# FreeIPA: jedno logowanie dla wszystkich linuksów

**Poziom: podstawy** **Dotyczy: FreeIPA, sekcja tej książki** **Czas: ~15 min**

*Ta strona otwiera w tej książce sekcję o FreeIPA: skąd wziął się pomysł na własną domenę tożsamości dla linuksów, z jakich starszych projektów FreeIPA faktycznie się składa i dlaczego Zielona trzyma ją osobno od Active Directory, zamiast dołączać każdy serwer wprost do AD.*

### Skróty użyte na tej stronie (12)

| Skrót | Co znaczy |
|---|---|
| **AD** | Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie |
| **DNS** | Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP |
| **GPO** | Group Policy Object: zestaw ustawień wypychanych z Active Directory na komputery |
| **IdM** | Identity Management: nazwa produktu Red Hata, płatnej i wspieranej wersji otwartego, darmowego FreeIPA |
| **IPA** | Identity, Policy, Audit, czyli tożsamość, polityka i audyt: rozwinięcie nazwy FreeIPA, opisujące trzy warstwy, które projekt łączy w jednej instalacji |
| **IT** | Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy |
| **KDC** | Key Distribution Center: serwer Kerberosa wydający bilety logowania |
| **LDAP** | Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA) |
| **MIT** | MIT License: bardzo liberalna licencja wolnego oprogramowania, pozwala na dowolne użycie i modyfikację kodu |
| **NIS** | Network Information Service: przestarzały, mało bezpieczny mechanizm centralnej tożsamości w Unixie sprzed czasów LDAP i Kerberosa, który systemy takie jak FreeIPA miały zastąpić |
| **RHEL** | Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa |
| **SSSD** | System Security Services Daemon: usługa na kliencie linuksowym tłumacząca logowanie, sudo i sprawdzanie grup na zapytania do katalogu, czy to FreeIPA, czy Active Directory |

# Skąd się wzięło

Nazwa IPA rozwija się jako Identity, Policy, Audit, czyli tożsamość, polityka i audyt: trzy warstwy, które FreeIPA miała połączyć w jedną instalację zamiast trzech osobnych systemów. Projekt sponsoruje Red Hat, dla którego FreeIPA jest wersją upstream, otwartą podstawą płatnego produktu Red Hat Identity Management (IdM) dostępnego w RHEL. Pierwsza wersja, FreeIPA v1, ukazała się w kwietniu 2008 roku jako odpowiedź na dwa problemy naraz: firmy odchodziły wtedy od przestarzałego NIS, a utrzymanie własnej instalacji LDAP i Kerberosa od zera było na tyle kosztowne, że niewielu administratorów chciało się w to angażować w pojedynkę.

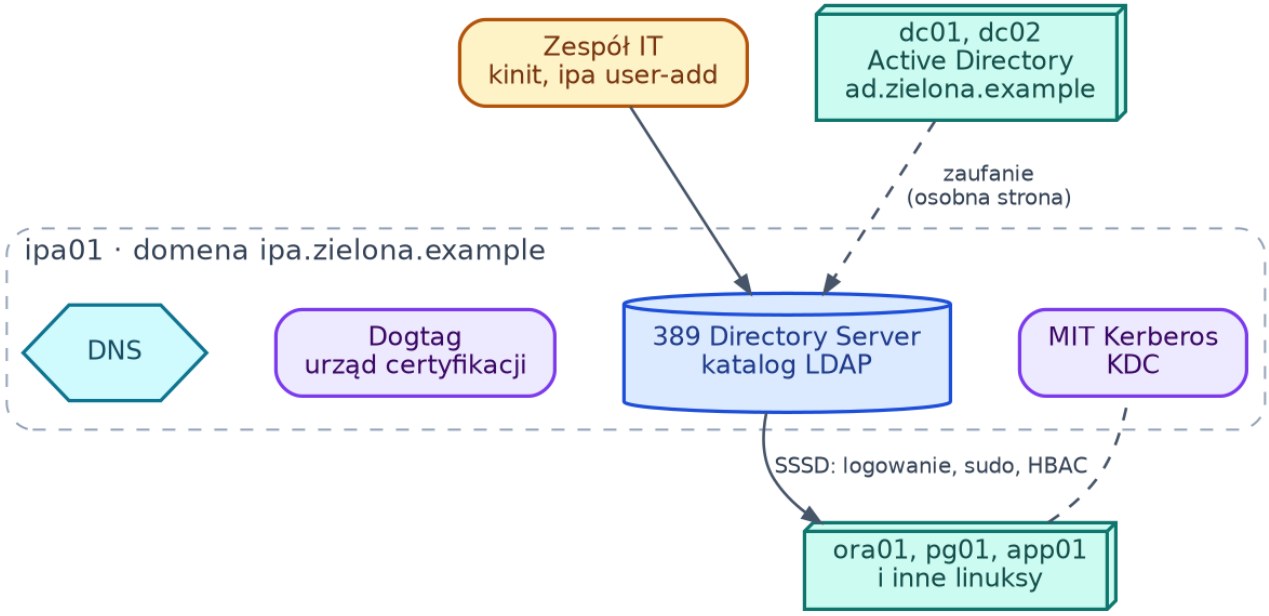
FreeIPA nie napisano od zera. Złożono ją z kilku dojrzałych projektów, z których każdy miał już swoją historię. Katalog LDAP to 389 Directory Server, którego rodowód sięga 1996 roku, gdy zespół `SLAPD` z Uniwersytetu Michigan trafił do Netscape Communications i tam powstał Netscape Directory Server. Prawa do kodu przechodziły później przez AOL i Suna, aż Red Hat odkupił je od AOL i 1 czerwca 2005 roku wydał źródła jako wolne oprogramowanie, najpierw pod nazwą Fedora Directory Server. W maju 2009 roku projekt zmienił nazwę na 389 Directory Server, od numeru portu, na którym LDAP domyślnie nasłuchuje, żeby nazwa nie kojarzyła się wyłącznie z Fedorą.

> **Pojęcie: MIT Kerberos.** Protokół uwierzytelniania z biletami, zamiast wysyłania hasła przy każdym logowaniu, opracowany w latach osiemdziesiątych na MIT w ramach projektu Athena. To ten sam protokół, którego używa Active Directory, opisany na stronie Dołączenie do domeny AD przez realmd, FreeIPA korzysta z niezmienionej implementacji referencyjnej MIT, a nie z własnej.

Urząd certyfikacji FreeIPA, Dogtag, ma podobny rodowód co katalog LDAP: wywodzi się z komercyjnego Netscape Certificate Management System, przejętego i otwartego przez Red Hata w tej samej fali co katalog, na przełomie lat dwutysięcznych. Ostatnim elementem układanki jest SSSD, czyli usługa działająca po stronie każdego klienta linuksowego, tłumacząca zapytania systemu (logowanie, `sudo`, `id`) na zapytania do katalogu, niezależnie od tego, czy katalogiem zarządzającym jest FreeIPA czy Active Directory. Obecna wersja FreeIPA to 4.13.4, wydana we wrześniu 2026 roku.

# Jak to działa w jednym obrazku

Serwer FreeIPA łączy w jednej instalacji katalog LDAP, ośrodek Kerberosa, urząd certyfikacji i serwer DNS, więc dołączony do niego linux rozwiązuje przez jeden system i tożsamość, i uwierzytelnianie, i certyfikaty.




*Serwer FreeIPA na ipa01 łączący katalog LDAP, Kerberos KDC, urząd certyfikacji Dogtag i DNS, z linuksami dołączonymi przez SSSD i osobną domeną Active Directory obok (kliknięcie otwiera pełny rozmiar)*

# Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Zima 2023 roku. Zespół IT Zielonej dokłada kolejne serwery linuksowe, `ora01`, `pg01`, `app01`, `docker01`, każdy z osobnym kontem lokalnym `admin`. Odejście jednej osoby z zespołu oznacza zmianę hasła na dziewięciu maszynach po kolei, a audytor pan Wojtek pyta, skąd wiadomo, kto miał dostęp do `ora01` w marcu, skoro logowania szły przez wspólne konto.

Zielona mogła dołączyć każdy z tych serwerów wprost do istniejącej domeny `ad.zielona.example` przez `realmd`, tak jak opisuje strona Dołączenie do domeny AD przez realmd, i to nadal jest właściwy wybór dla pojedynczej maszyny, która tylko od czasu do czasu potrzebuje logowania kontem domenowym. Zespół wybrał jednak osobną domenę FreeIPA, `ipa.zielona.example`, dla serwerów, którymi administruje na co dzień, bo reguły `sudo` i `HBAC` (kto może się zalogować na który host) zarządza się w FreeIPA centralnie z jednego miejsca, bez pisania GPO, które i tak słabo rozumieją format plików `sudoers`.

| Cecha | FreeIPA (`ipa.zielona.example`) | Dołączenie wprost do AD (`realmd`) |
|---|---|---|
| Dla czego zbudowana | linuksy i usługi, natywnie | Windows, linux dołącza jako gość |

| Cecha | FreeIPA (`ipa.zielona.example`) | Dołączenie wprost do AD (`realmd`) |
|---|---|---|
| Reguły `sudo` i logowania (HBAC) | centralnie w katalogu, jedna zmiana widoczna wszędzie | przez GPO albo ręcznie per host |
| Certyfikaty dla usług linuksowych | wbudowany urząd certyfikacji Dogtag | osobny AD CS albo zewnętrzny urząd |
| Źródło kont | osobne konta w FreeIPA, albo zaufanie do AD, patrz FreeIPA i Active Directory: zaufanie między domenami | te same konta co na Windows, jedno źródło tożsamości |
| Liczba domen Kerberos w firmie | druga domena obok AD, wymaga zaufania dla wspólnych kont | jedna domena, mniej elementów do utrzymania |
| Typowy wybór w Zielonej | serwery administrowane na co dzień (`ora01`, `pg01`, `app01`...) | maszyna dołączona okazjonalnie, bez własnych reguł `sudo` |

# Mapa tej książki

Poniższa mapa obejmuje strony poświęcone samemu FreeIPA. Reszta tej książki, Gitea, NetBox i NetWorker, ma własne, osobne strony opowieści.

| Strona | Na jakie pytanie odpowiada |
|---|---|
| FreeIPA: jedno logowanie dla wszystkich linuksów | Skąd wziął się FreeIPA i czym różni się od zwykłego dołączenia do AD |
| Instalacja serwera FreeIPA na ipa01 | Jak postawić własną domenę tożsamości dla linuksów Zielonej |
| FreeIPA i Active Directory: zaufanie między domenami | Jak połączyć obie domeny, żeby konta z AD działały też na linuksach |
| FreeIPA | Codzienna praca: użytkownicy, grupy, reguły sudo i HBAC, bilety Kerberosa |

**Powiązane:** Dołączenie do domeny AD przez realmd · FreeIPA · Świat przykładów: Zielona

**Źródła:** en.wikipedia.org/wiki/FreeIPA · en.wikipedia.org/wiki/389_Directory_Server · freeipa.org/page/IPA_v1_Release · freeipa.org/About.html · dogtagpki.org/wiki/PKI_History

---

Revision #22
Created 2026-09-28 17:15:41 UTC by Tomasz Konieczny
Updated 2026-10-26 14:14:48 UTC by Tomasz Konieczny