

Open Source identity management



FreeIPA

původně I identity P policy A audit

Ale IPA zustalo

Kompletní Linux domain controller
Umí integrovat AD jako další zdroj Identity
Multi-server replikace pro zajištění HA
Přináší centralizovanou správu
Production ready
Vychází z Red Hat Identity Managementu

https://www.freeipa.org/page/Main_Page

Komponenty:

sssd - manager pristupu do vzdalenyh directory autentifikacnich mechanismu

389 Directory – speciálně upravený pro potřeby identity manageru FreeIPA – proto je plochá struktura

Dogdag (CA)

MIT Kerberos

BIND – DNS (**B**erkeley **I**nternet **N**ame **D**omain)

Python

Apache for GUI

Antonín Ečer, DiS.

<https://ae.cz9.cz>



(PRINCE2® Foundation Certified, ITIL4® Foundation Certified, TOGAF 9.2 L2 Certified)

Obsah

- **Instalace**
- **Instalace repliky**
- **Nastavení defaultního chování**
- **Práce s uživateli**
- **Přidání veřejných ssh klíčů**
- **2FA**
- **Politiky**
- **Certifikáty**
- **DNS**
- **Migrace z LDAP**
- **Napojení na FreeIPA**

Instalace

```
ipa-server-install  
ipa-client-install
```

Fedora / CentOS / RHEL / Ubuntu (community) – ve verzi 20.04 odebrána z repozitory kvůli konfliktu v BIND(DNS) modulu
Doporučuji použití CentOS

```
hostnamectl set-hostname ipa.apollo.local  
yum update -y  
yum install ipa-server ipa-server-dns -y  
ipa-server-install
```

Pozor při prvním nasazení je aktivní shell `/bin/sh` buď v GUI, nebo příkazem
`ipa config-mod --defaultshell=/bin/bash` přepnout na bash

Ohledně centralizovaného logování je doporučení nasazení Kibana/Elastic search
https://www.freeipa.org/page/Centralized_Logging

HA – zajištěno replikami

Instalace Replika serveru

Přidání repliky:

dat navzájem do hosts na sebe adresy, mit spravné hostname
na primarni ipu dat:

```
ipa hostgroup-add-member ipaservers --hosts=ipa1.apollo.local  
prosim vypnout selinux na obou strojich
```

1. přidat server jako ipa client

```
sudo ipa-client-install --hostname=`ipa1.apollo.local` -f --mkhomedir --server=ipa.apollo.local --  
domain apollo.local --realm APOLLO.LOCAL
```

2. na freeipa serveru přidat tento server do skupiny - dělá se pod přihlášením z ldapu(ipi) jinak ipa:
ERROR: neobdrženy ověřovací údaje Kerberos

```
[admin@ipa ~]$ ipa hostgroup-add-member ipaservers --hosts=ipa1.apollo.local
```

```
firewall-cmd --permanent --add-port={80/tcp,443/tcp,389/tcp,636/tcp,88/tcp,464/tcp,53/tcp,88/  
udp,464/udp,53/udp,123/udp}
```

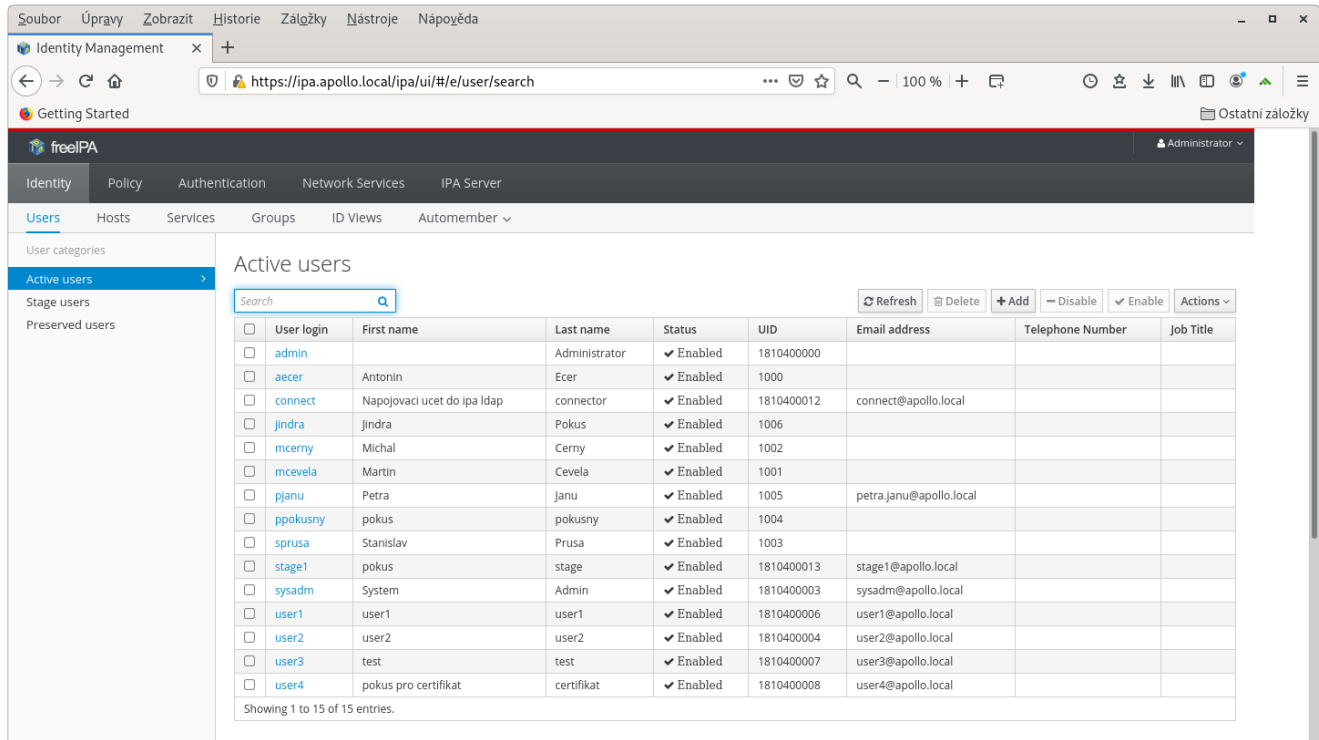
```
firewall-cmd --reload  
yum install ipa-server  
sudo ipa-replica-install
```

To je celé.

Defaultní chování

The screenshot displays the freIPA web interface. The top navigation bar includes tabs for Identity, Policy, Authentication, Network Services, IPA Server, and Configuration. The Configuration tab is active, showing a sub-header with links to Role-Based Access Control, ID Ranges, Realm Domains, Topology, API Browser, and Configuration. The main content area is titled 'Configuration' and features a 'Search Options' section with input fields for 'Search size limit' (100) and 'Search time limit' (2). To the right is a 'User Options' section with various settings: 'User search fields' (uid, givenname, sn, telephonenumber, ou, title), 'Default e-mail domain' (apollo.local), 'Domain resolution order' (empty), 'Default users group' (lpausers), 'Home directory base' (/home), 'Default shell' (/bin/bash), 'Maximum username length' (32), 'Password Expiration Notification (days)' (4), 'Password plugin features' (AllowNThash, KDC:Disable Last Success, KDC:Disable Lockout), and 'Default user authentication bytes' (empty).

Administrace uživatelů z GUI:



The screenshot shows the freeIPA web interface in a browser window. The address bar displays `https://ipa.apollo.local/ipa/ui/#/e/user/search`. The interface has a top navigation bar with tabs: Identity, Policy, Authentication, Network Services, and IPA Server. Below this is a sub-navigation bar with tabs: Users, Hosts, Services, Groups, ID Views, and Automember. The 'Users' tab is selected, and the 'Active users' sub-tab is also selected. On the left, there is a sidebar with 'User categories' including 'Active users', 'Stage users', and 'Preserved users'. The main content area is titled 'Active users' and contains a search bar and a table of active users. The table has columns: User login, First name, Last name, Status, UID, Email address, Telephone Number, and Job Title. The table lists 15 users, all with a status of 'Enabled'. The bottom of the table indicates 'Showing 1 to 15 of 15 entries'.

☐	User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
☐	admin		Administrator	✓ Enabled	1810400000			
☐	aecer	Antonin	Ecer	✓ Enabled	1000			
☐	connect	Napojovací ucet do ipa ldap	connector	✓ Enabled	1810400012	connect@apollo.local		
☐	jindra	Jindra	Pokus	✓ Enabled	1006			
☐	mcerny	Michal	Cerny	✓ Enabled	1002			
☐	mcevela	Martin	Cevela	✓ Enabled	1001			
☐	pjanu	Petra	Janu	✓ Enabled	1005	petra.janu@apollo.local		
☐	ppokusny	pokus	pokusny	✓ Enabled	1004			
☐	sprusa	Stanislav	Prusa	✓ Enabled	1003			
☐	stage1	pokus	stage	✓ Enabled	1810400013	stage1@apollo.local		
☐	sysadm	System	Admin	✓ Enabled	1810400003	sysadm@apollo.local		
☐	user1	user1	user1	✓ Enabled	1810400006	user1@apollo.local		
☐	user2	user2	user2	✓ Enabled	1810400004	user2@apollo.local		
☐	user3	test	test	✓ Enabled	1810400007	user3@apollo.local		
☐	user4	pokus pro certifikat	certifikat	✓ Enabled	1810400008	user4@apollo.local		

Stage users (připravování uživatelé) - může připravovat specializovaný uživatel, pak správce zaktivuje uživatele

Preserved Users (po zrušení účtu je možné ponechat zde, nebo rovnou smazat)

Přidání veřejných ssh klíčů

The screenshot shows the Identity Management web interface for a user named 'sprusa'. The interface is divided into two main sections: 'Identity Settings' and 'Account Settings'.

Identity Settings:

- Job Title: Pokusny uzivatel
- First name: Stanislav
- Last name: Prusa
- Full name: Stanislav Prusa
- Display name: Stanislav Prusa
- Initials: SP
- GECOS:
- Class:

Account Settings:

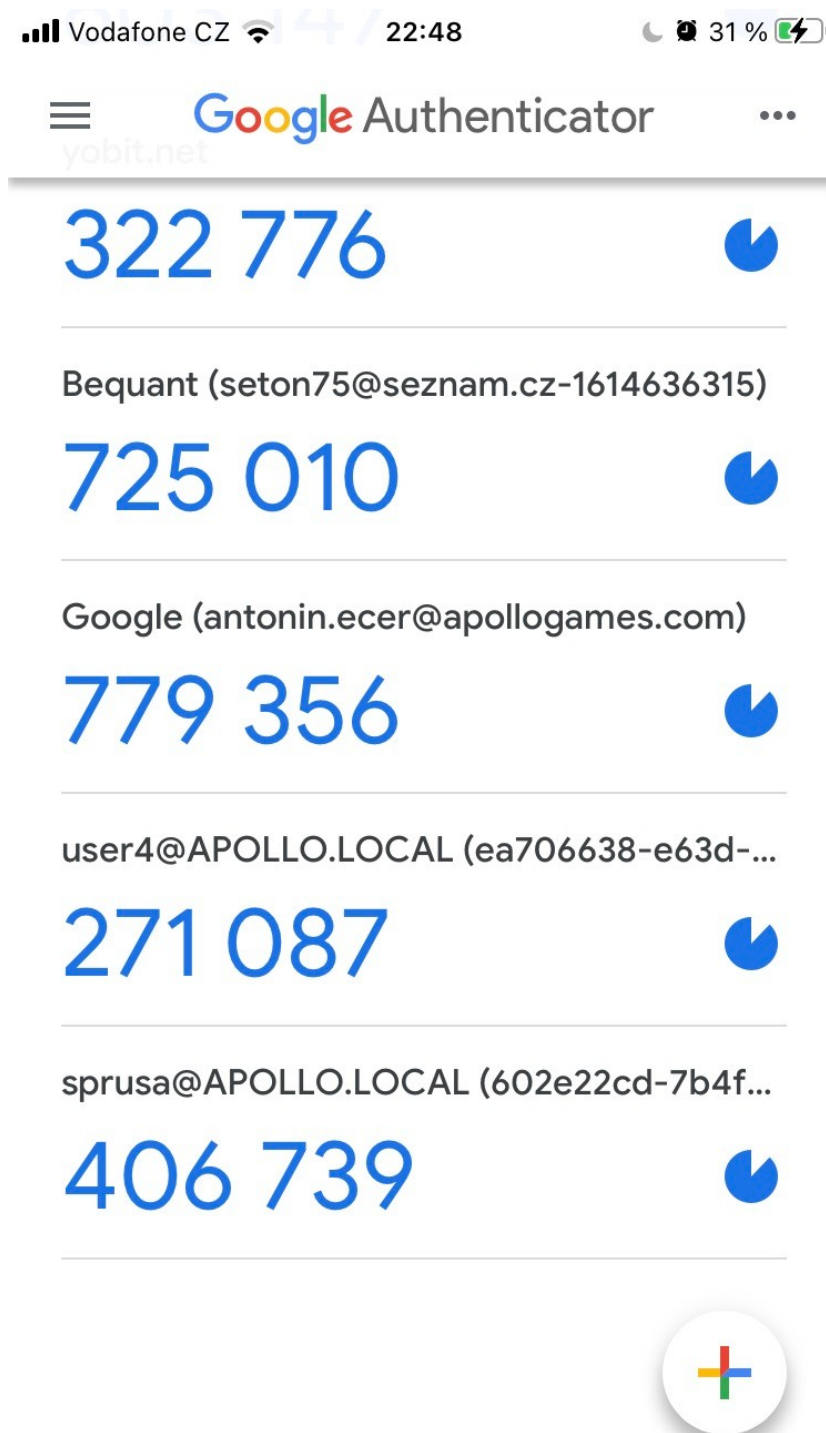
- User login: sprusa
- Password: *****
- Password expiration: 2021-08-29 12:20:31Z
- UID: 1003
- GID: 500
- Principal alias: sprusa@APOLLO.LOCAL
- Kerberos principal expiration: YYYY-MM-DD hh:mm UTC
- Login shell: /bin/bash
- Home directory: /home/sprusa
- SSH public keys: SHA256:UsWwlcq4RRkzKrWYz8aoLWHrlz3wz2zOu1VqyNiOb7c tonda@Tonda (ssh-rsa)
- Certificates:

The 'SSH public keys' section is highlighted with a red circle, indicating the area where new keys can be added.

2FA

OTP – lze použít Google authenticator/ FreeOTP aplikace z app storu

V záložce detailu uživatele v akcích - „Add OTP Token“ - nezapomenout zapnout v sekci „User authentication types“ a pak uložit, poté se k heslu na konec připojí OTP kód
Lze je nalézt i celkově na Authentication – OTP Tokens



Password Policy

Policy – Password Policies

(v závorkách jsou přednastavené hodnoty)

doba (90dní), délka hesla (8), uzamčení po x pokusech(6), reset interval (60sec), auto odemčení (10 min)

Sudo Policy

- nadefinují se povolené příkazy, spojí se do skupin, nadefinují se skupiny hostů(PC), skupiny uživatelů, vytvoří se role (ALL pro uživate/skupinu uživatelů (admins), Any host, any command, nebo přeba jen pro souborové operace – prohlížení logů, kopírování, atd..)

Host-Based Access Control

- nadefinují se povolené služby, spojí se do skupin, nadefinují se skupiny hostů(PC), skupiny uživatelů, vytvoří se role

Standardně připravené 2 role [allow_all](#) a [allow_systemd-user](#)

SELinux User Maps

- defaultně nenastaveno – zde odkaz na konfiguraci <https://blog.delouw.ch/2018/07/02/centrally-manage-selinux-user-mapping-with-freeipa/>

Kerberos Ticket Policy

- defaultně nastavené hodnoty

Max renew (seconds) 604800 = týden

Max life (seconds) 86400 = den

Certifikáty (Dogdag PKI)

https://www.dogtagpki.org/wiki/PKI_Main_Page

Certifikační Autorita + celý životní cyklus certifikátů od založení žádosti po revokování
Authentication - Cetificates

The screenshot shows the freeIPA web interface. The top navigation bar includes 'Soubor', 'Úpravy', 'Zobrazit', 'Historie', 'Záznamy', 'Nástroje', and 'Nápověda'. The main menu on the left has 'Identity Management' selected. The 'Certificates' page is displayed, showing a list of certificates. The table has columns for 'Serial Number', 'Subject', 'Issuing CA', and 'Status'. The table contains 18 entries, all with 'ipa' as the Issuing CA. The status of the certificates varies: 13 are 'VALID', 1 is 'REVOKED', and 4 are 'VALID'.

Serial Number	Subject	Issuing CA	Status
1	CN=Certificate Authority,O=APOLLO.LOCAL	ipa	VALID
2	CN=OCSP Subsystem,O=APOLLO.LOCAL	ipa	VALID
3	CN=ipa.apollo.local,O=APOLLO.LOCAL	ipa	VALID
4	CN=CA Subsystem,O=APOLLO.LOCAL	ipa	VALID
5	CN=CA Audit,O=APOLLO.LOCAL	ipa	VALID
6	CN=ipa-ca-agent,O=APOLLO.LOCAL	ipa	VALID
7	CN=IPA RA,O=APOLLO.LOCAL	ipa	VALID
8	CN=ipa.apollo.local,O=APOLLO.LOCAL	ipa	VALID
9	CN=ipa.apollo.local,O=APOLLO.LOCAL	ipa	VALID
10	CN=ipa.apollo.local,O=APOLLO.LOCAL	ipa	VALID
11	CN=ui14.apollo.local,O=APOLLO.LOCAL	ipa	VALID
12	CN=user4,O=APOLLO.LOCAL	ipa	VALID
13	CN=user4,O=APOLLO.LOCAL	ipa	REVOKED
14	CN=ipa1.apollo.local,O=APOLLO.LOCAL	ipa	VALID
15	CN=ipa1.apollo.local,O=APOLLO.LOCAL	ipa	VALID
16	CN=ipa1.apollo.local,O=APOLLO.LOCAL	ipa	VALID
17	CN=ipa1.apollo.local,O=APOLLO.LOCAL	ipa	VALID
18	CN=ipjanu,O=APOLLO.LOCAL	ipa	VALID

The screenshot shows the freeIPA web interface with the 'Issue New Certificate' dialog box open. The dialog box has fields for 'Principal' (mcevel), 'CA' (ipa), and 'Profile ID' (caIPASvcCert). It also includes a checkbox for 'Add principal' and a text area for the certificate request. The background shows the same 'Certificates' page as the previous screenshot.

Principal: mcevel

CA: ipa

Profile ID: caIPASvcCert

1. Create a certificate database or use an existing one. To create a new database:
certutil -N -d <database path>

2. Create a CSR with subject CN=<common name>,O=<realm>, for example:
certutil -R -d <database path> -a -g <key size> -s "CN=<common name>,O=APOLLO.LOCAL"

3. Copy and paste the CSR (from -----BEGIN NEW CERTIFICATE REQUEST----- to -----END NEW CERTIFICATE REQUEST-----) into the text area below:

```
[admin@ipa tonda]$ sudo certutil -R -d /etc/pki/CA -a -g 2048 -s 'CN=mcevela,O=APOLLO.LOCAL'
[sudo] heslo pro admin:
Enter Password or Pin for "NSS Certificate DB":
```

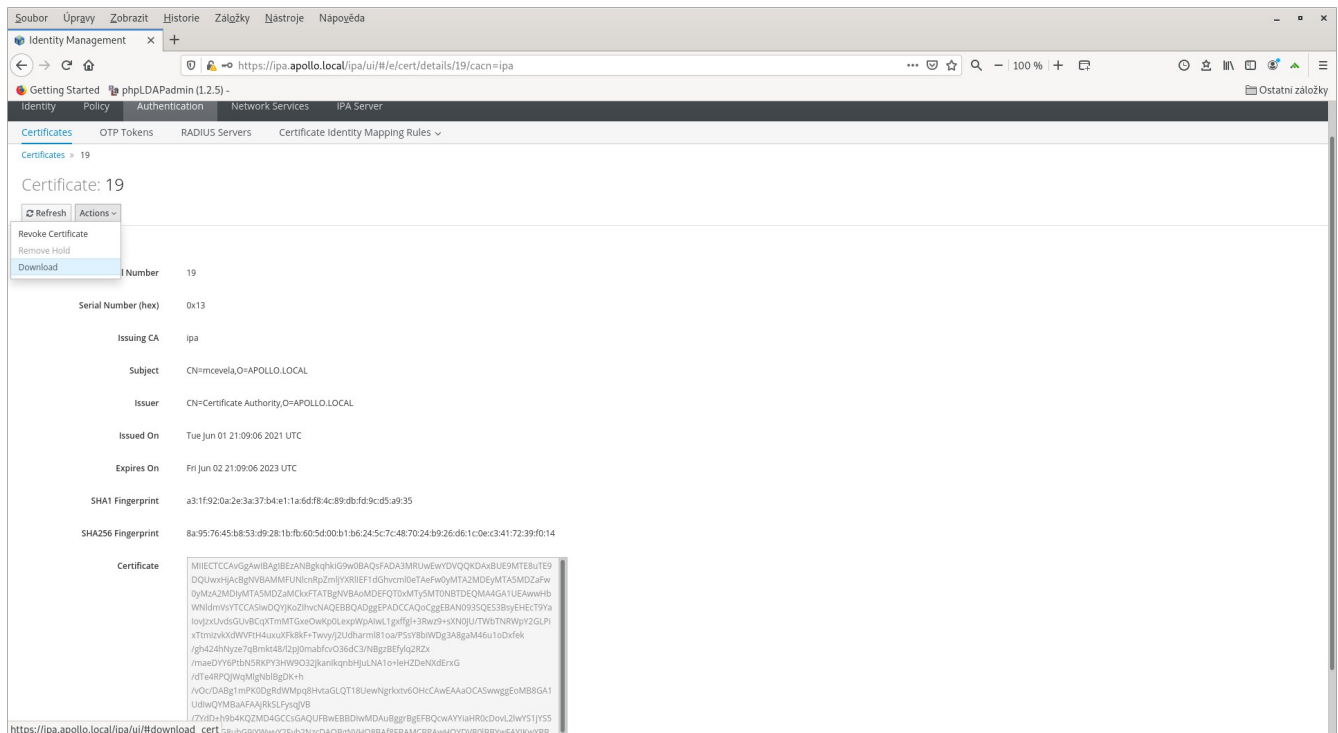
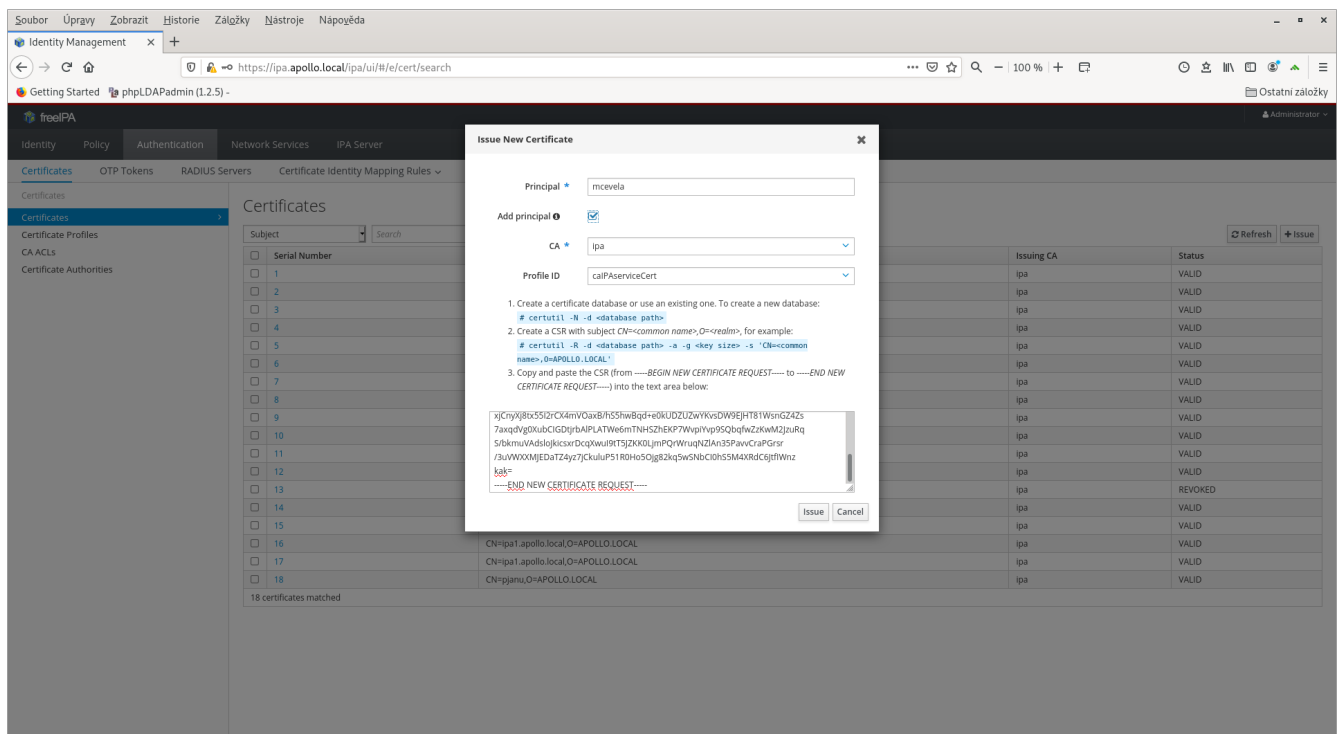
A random seed must be generated that will be used in the creation of your key. One of the easiest ways to create a random seed is to use the timing of keystrokes on a keyboard.

To begin, type keys on the keyboard until this progress meter is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!

Continue typing until the progress meter is full:

```
|*****|

-----BEGIN NEW CERTIFICATE REQUEST-----
MIICbjCCAVYCAQAwKTEVMBMGGA1UEChMMQVBPTExPLkxPQ0FMMRAwDgYDVQQDEwdt
Y2V2ZWxhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3T3dJARLcGzI
QcRxP1hoii8nPFS92wZS8EKpdOYxMbF47AqnQt7GlakAjAvWDF9+CX7dHDP36xc3
QlT9NZtM1FaljYYs+LFO2aLO+Rd1ZUW0fi7G5cWTyQX5PC/L+PZR2FquaXzWhr89
KxjxuJYODcDyBozjq7WgPF96T+CHjbiE3LN7uoGaS3jz+XaknSZpt9y87fp0Lf80
GDMER/KWrZFnH+Zp4Nhjo+1s3lEo9jcdB07fYmRqciSqdscm4s0DWj6V4dkN41d0
SvEb91N7hE9AlaoyWA1uUGAMr6H+85z8MAGDWY8rQOBF1Yymrwe+1oYtBPXxR7A2
CuTG2/o4dwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBANxv/1BUpOdZfbvVw7kc
/t8CEJWw9x1tImnX8/6hLTzuo4HSqMwIlKXVABIG0W6dOLUYyiM0VlM7sqM/OaAC
xjCnyXj8tx55I2rCX4mVOaxB/hS5hwBqd+e0kUDZUZwYKvsDW9EJHT81WsnGZ4Zs
7axqdVg0XubCIGDtjrbAlPLATWe6mTNHSZhEKP7WvpiYvp9SQbqfwZzKwM2JzuRq
S/bkmUvAdslOJkicsxrDcqXwuI9tT5JZKK0LjmPQrWruqNZlAn35PavvCraPGrsr
/3uVWXXMJEDaTZ4yz7jCkuluP51R0Ho5Ojg82kq5wSNbCI0hS5M4XRdC6JtfIWnz
kak=
-----END NEW CERTIFICATE REQUEST-----
```

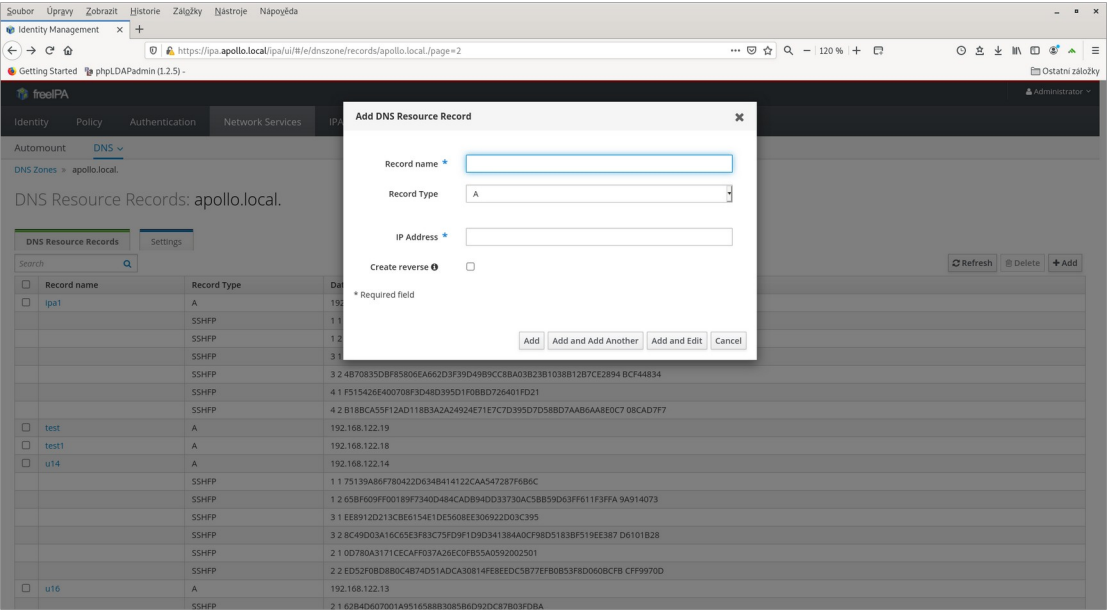
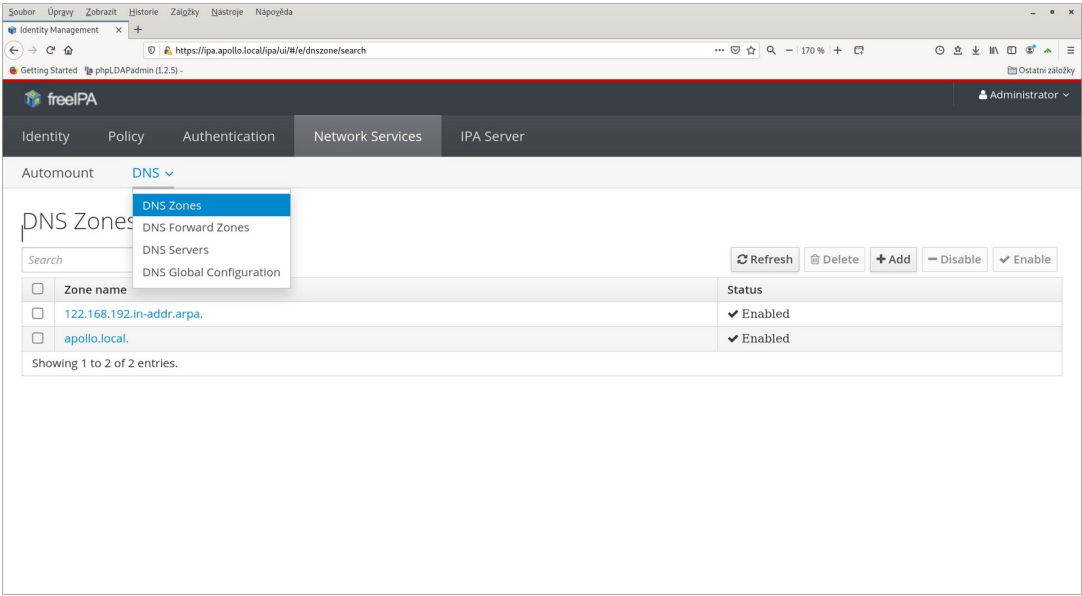


<https://www.freeipa.org/page/Certmonger>

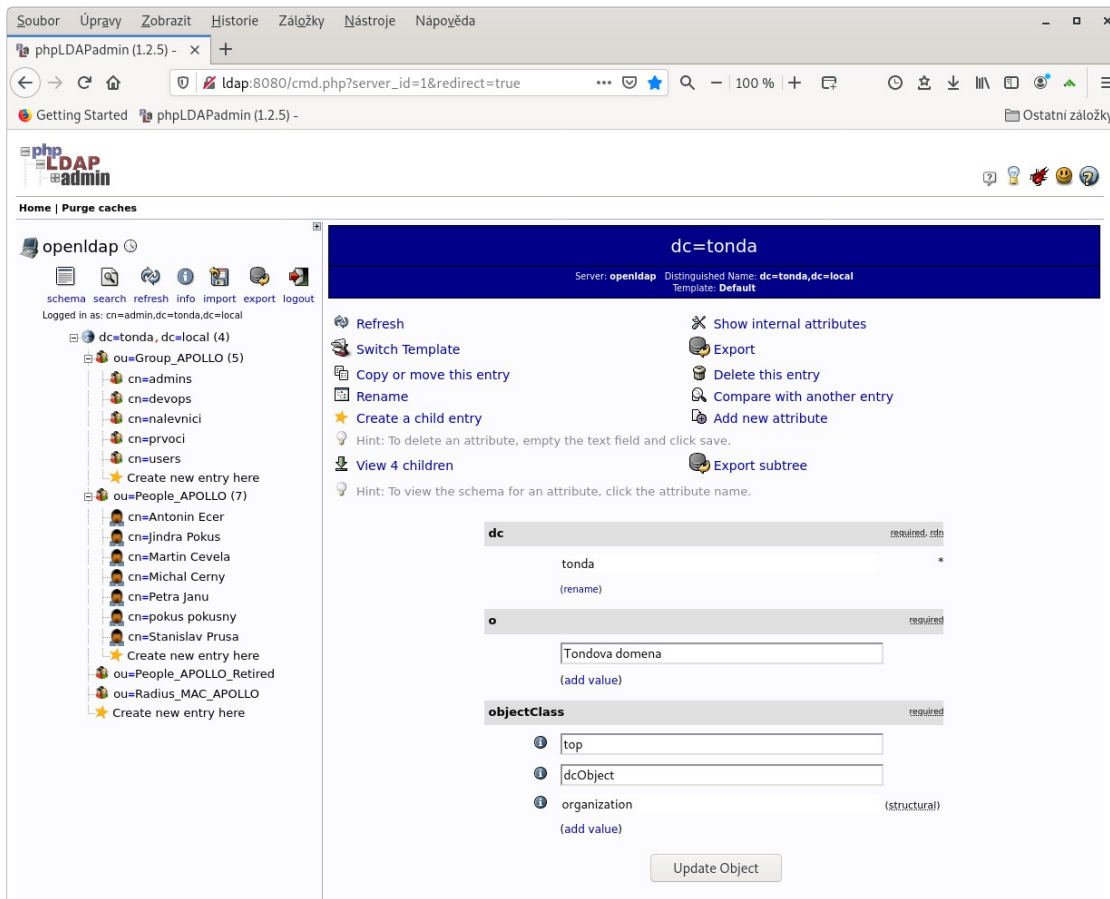
[https://www.freeipa.org/page/V4/Automatic Certificate Request Generation](https://www.freeipa.org/page/V4/Automatic%20Certificate%20Request%20Generation)

<https://www.systutorials.com/docs/linux/man/1-certutil/> (pridani všech parametru stat, email, city atd)

DNS



Migrace z LDAP



ipa migrate-ds --bind-dn="cn=admin,dc=tonda,dc=local" --user-container="ou=People_APOLLO,dc=tonda,dc=local" --user-objectclass="inetOrgPerson" --group-container="ou=Group_APOLLO,dc=tonda,dc=local" --group-objectclass="posixGroup" --with-compat <ldap://ldap.tonda.local>

Všechny ipa příkazy je nutné spouštět pod ipa uživatelem s příslušnými právy(admin)

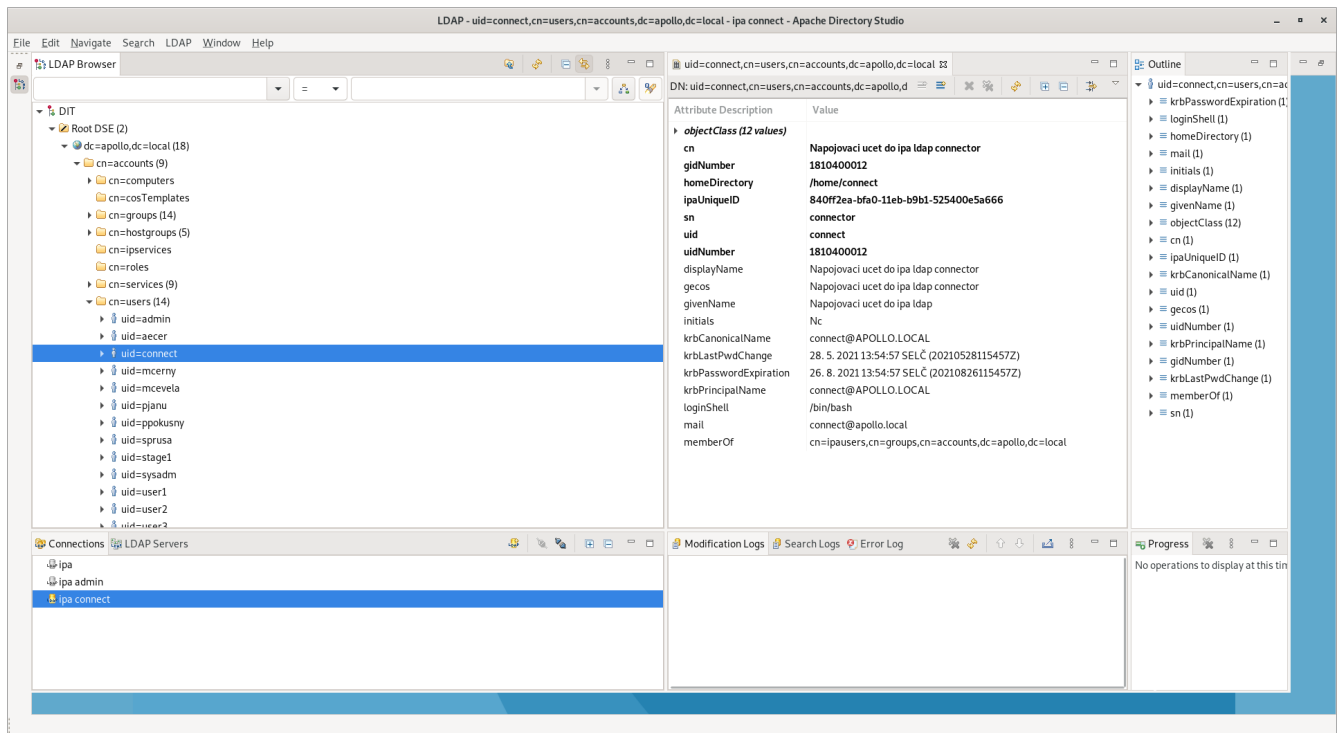
```
-----
migrate-ds:
-----
Migrated:
  group: users, devops
Failed user:
  aecer: This entry already exists
  mcerny: This entry already exists
  mcevela: This entry already exists
Failed group:
  admins: This entry already exists. Check GID of the existing group. Use --group-overwrite-gid option to overwrite the GID
-----
Passwords have been migrated in pre-hashed format.
IPA is unable to generate Kerberos keys unless provided
with clear text passwords. All migrated users need to
login at https://your.domain/ipa/migration/ before they
can use their Kerberos accounts.
```

Pozor sice namigruje skupiny a uživatele, ale ne příslušnost uživatelů ke skupinám, třeba projít a nastavit

Jinak veme hesla z původního LDAPu, lze se přihlásit na vm, když se přidá public key a ještě nebyl přihlášen, rovnou se přihlásí s PK, pokud již byl přihlášen, musí se zadat heslo a odhlásit, po dalším přihlášení již bere PK

Napojení na FreeIPA

Na FreeIPA se lze napojit jak LDAP protokolem, tak přes Kerberos



kinit účet – vystavení kerberos ticketu

klist – kontrola kerberos tiketů