Open Source identity management

FreeIPA

původně I identity P policy A ~~audit~~

Ale IPA zustalo

Kompletní Linux domain controller
Umí integrovat AD jako další zdoj Identit
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 vzdalenych directory autentifikacnich mechanizmu
389 Directory – specielně 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

ipa-server-install
ipa-client-install

Fedora / CentOS / RHEL / Ubuntu (community) – ve versi 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 navzajem 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

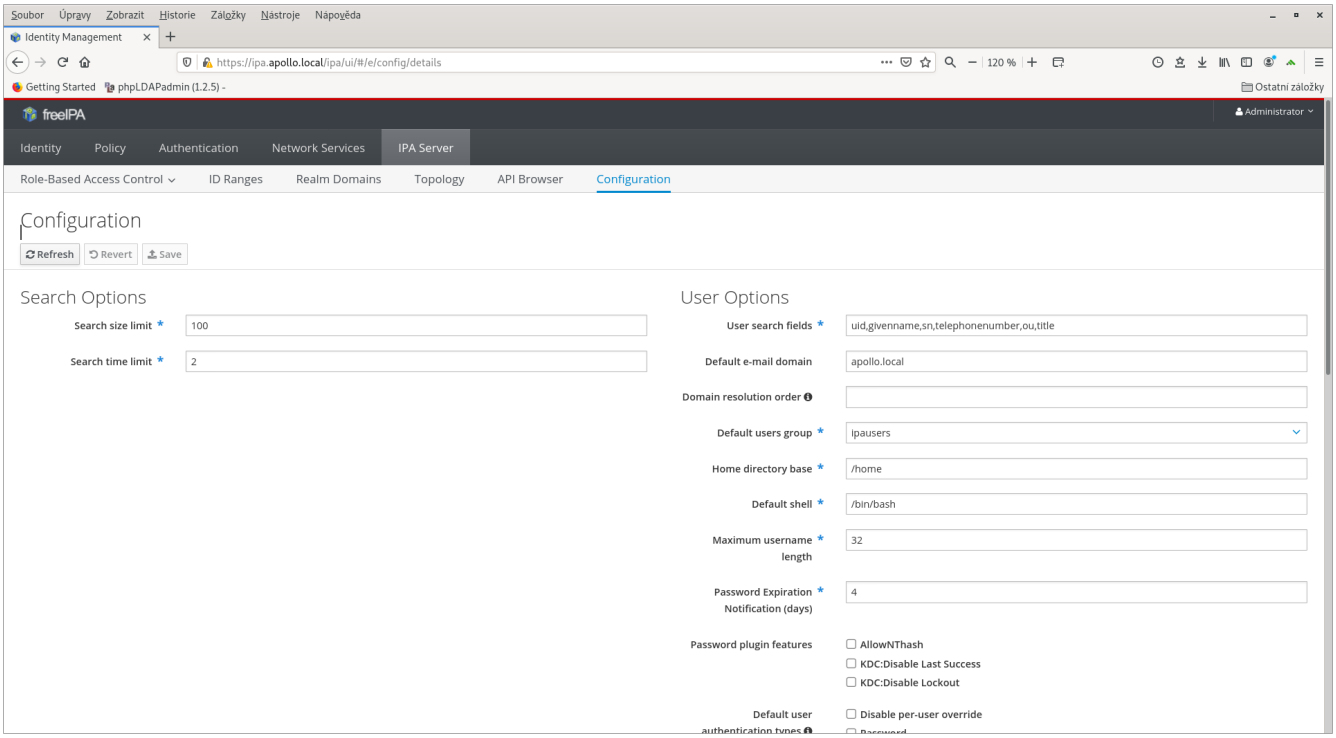
2. na freeipa serveru přidat tento server do skupiny - dělá se pod přihlášením z ldapu(ipi) jinak ipa:
ERROR: neobdrženy ověřovací údaje Kerberos
[admin@ipa ~]$ ipa hostgroup-add-member ipaservers --hosts=ipa1.apollo.local

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}

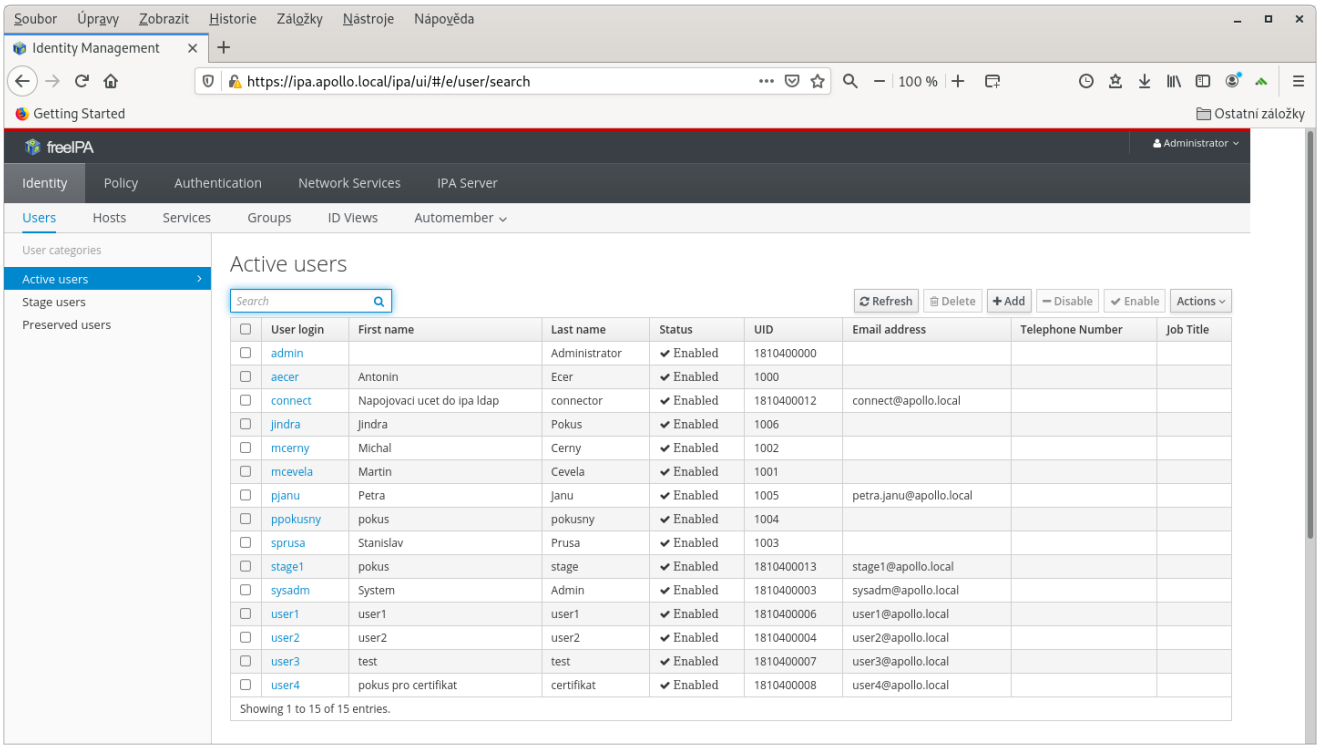
firewall-cmd --reload
yum install ipa-server
sudo ipa-replica-install

To je celé.

Defaultní chování



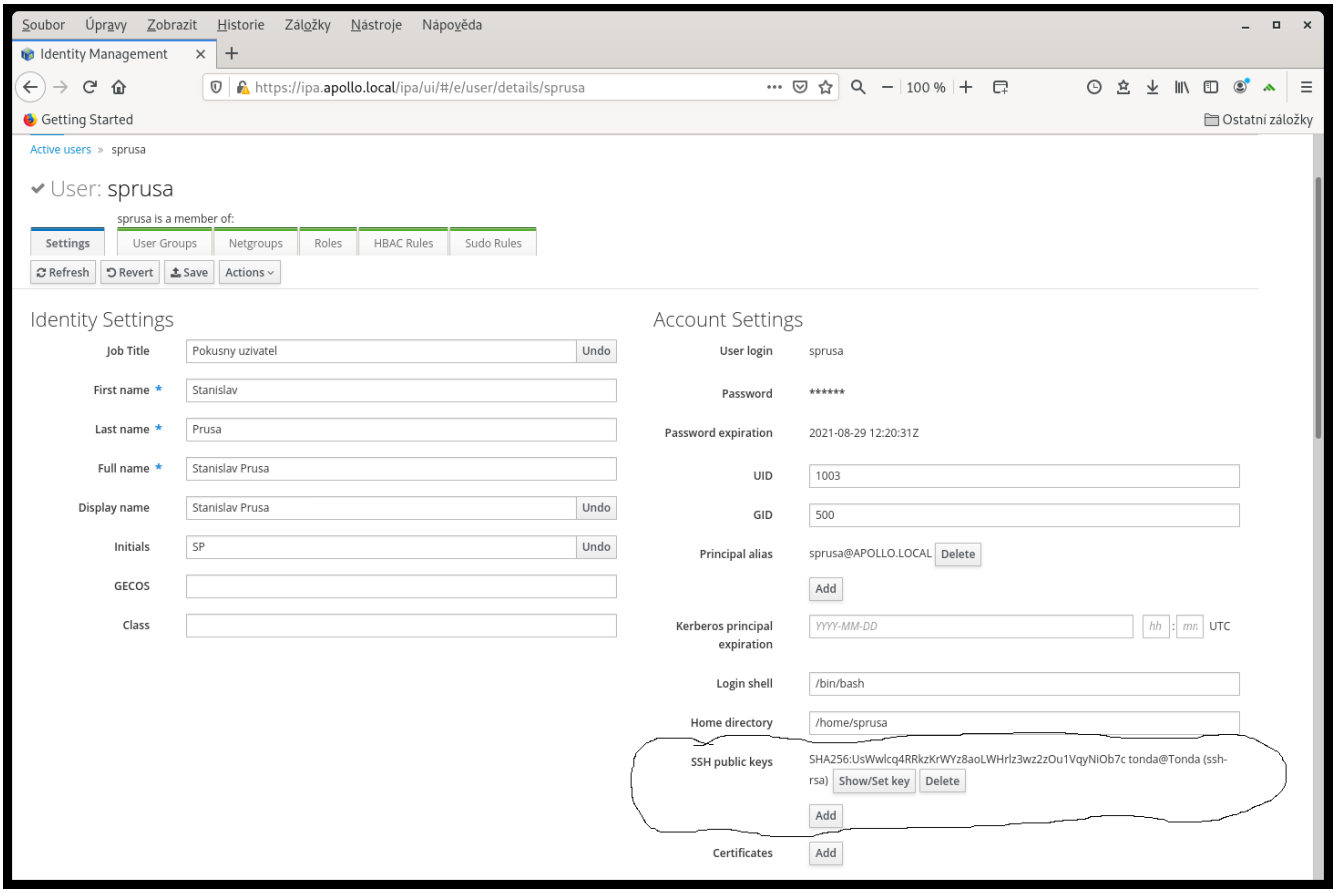
Administrace uživatelů z GUI:



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

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

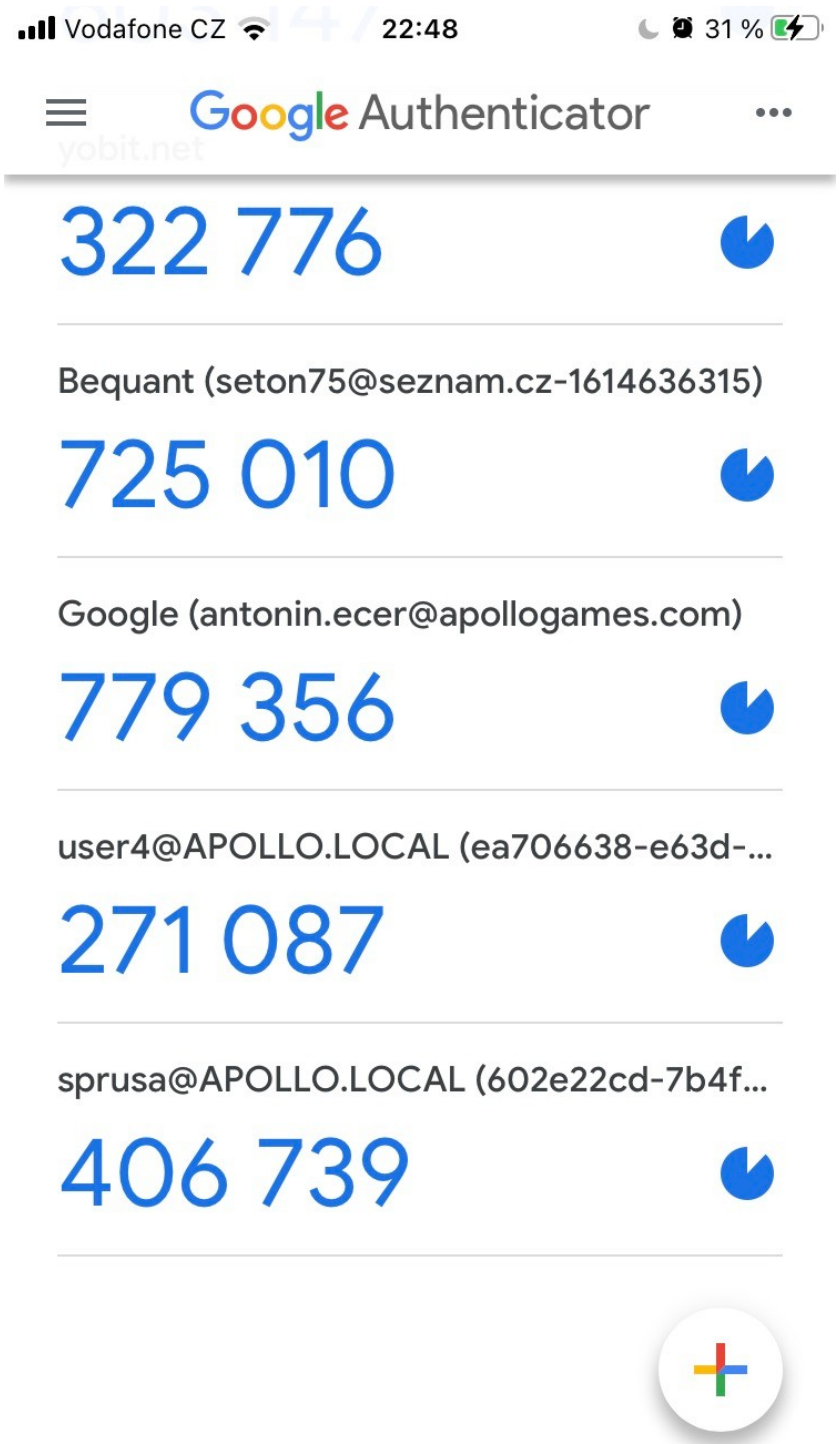
Přidání veřejných ssh klíčů



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

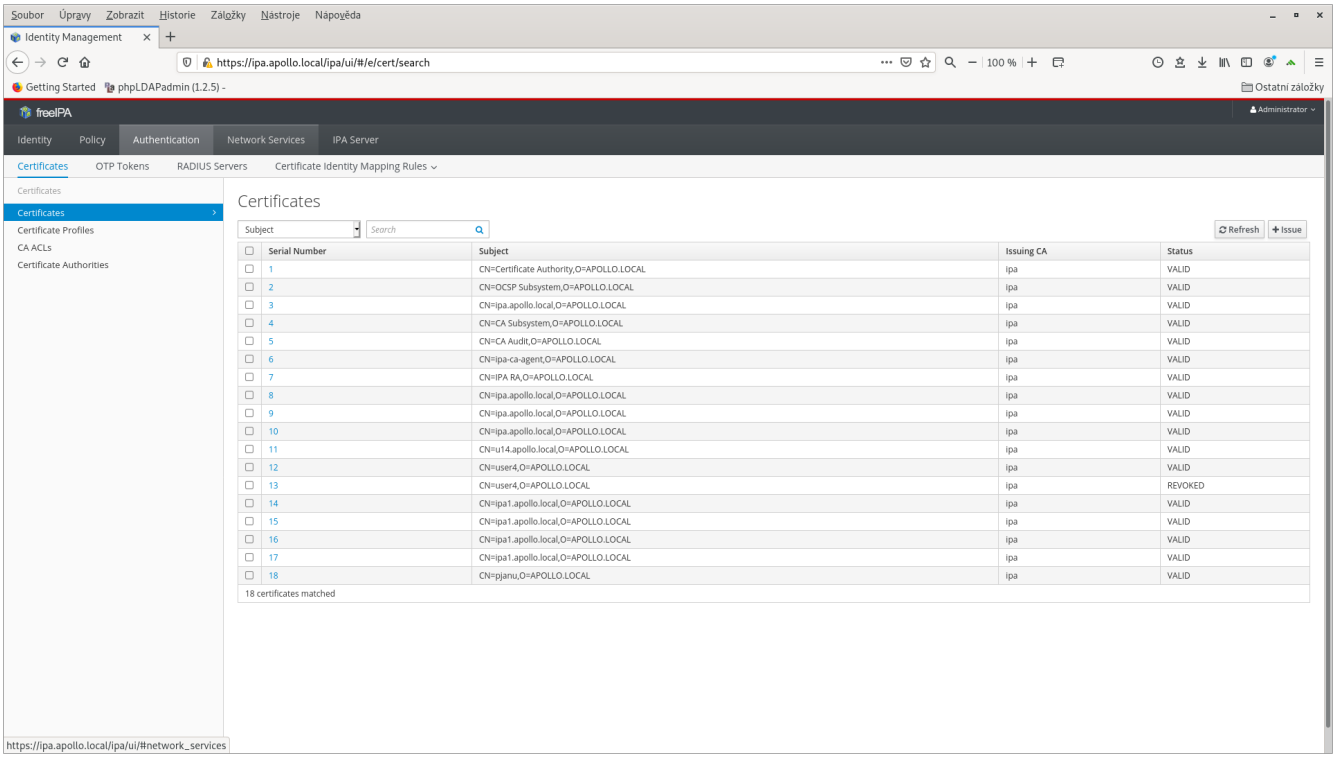
- defaultně nastavené hodnoty
Max renew (seconds) 604800 = týden
Max life (seconds) 86400 = den

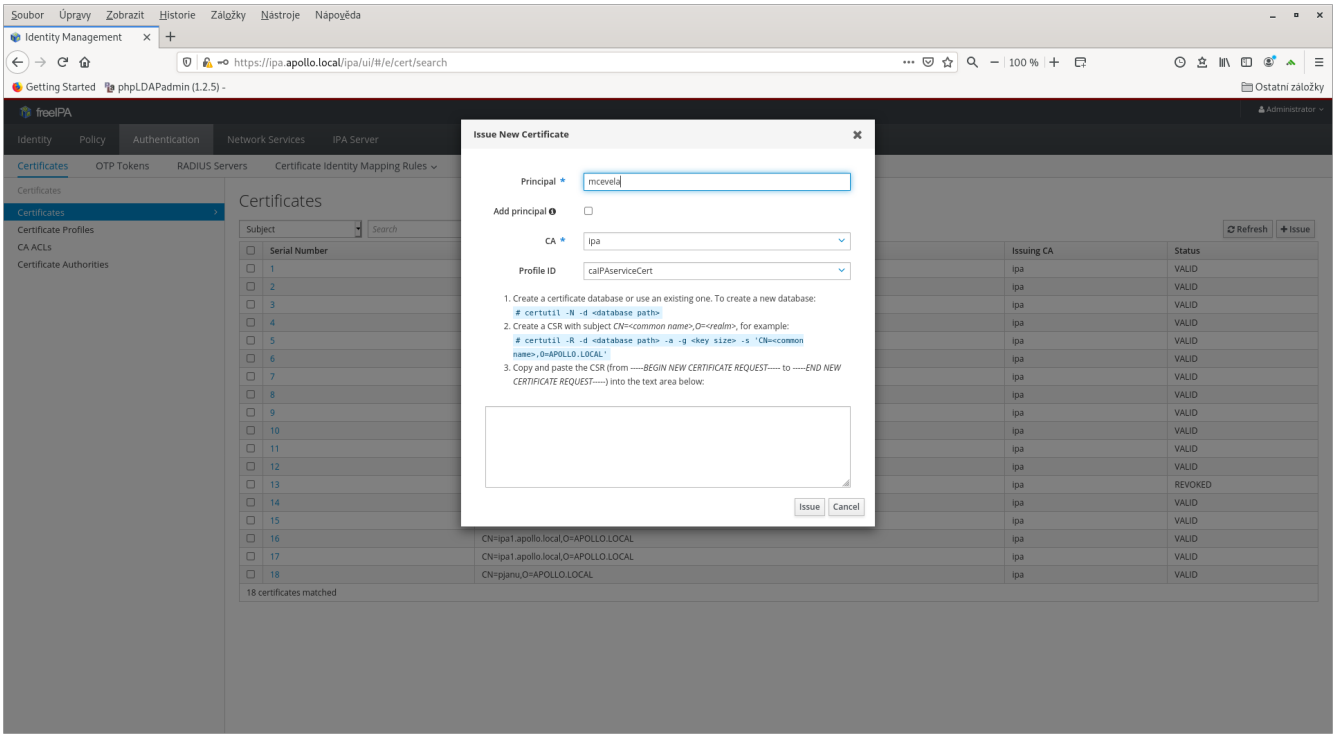
Certifikáty (Dogdag PKI)

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

Certtifikační Autorita + celý životní cyklus certifikátů od založení žádosti po revokování

Authentication - Cetificates





[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":

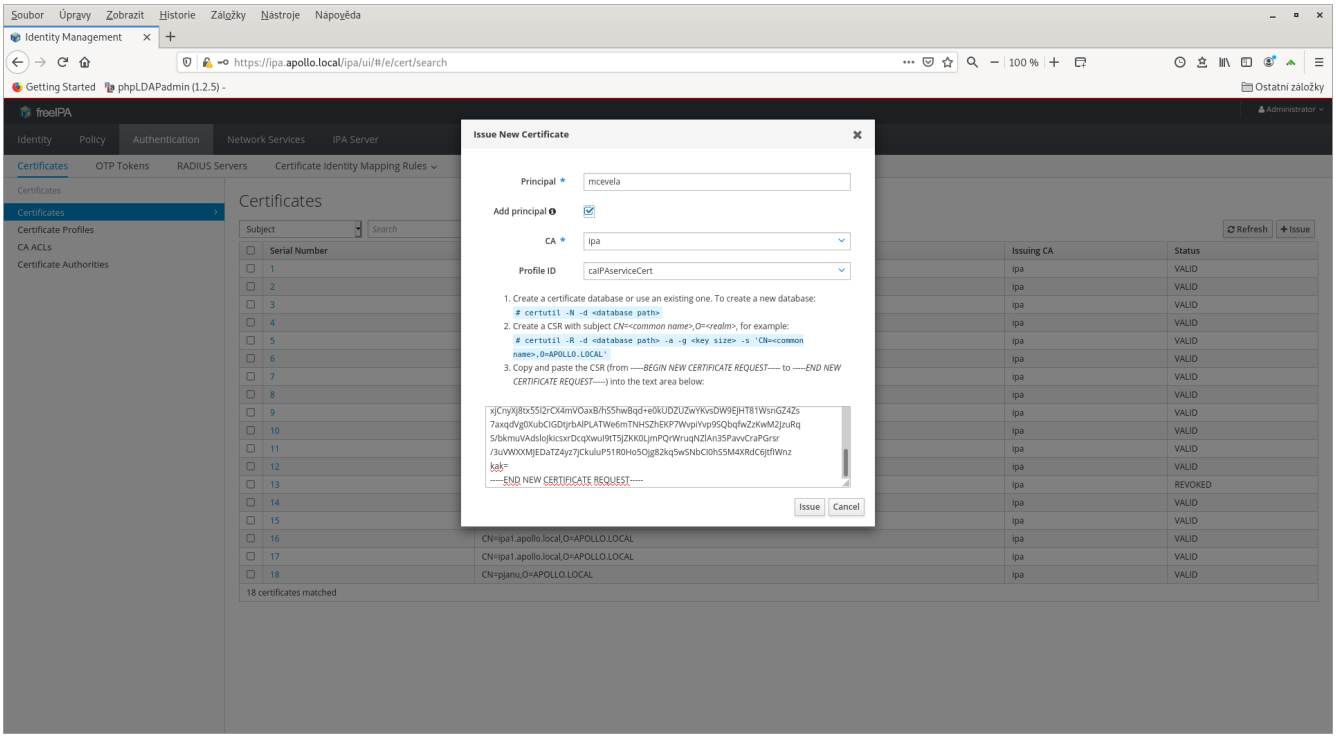
A random seed must be generated that will be used in the
creation of your key. One of the easiest ways to create a
random seed is to use the timing of keystrokes on a keyboard.

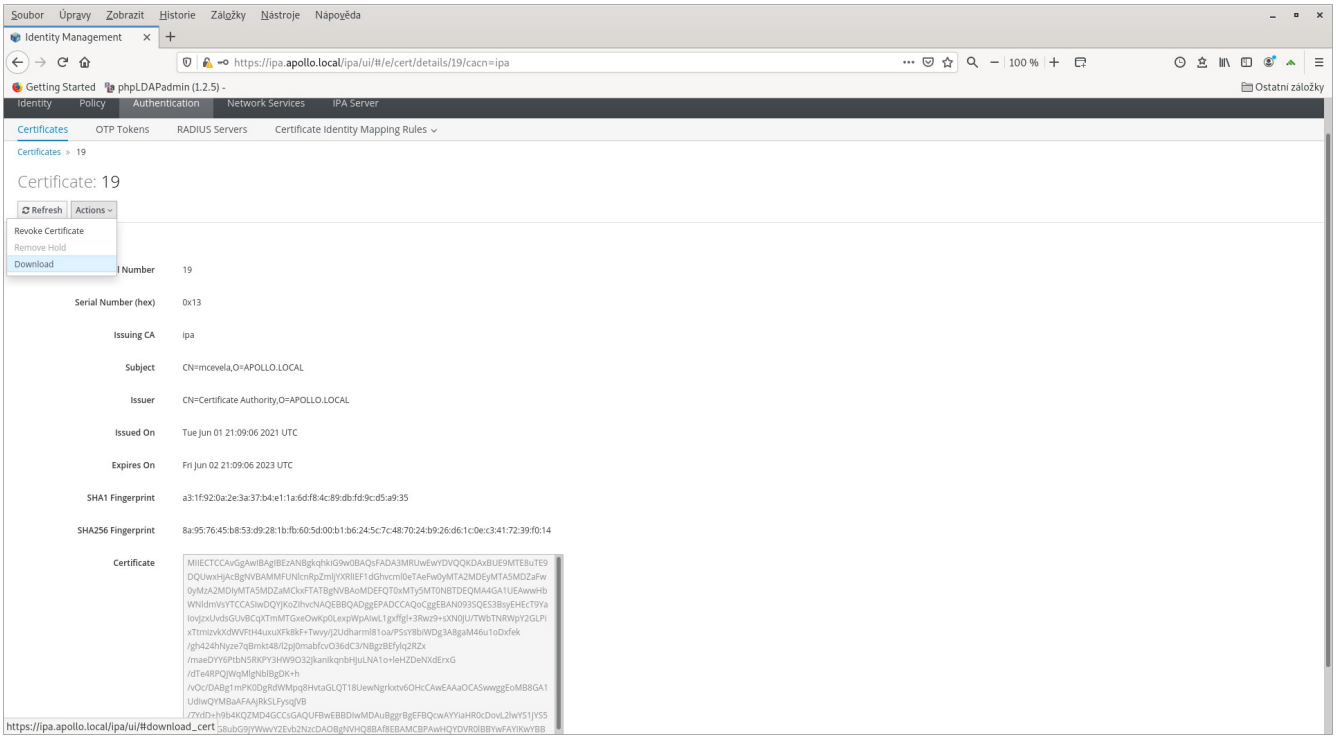
To begin, type keys on the keyboard until this progress meter
is full. DO NOT USE THE AUTOREPEAT FUNCTION ON YOUR KEYBOARD!

Continue typing until the progress meter is full:

|**|

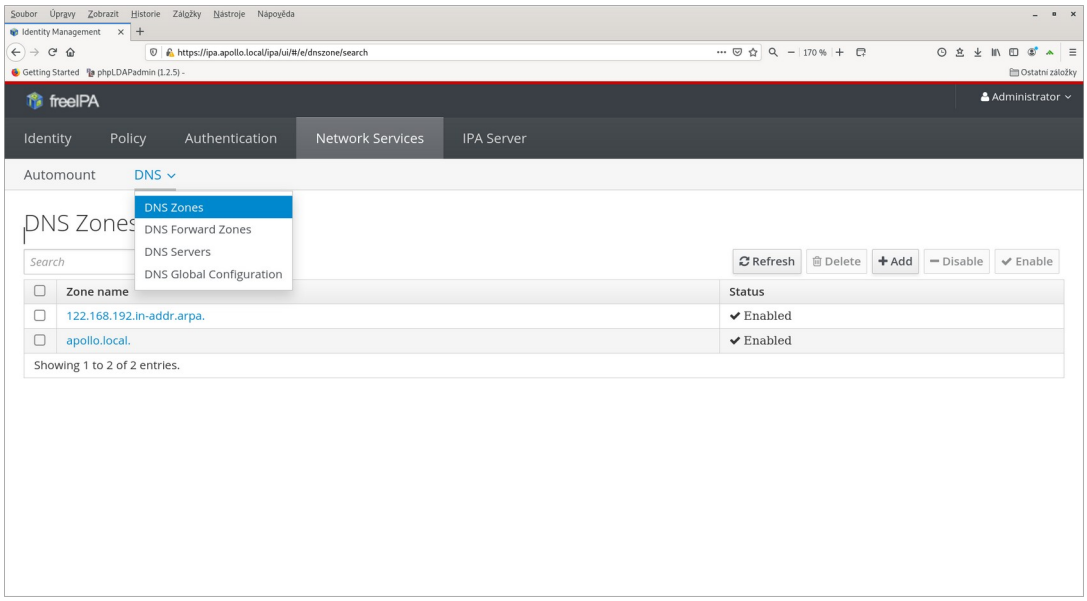
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICbjCCAVYCAQAwKTEVMBMGA1UEChMMQVBPTExPLkxPQ0FMMRAwDgYDVQQDEwdt
Y2V2ZWxhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3T3dJARLcGzI
QcRxP1hoii8nPFS92wZS8EKpdOYxMbF47AqnQt7GlakAjAvWDF9+CX7dHDP36xc3
QlT9NZtM1FaljYYs+LFO2aLO+Rd1ZUW0fi7G5cWTyQX5PC/L+PZR2FquaXzWhr89
KxjxuJYODcDyBozjq7WgPF96T+CHjbiE3LN7uoGaS3jz+XaknSZpt9y87fp0Lf80
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-----

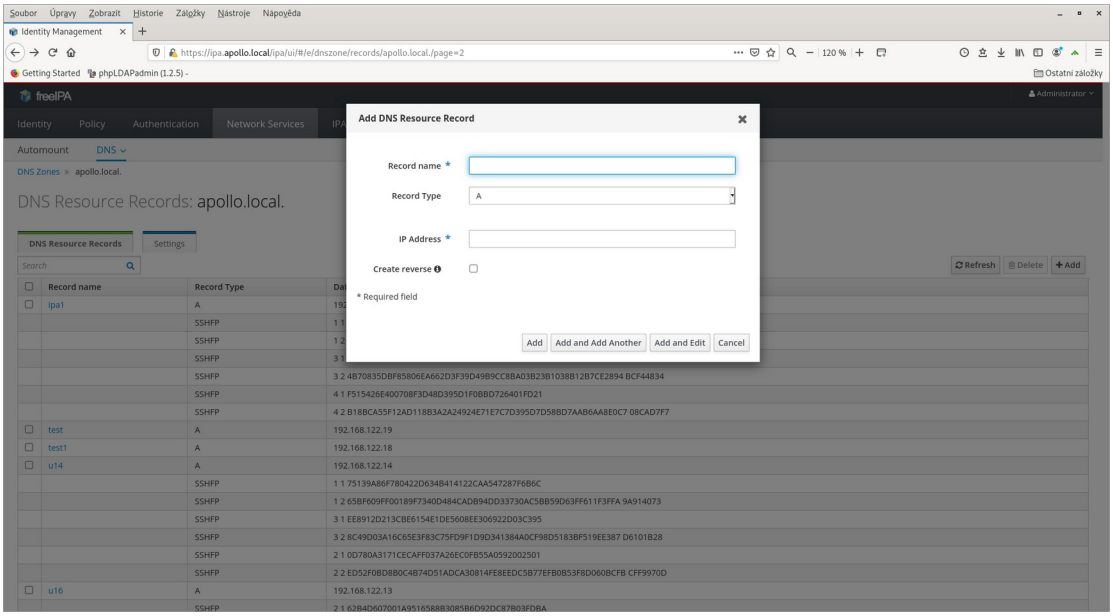




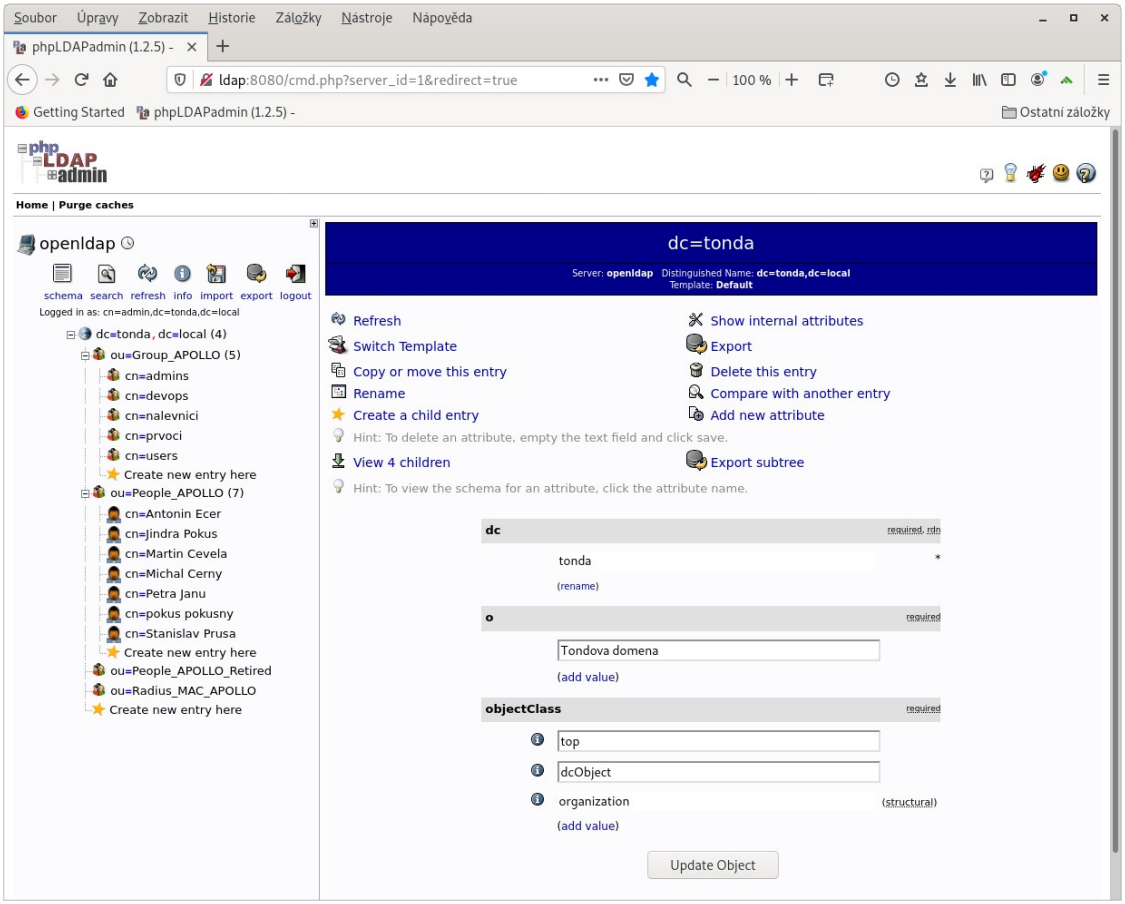
https://www.freeipa.org/page/Certmonger
https://www.freeipa.org/page/V4/Automatic_Certificate_Request_Generation
https://www.systutorials.com/docs/linux/man/1-certutil/ (pridani všech parametru stat, email, city atd)

DNS


freeIPA
Administrator
Identity
Policy
Authentication
Network Services
IPA Server
Automount
DNS
DNS Zones
DNS Forward Zones
DNS Servers
DNS Global Configuration
DNS Zones
Search
Refresh
Delete
Add
Disable
Enable
Zone name
Status
122.168.192.in-addr.arpa.
Enabled
apollo.local.
Enabled
Showing 1 to 2 of 2 entries.


Add DNS Resource Record
Record name *
Record Type
A
IP Address *
Create reverse
* Required field
Add
Add and Add Another
Add and Edit
Cancel
DNS Resource Records: apollo.local.
DNS Resource Records
Settings
Refresh
Delete
Add
Record name
Record Type
ipa1
test
test1
ut4
ut6

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)

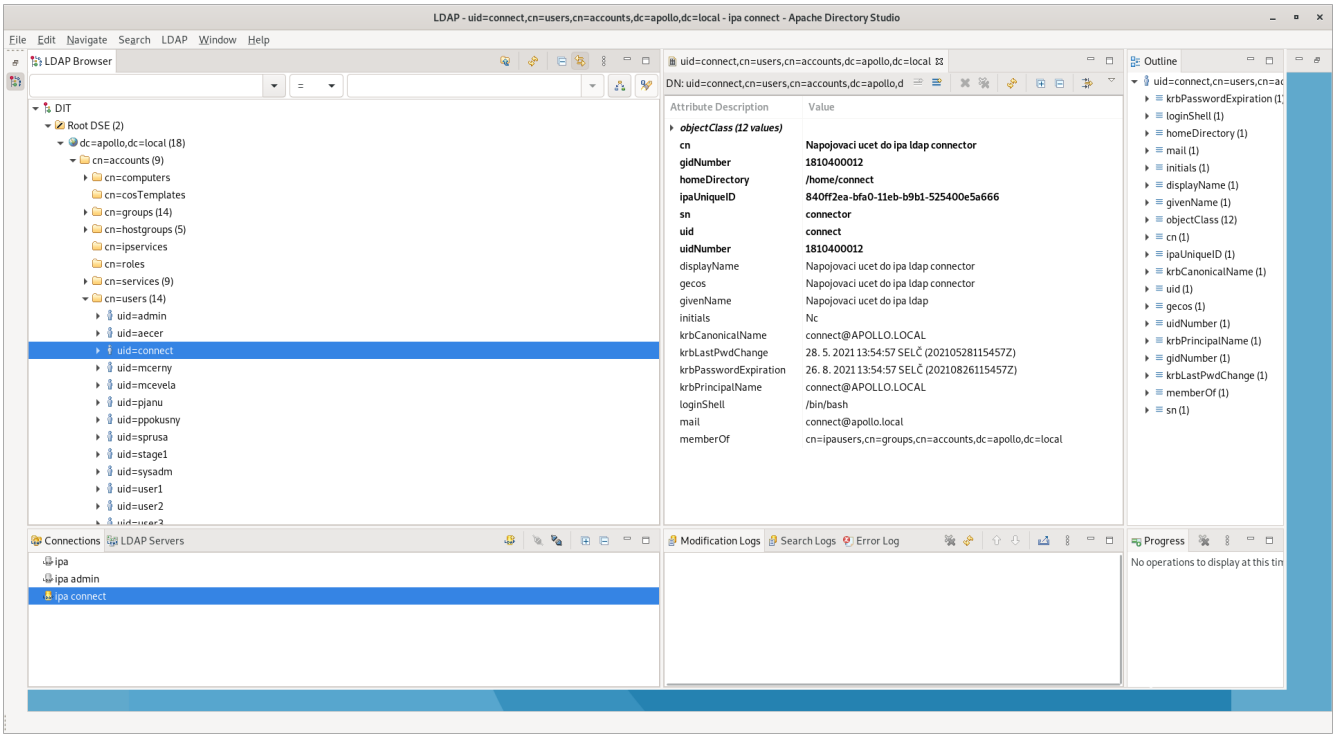
```
-----------
migrate-ds:
-----------
Migrated:
  group: users, devops
Failed user:
  aecer: This entry already exists
  mcerny: This entry already exists
  mcevela: This entry already exists
Failed group:
  admins: This entry already exists. Check GID of the existing group. Use --group-overwrite-gid 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 učet – vystavení kerberos ticketu
klist – kontrola kerberos tiketů