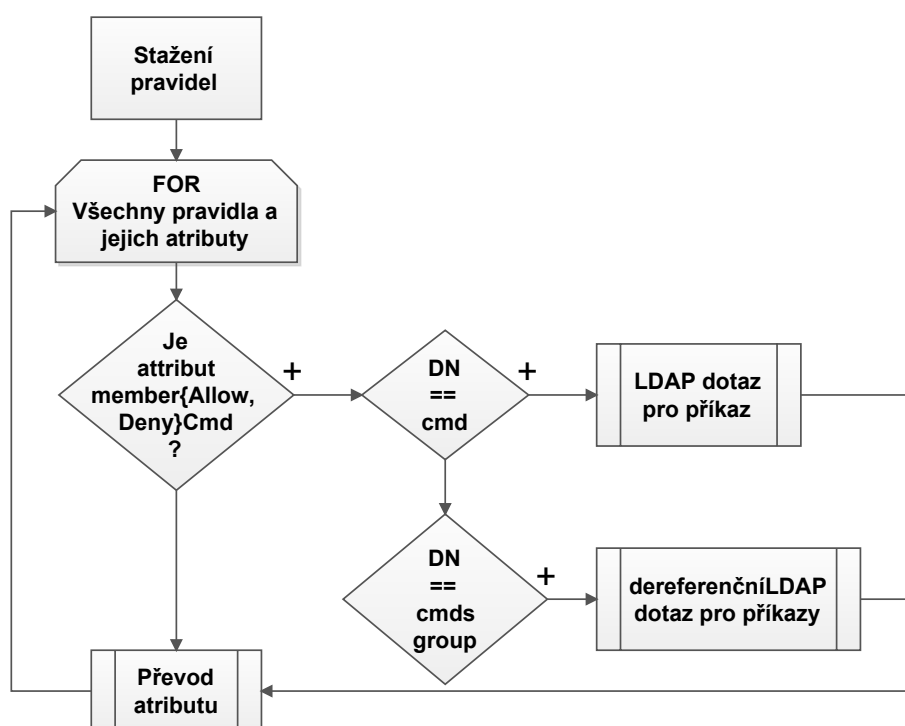
Jestliže víme, jak specifikovat sudo pravidla aplikovatelná na klientský počítač, další krokem je samotné stažení těchto pravidel z IPA serveru. LDAP SUDO provider stahuje sudo pravidla pomocí jediného LDAP dotazu, protože kompletní záznamy sudo pravidel se nacházejí většinou v kontejneru `ou=SUDOers,$DC`³. Sudo pravidla na IPA serveru jsou ovšem

³prohledávanou oblast je možné specifikovat v `sssd.conf` pomocí volby `ldap_sudo_search_base`

rozmístěna ve třech kontejnerech, viz Sekce 2.2.1. Pro stažení kompletních sudo pravidel se nabízí několik následujících přístupů.

1. Postupné dotazování

První přístup, který se nabízí a který popisuje diagram 4.1, je stažení všech pravidel aplikovatelných na daný počítač. To znamená konkrétní záznamy o sudo pravidlech z kontejneru `cn=sudorules,cn=sudo,$DC`. Pro tyto záznamy je ovšem nezbytné ještě stáhnout příkazy. Bylo by tedy nutné iterovat před stažené záznamy a pro každý odkaz na sudo příkaz provést LDAP dotaz jehož výsledkem by již byl konkrétní příkaz. Pokud by se jednalo o skupinu příkazu, pak by bylo nutné provést dereferenční dotaz, jehož výsledkem by byl záznam, kde by se nacházel již konkrétní příkaz.



Obrázek 4.1: Stažení kompletních sudo pravidel postupným dotazováním.

Tento přístup má tyto výhody:

1. Zpracování pravidel, které představuje překlad pravidel z IPA schématu do nativního LDAP schématu, viz. Sekce 4.1.3, je možné provést v jediném cyklu.
2. Nejsou stahována žádná přebytečná sudo pravidla, příkazy nebo jiné záznamy.

Při rozsáhlé databázi sudo pravidel by to ovšem mohlo znamenat velké množství LDAP dotazů. Pravidla by navíc mezi těmito dotazy mohla být modifikována.

2. Další dotaz pro příkazy

Jiným přístupem, který se nabízí, je stažení všech záznamů o sudo pravidlech aplikovatelných na klientský počítač. Tyto záznamy projít a sestavit filtr pro LDAP dotaz, který stáhne všechny potřebné příkazy pro stažená pravidla.

Příklad staženého sudo záznamu z IPA serveru

```
dn: ipaUniqueID=7f9192b2,cn=sudorules,cn=sudo,$DC
...
memberDenyCmd: cn=group,cn=sudocmdgroups,cn=sudo,$DC
memberAllowCmd: cn=user,cn=sudocmdgroups,cn=sudo,$DC
memberAllowCmd: ipaUniqueID=6f545188,cn=sudocmds,cn=sudo,$DC
...
```

```
(&(objectClass=ipaSudoCmd)
  (|(memberOf=cn=group,cn=sudocmdgroups,cn=sudo,$DC)
    (memberOf=cn=user,cn=sudocmdgroups,cn=sudo,$DC)
    (ipaUniqueID=6f545188)
  )
)
```

Obrázek 4.2: Sestavení LDAP filtru pro sudo příkazy.

Záznamy o skupinách sudo příkazů není nutné stahovat. Tyto skupiny totiž není možné do sebe zanořovat. Každý sudo příkaz má atribut `memberOf`, který obsahuje DN skupin příkazů, kterých je členem. Jestliže se `memberAllowCmd` nebo `memberDenyCmd` odkazuje na skupinu sudo příkazů, pak je možné dané příkazy na základě `memberOf` atributu zjistit.

Výhodou tohoto přístupu je, že redukuje počet LDAP dotazů, nutných pro stažení všech záznamů potřebných pro překlad sudo pravidel, na dva a zároveň nestahuje žádné přebytečné informace.

3. Stažení všech příkazů

Množina sudo příkazů je obecně malá. Bylo by tedy možné v jediném LDAP dotazu stáhnout sudo pravidla aplikovatelná na klientský počítač a zároveň **veškeré** sudo příkazy.

Výhodou tohoto přístupu je, že pro stažení kompletních sudo pravidel postačí jediný LDAP dotaz. Jejich následný překlad je možné provést v jednom cyklu. Může ovšem nastat situaci, kdy se na klienta bude aplikovat např. pouze jedno sudo pravidlo. Jestliže se na serveru nachází velké množství sudo pravidel a jejich sudo příkazů, pak by to znamenalo přenášení spousty záznamů, které nebudou použity. Bylo by je ovšem nutné zpracovat, což přináší výkonnostní ztráty.

4.1.3 Překlad pravidel

Jelikož program sudo dokáže zpracovat pouze pravidla, která odpovídají nativnímu LDAP sudo schématu. Je nutné provést překlad stažených pravidel. Příklad tohoto překladu, který v současné době provádí compat plugin demonstruje schéma 3.12.

Některé atributy je možné přeložit pouhým zkopírováním hodnoty a záměnou jména atributu. Mezi tyto atributy patří například: `cn`, `externalUser` nebo `ipaSudoOpt`. Atributy jako jsou například `memberHost` nebo `memberUser` obsahují DN záznamu daného počítače, popř. uživatele. Jelikož projekt FreeIPA garantuje použitá schémata, je možné dané hodnoty z DN odvodit. Například z hodnoty atributu `memberUser`:

```
memberUser: cn=students,cn=groups,cn=accounts,$DC
```

je možné odvodit, že je pravidlo aplikovatelné na všechny uživatele skupiny „students“. U `*Category` atributů je nutné provést pouze záměnu malých písmen za velká.

```
hostCategory: all => sudoCommand: ALL
```

Pro atributy `memberAllowCmd` a `memberDenyCmd` je nutné vyhledat potřebný příkaz, popř. skupinu příkazů, jedná-li se o odkaz na skupinu příkazů. Pro všechny atributy které IPA SUDO schéma definuje je tedy nutné určit jakým způsobem bude přeložena jejich hodnota. Atributy lze rozdělit na několik typů. Jakým způsobem je nutné který typ přeložit popisuje tabulka 4.1. Mohlo by se zdát, že typ `USER_GROUP` a `HOST_GROUP` není nutné rozlišovat, ovšem liší se v prefixu, který je k nové hodnotě nutno přidat. Viz. příklady hodnot atributů `sudoUser` a `sudoHost`, které zobrazují tabulky 2.1 a 2.2.

Typ atributu	Způsob překladu hodnoty
USER	DN (hodnota kontejneru uid)
USER_GROUP	DN (hodnota kontejneru cn)
HOST	DN (hodnota kontejneru fqdn)
HOST_GROUP	DN (hodnota kontejneru cn)
COMMAND	DN (hodnota kontejneru ipaUniqueID je použita pro filtr)
CMDS_GROUP	hodnota je použita pro filtr pro příkazy
UPPER_CASE	převedení malých písmen hodnoty na velká
COPY	kopie původní hodnoty

Tabulka 4.1: Typy atributů a způsob jejich překladu.

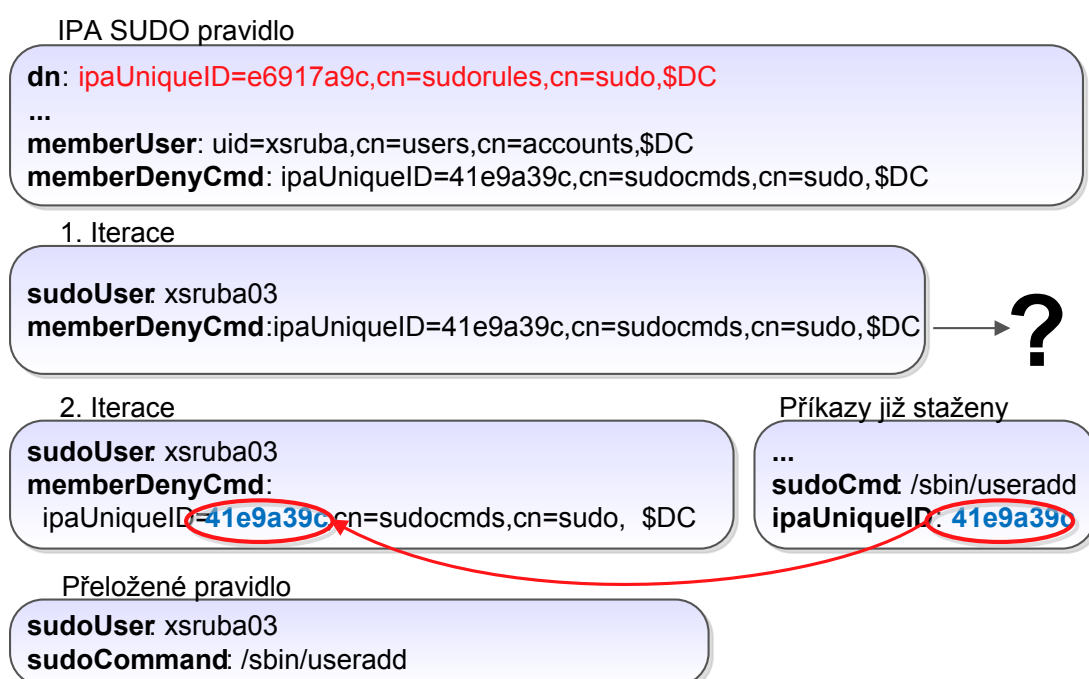
Pro algoritmus překladu pravidel byla vytvořena překladová tabulka, která definuje jakým způsobem má být proveden překlad jednotlivých jmen a hodnot atributů včetně příkladů, viz. Příloha A. Tato tabulka byla vytvořena na základě implementace compat pluginu a byla diskutována s vývojáři projektu FreeIPA. Při jejím sestavování byla také objevena chyba, které se vyskytuje ve webovém rozhraní serveru FreeIPA. Ta umožňuje atributu `ipaSudoRunAsGroup` přiřadit libovolnou skupinu. Správně by mělo být možné tomuto atributu přiřadit pouze POSIX skupinu. Pro tuto chybu byl vytvořen ticket číslo

4314⁴.

Algoritmus překladu pravidel

Uvažujeme variantu stahování sudo pravidel popsanou v sekci 4.1.2, tj. stažení pravidel pomocí dvou LDAP dotazů. Po prvním dotazu získáme množinu záznamů sudo pravidel. Druhý dotaz vrátí množinu záznamů sudo příkazů pro stažená pravidla.

Pro získání filtru, potřebného pro dotaz pro sudo příkazy, je nutné nejméně jednou iterovat přes množinu stažených sudo pravidel. Při této iteraci je již možné provést překlad všech atributů kromě těch, které se odkazují na příkazy, tj. `memberAllowCmd` a `memberDenyCmd`. Jakmile obdržíme sudo příkazy, můžeme provést druhou iteraci množinou sudo pravidel, při které doplníme potřebné příkazy.



Obrázek 4.3: Dvouprůchodový překlad IPA SUDO pravidel

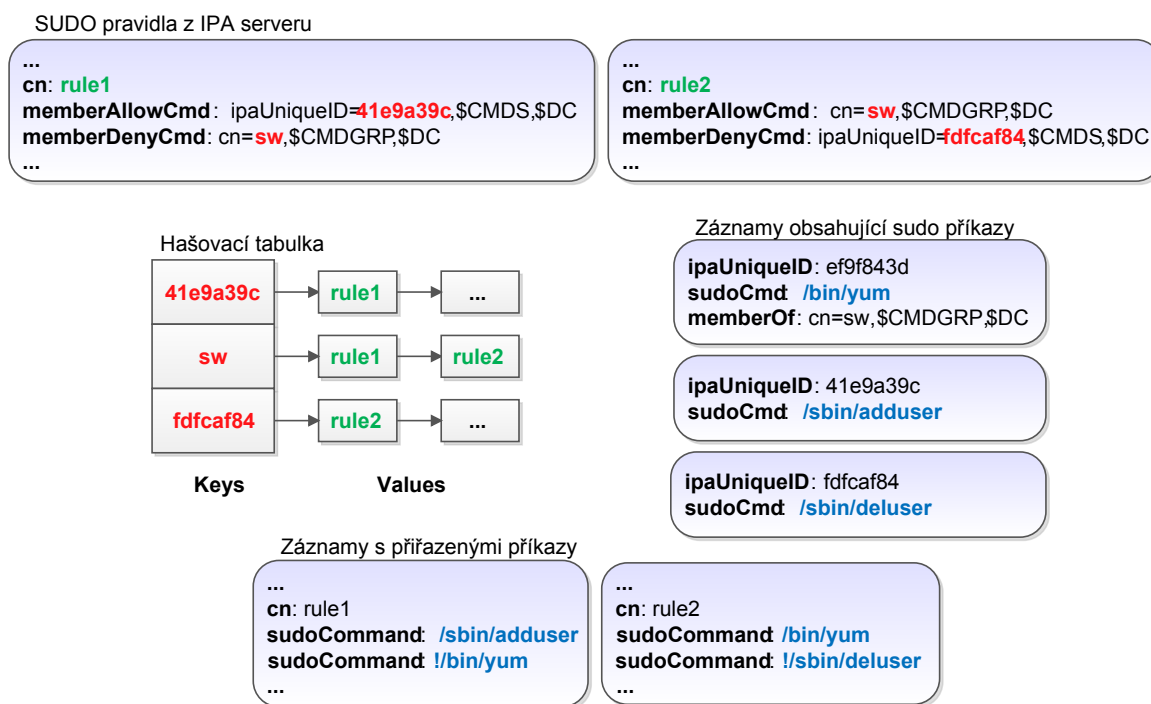
Tento způsob překladu má ovšem následující nevýhody:

- Při druhém průchodu nevíme, kde se nepřeložené atributy `memberAllowCmd` a `memberDenyCmd` nacházejí a proto je nutné je v pravidlech znovu dohledat.
- Pro každý `memberAllowCmd` a `memberDenyCmd` atribut je nutné vyhledat potřebný příkaz, což vede k mnoha iteracím nad **neměnicí** se množinou příkazů.

Optimalizací tohoto přístupu by mohlo být uchování hodnot odkazů na příkazy a pravidla ve kterých se příkaz vyskytl. Stále je ovšem nutné N-krát iterovat množinou příkazů, kde N je počet odkazů na příkazy v záznamech sudo pravidel. Tyto problémy je možné

⁴<https://fedorahosted.org/freeipa/ticket/4314#no1>

odstranit za pomoci použití hašovací tabulky. Tento přístup zobrazuje schéma 4.4. Jako klíč může posloužit DN záznamu sudo příkazu nebo skupiny příkazů. Hodnotou položky této tabulky poté může být seznam všech pravidel, ve kterých se daný příkaz nebo skupina příkazů vyskytuje. Je ovšem nutné si také uchovat informaci o tom, zda má být daný příkaz povolen/zakázán a také pořadí daných příkazů na kterém záleží, viz. Sekce 2.1.2.



Obrázek 4.4: Použití hašovací tabulky pro překlad atributu s příkazy.

Hlavní výhodou tohoto přístupu je snížení počtu iterací. Tento přístup je vhodný v případech kdy pracujeme s velkým počtem záznamů o sudo pravidlech a příkazech. Typicky tedy při provádění úplných aktualizací. Při aktualizaci pravidel a průběžných aktualizacích budou tyto množiny obecně menší. Použití hašovací tabulky by tedy v těchto případech nebylo nutné. Typ aktualizace je znám před samotným stažením pravidel a počet stažených sudo pravidel po prvním dotazu. Je tedy možné provádět výběr zvoleného algoritmu na základě těchto informací.

Jestliže máme zvolený algoritmus překladu pravidel, pak je nutné rozhodnout, kdo tento překlad bude realizovat. Nabízí se řešení uložit stažená sudo pravidla v IPA formátu přímo do cache paměti a nechat SUDO respondera tyto pravidla překládat. Tento přístup sice je realizovatelný, ale není správný z pohledu architektury SSSD. Jak bylo řečeno v sekci 3.2, responderi mají s pomocí cache paměti pouze co nejrychleji odpovídat na dotazy klientských aplikací. Z tohoto důvodu musí být do sysdb uložena již přeložená sudo pravidla a jejich zpracování tedy musí provést SUDO provider. V tomto případě tedy překlad pravidel musí realizovat navrhovaný IPA SUDO provider.

4.1.4 Využitelnost LDAP pluginu

IPA SUDO provider bude provádět velmi podobnou funkcionalitu jako LDAP SUDO provider. Mohlo by se tedy zdát, že jediná úprava, kterou je nutno provést v LDAP SUDO providerovi, je přidání překladu pravidel před samotným uložením těchto pravidel do cache paměti. Překlad pravidel je ovšem specifický pro IPA providera. V kódu LDAP SUDO providera by se tedy muselo vyskytnout volání funkcí, které by se nacházely v IPA SUDO providerovi. Tento přístup je sice realizovatelný⁵, ovšem neodpovídá návrhu SSSD. Kód zajišťující překlad pravidel by byl součástí dynamické knihovny `libsss_ipa.so` zatímco kód LDAP SUDO providera se nachází v knihovně `libsss_ldap.so`. SSSD je ovšem možno nainstalovat a používat bez podpory IPA. Například je možno využít SSSD pouze ke cachování sudo pravidel uložených na LDAP serveru, kde se samozřejmě nacházejí v nativním LDAP SUDO schématu. V takovém případě není potřeba sudo pravidla překládat a SSSD je nakonfigurováno tak, aby využilo LDAP SUDO providera z knihovny `libsss_ldap.so`. Knihovna `libsss_ipa.so` tedy není potřeba. Při načítání `libsss_ldap.so` by poté nastal problém, jelikož by se odkazovala na funkce, které se nacházejí v knihovně, která není a ani by nebyla načtena do paměti. Proto není možné z LDAP SUDO providera volat kód z IPA sudo providera. Je ovšem možné z IPA SUDO providera volat kód LDAP SUDO providera, LDAP provider je možné si představit jako jakýsi stavební blok nad kterým mohou stavět ostatní provideři a toho je možno využít. Větší zásah do LDAP SUDO providera by také mohl vnést mnoho chyb do již fungujícího a odladěného kódu.

Asynchronní modul `sdap_async_sudo.c` provádí stažení a uložení sudo pravidel v nativním LDAP schématu do sysdb. Je tedy možné využít této asynchronní události pro stažení pravidel v IPA SUDO schématu. Pro tyto pravidla je nutné dále stáhnout sudo příkazy a poté provést překlad těchto pravidel. Jestliže máme sudo pravidla přeložena z IPA SUDO schématu do nativního LDAP schématu, můžeme opět využít zmiňovaného modulu pro aktualizaci cache paměti.

4.2 Implementace

Pro specifikaci pravidel aplikovatelných na klientský počítač byl vybrán přístup popsáný v podsektci 4.1.1. Výběr těchto pravidel je tedy proveden dotazem do kontejneru:

```
cn=sudorules,cn=sudo,$DC
```

Filtr pro LDAP dotaz, specifikuje klienta pomocí FQDN daného počítače a skupin ve kterých je členem. Pro získání těchto skupin je použita funkce `ipa_host_info_send()`. Základní filtr, který je použit pro úplnou aktualizaci vypadá následovně:

```
(&(objectClass=ipasudorule)
(ipaEnabledFlag=TRUE)
(|(cn=defaults)
(hostCategory=ALL)
(memberHost=FQDN)
(externalHost=FQDN)
(memberHost=DN of a HOSTGROUP)
...

```

⁵První prototyp byl na této myšlence založen.

)
)

Při aktualizaci pravidel jsou pouze přidána jména pravidel, stejně jako u LDAP SUDO providera. Zde by také bylo možné využít atributu `ipaUniqueID`, který jednoznačně identifikuje sudo pravidlo. To by ovšem vyžadovalo úpravu SUDO respondera, která by nepřinesla žádnou výhodu. Jelikož jsou hodnoty atributů `cn`, tj. jména sudo pravidel, jedinečná i v IPA SUDO schématu, není potřeba tuto změnu provádět. Při průběžných aktualizacích je opět využito atributu `EntryUSN`, k detekci nově přidáných nebo modifikovaných sudo pravidel.

Stažení kompletních sudo pravidel, tj. pravidla a příkazy, je provedeno pomocí dvou dotazů pro všechny typy aktualizací. Pro stažení pravidel jsou tedy zapotřebí **nejvýše tři** LDAP dotazy a nejméně dva v případě, že stažená pravidla neobsahují odkazy na další záznamy, tj. odkazy na záznamy příkazů. Zvažována byla také varianta, kde by se pro úplnou aktualizaci postupovalo podle metody 4.1.2, tzn. stažení sudo pravidel a všech příkazů v jediném LDAP dotazu. Zde ovšem vzniká problém s SDAP rozhraním, které neumožňuje specifikovat více než jednu mapu. Proto není možné obdržet záznamy, které nemají alespoň jednu stejnou třídu. Sudo pravidla v IPA SUDO schématu mají třídu `ipaSudoRule`, zatímco příkazy `ipaSudoCmd`. Tento problém je blíže popsán v sekci 3.3.1.

Jako řešení by se nabízelo využít druhého rozhraní tedy `sdap_deref_search_send()`, které dovoluje specifikovat více map. Problémem ovšem je, že neumožňuje specifikovat filtr a tedy množinu záznamů (sudo pravidel) ze kterých by bylo možné přes odkazy získat odkazované záznamy (sudo příkazy). Z implementačního hlediska by tyto rozhraní pro daný účel bylo možné upravit. I kdyby tato změna byla provedena, stále by byl problém s odkazy na skupiny příkazů. V těchto záznamech bychom totiž našli opět odkazy na příkazy, což by znamenalo další LDAP dotaz.

Pro překlad pravidel byl zvolen základní algoritmus s drobnými optimalizacemi, který se při testování osvědčil jako dostatečný pro malou množinu pravidel. V případě výkonnostních problémů je možno přidat podporu hašovací tabulky, která by při velké databázi pravidel mohla zvýšit rychlost překladu.

Pro prvotní stažení pravidel byl využit LDAP SUDO provider. Konkrétně jeho asynchronní modul popsaný v sekci 3.4.4. To ovšem vyžadovalo úpravu v synchronní funkci `sdap_sudo_refresh_load_done()`. Jestliže tento modul využívá IPA SUDO prvider. Pak stažená pravidla ještě nemohou být uložena do sysdb. Proto je asynchronní událost stažení pravidel označena jako dokončena před prací s cache pamětí a řízení je vráceno zpět IPA SUDO providerovi. Z tohoto modulu jsou dále využity funkce, které zajišťují práci s cache pamětí, tzn. odstraňování nevalidních a ukládání nově stažených a již **přeložených** pravidel. Pro plánování pravidelných aktualizací byl použit interní plánovač periodických událostí *ptask*. Nově navržený provider se skládá z následujících modulů:

- `ipa_sudo.c` – provádí počáteční inicializaci IPA SUDO providera, nastavuje SUDO handler a provádí nastavení průběžných aktualizací
- `ipa_async_sudo_hostgroups.c` – asynchronní získání skupin ve kterých je daný počítač členem
- `ipa_sudo_refreshes.c` – provádí nastavení parametrů pro jednotlivé typy aktualizací
- `ipa_async_sudo.c` – asynchronní stažení sudo pravidel z IPA serveru

- `ipa_async_sudo_cmds.c` – asynchronní stažení záznamů o příkazech pro stažená sudo pravidla
- `ipa_sudo_cmd.c` – sestavení LDAP filtru pro získání záznamů o příkazech pro stažená sudo pravidla
- `ipa_sudo_export.c` – překlad samotných pravidel

4.3 Testování

Pro tvorbu jednotkových testů využívá SSSD framework `cmocka`⁶, který podporuje Mock objekty. Pomocí těchto objektů je možné simulovat jakýkoliv reálný objekt. V našem případě byl jako Mock objekt zvolen IPA server, tj. veškerá rozhraní zajišťující komunikaci s IPA serverem. Jednotkové testy je tedy možné provádět bez přítomnosti IPA serveru či připojení k síti. Mock objekty tedy simulují IPA server a sudo pravidla, která se na něm nacházejí.

4.3.1 Metodika

Reálná sudo pravidla si každá společnost pečlivě střeží. Proto nebylo možné taková pravidla získat. Pro testování jsem tedy vytvořil sadu pravidel, které pokrývají následující případy použití:

- sudo pravidla jejichž atributy se neodkazují na žádné objekty (např. uživatele nebo počítače) IPA domény
- komplexní pravidla jejichž atributy se odkazují na jiné objekty IPA domény
- pravidla, která neobsahují odkazy na sudo příkazy
- výskyt neexistujícího atributu
- výskyt atributu, který se odkazuje na neexistující objekt v IPA doméně
- případ, kdy se na serveru nenacházejí žádná pravidla
- testování správného pořadí přeložených příkazů

⁶<http://cmocka.org/>

Kapitola 5

Závěr

Tato bakalářská práce popisuje LDAP schémata, která používají program sudo a server FreeIPA k ukládání sudo pravidel v LDAP adresářích. Srovnává jejich rozdíly a výhody jejich použití. Dále dokumentuje funkcionalitu ldap a ipa pluginů, které má k dispozici SUDO provider démonu SSSD. Tato dokumentace odkrývá nedostatek démonu SSSD, jelikož nepodporuje nativní IPA SUDO schéma. Tento nedostatek se podařilo odstranit navržením a implementací nativního IPA SUDO providera, který toto schéma podporuje. Přenáší tak překlad sudo pravidel ze serveru FreeIPA na klientský démon SSSD. Tento překlad byl také otestován pomocí jednotkových testů. Při návrhu byla také nalezena jedna chyba a bylo poukázáno na některé nedostatky současné implementace.

V práci je dále možno pokračovat například rozšířením jednotkových testů. Mohly by být provedeny výkonnostní testy, na jejichž základě by mohla být stanovena hranice pro výběr, konkrétního algoritmu pro překlad pravidel. Pro plánování aktualizací u LDAP SUDO provideru by taktéž mohl být použit ptask plánovač, popř. by toto rozhraní mohlo být navrženo takovým způsobem, aby jej mohli využít oba pluginy pro SUDO providera. Integrace obou pluginů SUDO providera by mohla být provedena ještě lépe, kde by všechny společné části využívaly stejný kód, čímž by se docílilo nulové redundance kódu. To by ovšem vyžadovalo nový návrh celého SUDO providera, což by znamenalo kompletní přepsání jak ldap tak ipa sudo pluginů pro SUDO providera.

Literatura

- [1] *RedHat Enterprise Linux 4 Security Guide*. Red Hat, Inc., second edition edition, 2008.
- [2] Ella Deon Lackey. Red hat enterprise linux 6 identity management guide.
https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Identity_Management_Guide/Red_Hat_Enterprise_Linux-6-Identity_Management_Guide-en-US.pdf, 2013.
- [3] Gordon S. Good Timothy A. Howes Ph.D., Mark C. Smith. *Understanding and Deploying LDAP Directory Services*. Addison Wesley, 2. edition, 2003.
- [4] Sudoers ldap manual [online]. <http://www.sudo.ws/sudoers.ldap.man.html>.
- [5] Sudoers manual [online]. <http://www.sudo.ws/sudoers.man.html>.
- [6] H. Chu. Ordered entries and values in ldap [online].
<http://tools.ietf.org/html/draft-chu-ldap-xordered-00>, 2006.
- [7] Rüdiger Landmann. *Red Hat Directory Server 8.2 Administration Guide*. Red Hat, Inc., 2010.
- [8] Prpič Martin Hradílek Jaromír, Silas Douglas. *Fedora 16 System Administrator's Guide*. Red Hat, Inc., 2011.
- [9] Pavel BŘEZINA. Talloc - a hierarchical memory allocator [online].
http://is.muni.cz/th/359290/fi_b/, 2012 [cit. 2014-04-05].
- [10] David Koňář. *Developer Support Tools for tevent Library*. FIT VUT v Brně, 2013.
- [11] T. Howes. The string representation of ldap search filters. rfc2254, December 1997.

Příloha A

Obsah CD

- `freeipa.schemas/` - LDAP schémata používaná FreeIPA serverem
- `freeipa.schemas/65sudo.ldif` - schéma definující IPA sudo pravidla a příkazy
- `latex` – kompletní zdrojový text této práce včetně všech schémat
- `export_table.pdf` – tabulka, která byla použita pro implementaci překladu atributů sudo pravidel
- `schema_compat.uldif` – schéma, které používá compat plugin pro předkad sudo pravidel
- `sssd` – kompletní zdrojové texty projektu SSSD
- `literature` – použitá literatura, která je volně dostupná