FreeIPA

Opowieść, instalacja serwera i zaufanie z Active Directory.

- FreeIPA: jedno logowanie dla wszystkich linuksów
- Instalacja serwera FreeIPA na ipa01
- FreeIPA i Active Directory: zaufanie między domenami

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.

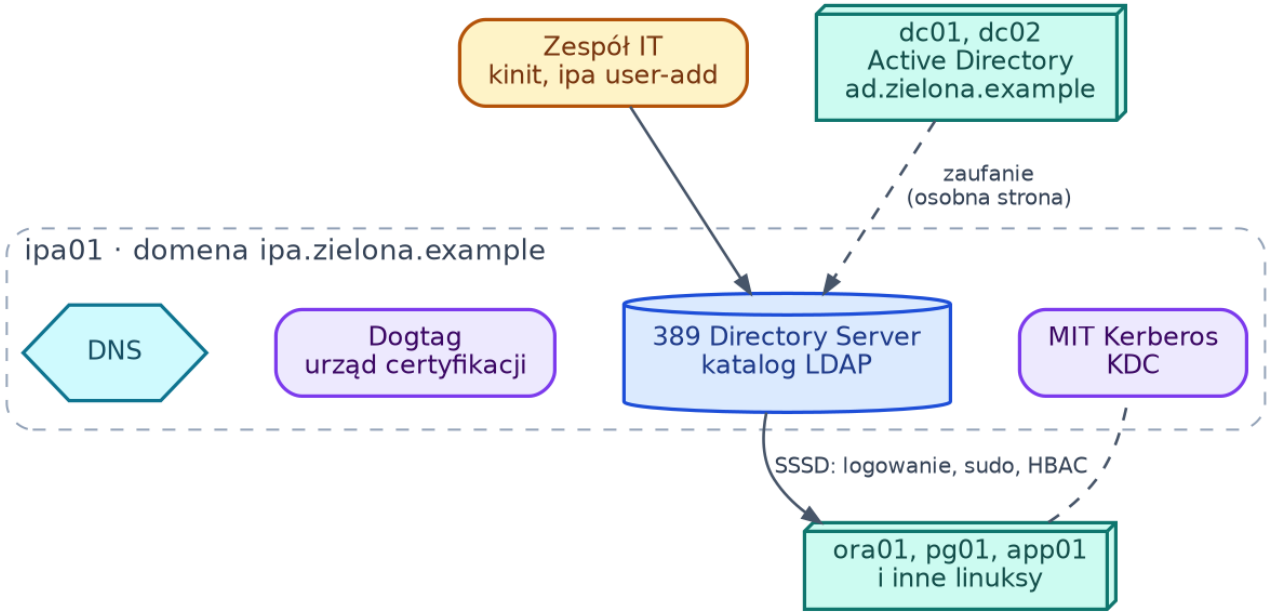
FreeIPA nie napisano od zera. Złożono ją z kilku dojrzałych projektów, z których każdy miał już swoją historię. Katalog LDAP to 389 Directory Server, którego rodowód sięga 1996 roku, gdy zespół `SLAPD` z Uniwersytetu Michigan trafił do Netscape Communications i tam powstał Netscape Directory Server. 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

Instalacja serwera FreeIPA na ipa01

Typ: procedura **Dotyczy: FreeIPA 4.x, Rocky Linux 9** **Czas: ~50 min**

Efekt: działający serwer FreeIPA z własną domeną `ipa.zielona.example`, zintegrowanym DNS, pierwszym kontem administratora i gotowy do dołączania kolejnych linuksów Zielonej. Dołączenie pojedynczego klienta opisuje strona FreeIPA, tutaj skupiamy się na samym serwerze, replice i kopii.

Skróty użyte na tej stronie (11)

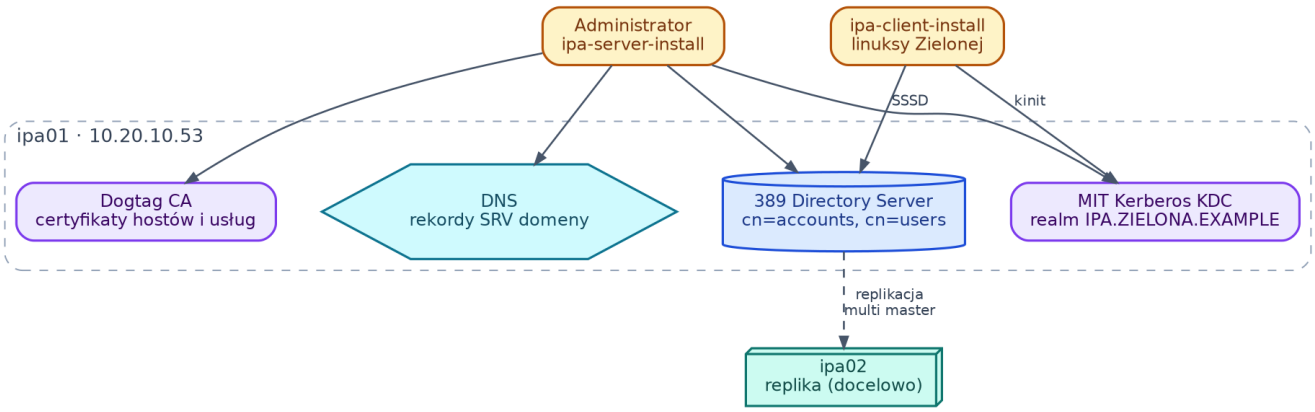
Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
CA	Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
HBAC	Host-Based Access Control: reguły FreeIPA mówiące, kto może się zalogować na który serwer
IdM	Identity Management: nazwa produktu Red Hata, płatnej i wspieranej wersji otwartego, darmowego FreeIPA
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
RHEL	Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa
SRV	rekord DNS wskazujący nie adres hosta, tylko usługę i port, pod którym jej szukać, np. kontroler domeny w sieci

Zanim zaczniemy

Komendy wykonujemy z CLI bash jako user z uprawnieniami sudo albo root, na świeżym Rocky Linux 9. Nazwa domeny i realm ustalamy raz, przed instalacją: zmiana ich później oznacza w

praktyce instalację od zera.

Wymaganie	Jak sprawdzić
Pełna, rozwiązywalna nazwa hosta (FQDN)	`hostnamectl`, u nas `ipa01.ipa.zielona.example`
DNS rozwiązuje tę nazwę w obie strony (do przodu i wstecz)	`dig +short ipa01.ipa.zielona.example`, `dig +short -x 10.20.10.53`
Zsynchronizowany zegar	`chronyc tracking`, pole *System time* poniżej kilku sekund
Porty 80, 443, 389, 636, 88, 464 i 53 wolne i otwarte na firewallu	patrz krok 5
Silne hasło Directory Managera i konta admin przygotowane z góry	osobne od siebie, oba trafiają do menedżera haseł zespołu



Serwer FreeIPA na ipa01 złożony z 389 Directory Server, MIT Kerberos KDC, Dogtag CA i DNS, z klientami dołączanymi przez ipa-client-install i docelową repliką ipa02 (kliknięcie otwiera pełny rozmiar)

Uważaj: `ipa-server-install` zakłada nową domenę Kerberos i nowy katalog LDAP od zera. Jeżeli host ma już zainstalowane jakiekolwiek starsze dane FreeIPA albo inny katalog LDAP na tym porcie, instalacja się nie powiedzie. Domenę `ipa.zielona.example` wybraliśmy osobno od `ad.zielona.example`, z powodów opisanych na stronie FreeIPA: jedno logowanie dla wszystkich linuksów.

Przebieg

1. Ustawienie nazwy hosta

```
sudo hostnamectl set-hostname ipa01.ipa.zielona.example
```

Przykład:

```
Static hostname: ipa01.ipa.zielona.example
```

2. Instalacja pakietów serwera

```
sudo dnf install -y ipa-server ipa-server-dns
```

Pakiet `ipa-server-dns` dokłada moduł zintegrowanego DNS, instalujemy go od razu, nawet jeśli ostatecznie zdecydujemy się go nie używać, bo dołożenie go po fakcie wymaga osobnej procedury.

3. Decyzja: zintegrowany DNS

> **Pojęcie: zintegrowany DNS FreeIPA.** Serwer DNS (`bind-dyndb-ldap`) trzymający strefy bezpośrednio w katalogu LDAP FreeIPA, zamiast w osobnych plikach strefy, dzięki czemu rekordy SRV usług Kerberosa i LDAP aktualizują się same przy każdej zmianie topologii (nowa replika, zmiana adresu).

Sytuacja	Decyzja w Zielonej
Domena `ipa.zielona.example` nie istnieje jeszcze w żadnym DNS	zintegrowany DNS: tak, FreeIPA sama utrzyma rekordy SRV bez ręcznego wpisywania ich na `dc01`
Firma ma już rozbudowaną infrastrukturę DNS, którą administruje inny zespół	zintegrowany DNS: nie, tylko `--no-host-dns`, a rekordy wpisujemy ręcznie na istniejącym DNS

Zielona wybiera zintegrowany DNS: `ipa.zielona.example` to nowa poddomena, którą i tak trzeba by gdzieś umieścić, a docelowe zaufanie z AD (patrz FreeIPA i Active Directory: zaufanie między domenami) i tak wymaga wzajemnego przekazywania zapytań między dwoma serwerami DNS, więc korzyść z ręcznego prowadzenia stref FreeIPA na `dc01` byłaby żadna.

4. Instalacja serwera: ipa-server-install

```
sudo ipa-server-install \
  --realm=IPA.ZIELONA.EXAMPLE \
  --domain=ipa.zielona.example \
  --setup-dns \
```

```
  --forwarder=10.20.10.11 \
  --hostname=ipa01.ipa.zielona.example \
  --unattended
```

> (gdzie `--forwarder` wskazuje `dc01`, kontroler domeny AD z DNS Zielonej, żeby zapytania spoza domeny `ipa.zielona.example` szły dalej przez znaną już infrastrukturę, a `--unattended` pomija interaktywne pytania, poza hasłami)

Komenda pyta osobno o hasło Directory Managera i osobno o hasło konta `admin`, oba podajemy dwukrotnie do potwierdzenia.

Przykład końcowego fragmentu instalacji:

```
Setup complete

Next steps:
1. You must make sure these network ports are open:
TCP Ports:
  * 80, 443: HTTP/HTTPS
  * 389, 636: LDAP/LDAPS
  * 88, 464: kerberos
UDP Ports:
  * 88, 464: kerberos
  * 53: bind

2. You can now obtain a kerberos ticket using the command: 'kinit admin'
```

Uważaj: instalacja trwa kilkanaście do kilkudziesięciu minut, dużą część czasu zajmuje konfiguracja urzędu certyfikacji Dogtag. Przerwanie jej w połowie zostawia host w stanie pośrednim, z którego jedynym pewnym wyjściem jest `ipa-server-install --uninstall` i powtórzenie instalacji od zera.

5. Firewalld

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

6. Pierwsze logowanie: kinit admin

```
kinit admin
```

Przykład:

```
Password for admin@IPA.ZIELONA.EXAMPLE:
```

Bilet Kerberosa dla `admin` jest wymagany przed każdą komendą `ipa`, dokładnie tak samo jak opisano przy kliencie FreeIPA na stronie FreeIPA.

7. Dodanie pierwszego użytkownika zespołu

```
ipa user-add tomek.nowicki --first=Tomek --last=Nowicki --email=tomek.nowicki@zielona.example
```

Przykład:

```
Added user "tomek.nowicki"
--------------------------
  User login: tomek.nowicki
  First name: Tomek
  Last name: Nowicki
  Full name: Tomek Nowicki
```

Dodawanie kolejnych użytkowników, grup i reguł `sudo` / `HBAC` na co dzień opisuje strona FreeIPA, tutaj tego nie powtarzamy.

8. Dołączenie pierwszego klienta

Każdy kolejny linux Zielonej dołączamy komendą `ipa-client-install`, opisaną krok po kroku na stronie FreeIPA. Tam samo dodajemy też pierwszą regułę HBAC zawężającą domyślne `allow_all`, zanim dołączymy więcej niż jeden host produkcyjny.

9. Replika

```
sudo ipa-client-install --domain=ipa.zielona.example --server=ipa01.ipa.zielona.example
sudo ipa-replica-install --setup-dns --forwarder=10.20.10.11 --setup-ca
```

> **Pojęcie: replika.** Kolejny serwer FreeIPA w tej samej domenie, najpierw dołączony jak zwykły klient, a potem podniesiony do roli pełnej repliki komendą `ipa-replica-install`. Od tego momentu przyjmuje zarówno odczyty, jak i zapisy na równi z `ipa01`, architektura wieloserwerowa (multi master) synchronizuje zmiany w obie strony. Zielona planuje drugą replikę, `ipa02`, dopiero gdy liczba dołączonych serwerów linuksowych uzasadni odporność na awarię pojedynczego `ipa01`, instalujemy tylko jedną replikę naraz, FreeIPA nie wspiera równoległej instalacji kilku replik jednocześnie.

10. Kopia zapasowa: ipa-backup

```
sudo ipa-backup
```

Przykład:

```
Preparing backup on ipa01.ipa.zielona.example
Stopping IPA services
Backing up ipa
ipa-backup was successful
```

> **Pojęcie: ipa-backup.** Narzędzie tworzące pełną kopię serwera (katalog LDAP, konfiguracja, certyfikaty CA) w katalogu `/var/lib/ipa/backup`, w pliku nazwanym `ipa-full-RRRR-MM-DD-GG-MM-SS`. Kopia jest przywracalna tylko na tym samym hoście i w tej samej wersji FreeIPA, z której powstała, więc katalog `/var/lib/ipa/backup` wysyłamy dalej na `bkp01` tą samą drogą co inne kopie serwerów linuksowych, ale traktujemy ją jako kopię `ipa01`, nie jako coś do odtworzenia na dowolnej maszynie.

Weryfikacja

```
sudo ipactl status
```

Przykład:

```
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
httpd Service: RUNNING
ipa-custodia Service: RUNNING
pki-tomcatd Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
named Service: RUNNING
ipa: INFO: The ipactl command was successful
```

```
dig +short SRV _kerberos._tcp.ipa.zielona.example
```

Przykład:

```
0 100 88 ipa01.ipa.zielona.example.
```

```
kinit admin && ipa user-find tomek.nowicki
```

Wycofanie zmian

```
sudo ipa-server-install --uninstall -U
```

Przykład:

```
The ipa-server-install command was successful
```

Uważaj: odinstalowanie na hoście, który jest już jedyną repliką z rolą CA, kasuje bezpowrotnie urząd certyfikacji domeny razem z wystawionymi przez niego certyfikatami. Zanim odinstalujemy jedyny serwer w domenie, upewniamy się, że nie ma na nim jedynych kopii certyfikatów, których gdzieś jeszcze potrzebujemy.

Gdy coś nie zadziała

Objaw	Przyczyna	Naprawa

`ipa-server-install` kończy się błędem o rozwiązywaniu FQDN	DNS nie rozwiązuje jeszcze nazwy hosta w obie strony	`dig +short ipa01.ipa.zielona.example` i `dig +short -x 10.20.10.53`, poprawiamy wpisy przed ponowną próbą
Instalacja przerywa się na etapie konfiguracji Kerberosa z `Clock skew too great`	zegar hosta rozjechany z resztą infrastruktury o więcej niż kilka minut	`chronyc tracking`, `sudo chronyc makestep`, dopiero potem ponawiamy instalację
`kinit admin` zwraca `kinit: Cannot contact any KDC`	usługa `krb5kdc` nie wstała albo port 88 zablokowany na firewallu	`sudo ipactl status`, `firewall-cmd --list-ports`, dodajemy brakujące porty z kroku 5
Klienci nie widzą nowych rekordów SRV po dołożeniu repliki	zintegrowany DNS nie działa na tym hoście, mimo `--setup-dns` przy replice	`dig +short SRV _ldap._tcp.ipa.zielona.example`, sprawdzamy `systemctl status named-pkcs11` na replice

Powiązane: FreeIPA: jedno logowanie dla wszystkich linuksów · FreeIPA · FreeIPA i Active Directory: zaufanie między domenami · Świat przykładów: Zielona

Źródła: docs.redhat.com, „Installing an IdM server: With integrated DNS", RHEL 9 · docs.redhat.com, „Installing an IdM replica", RHEL 9 · freeipa.org, strona `V4/Firewall_Configuration` · `man ipa-server-install` · `man ipa-backup` · `man ipa-replica-install`

FreeIPA i Active Directory: zaufanie między domenami

Typ: procedura **Dotyczy: FreeIPA 4.x na ipa01, Active Directory na dc01/dc02**

Czas: ~40 min

Efekt: konta z domeny `ad.zielona.example` mogą logować się na linuksach dołączonych do `ipa.zielona.example`, bez zakładania dla nich osobnych kont w FreeIPA. Domeny zostają dwiema osobnymi domenami Kerberos, połączonymi relacją zaufania, nie jedną wspólną domeną.

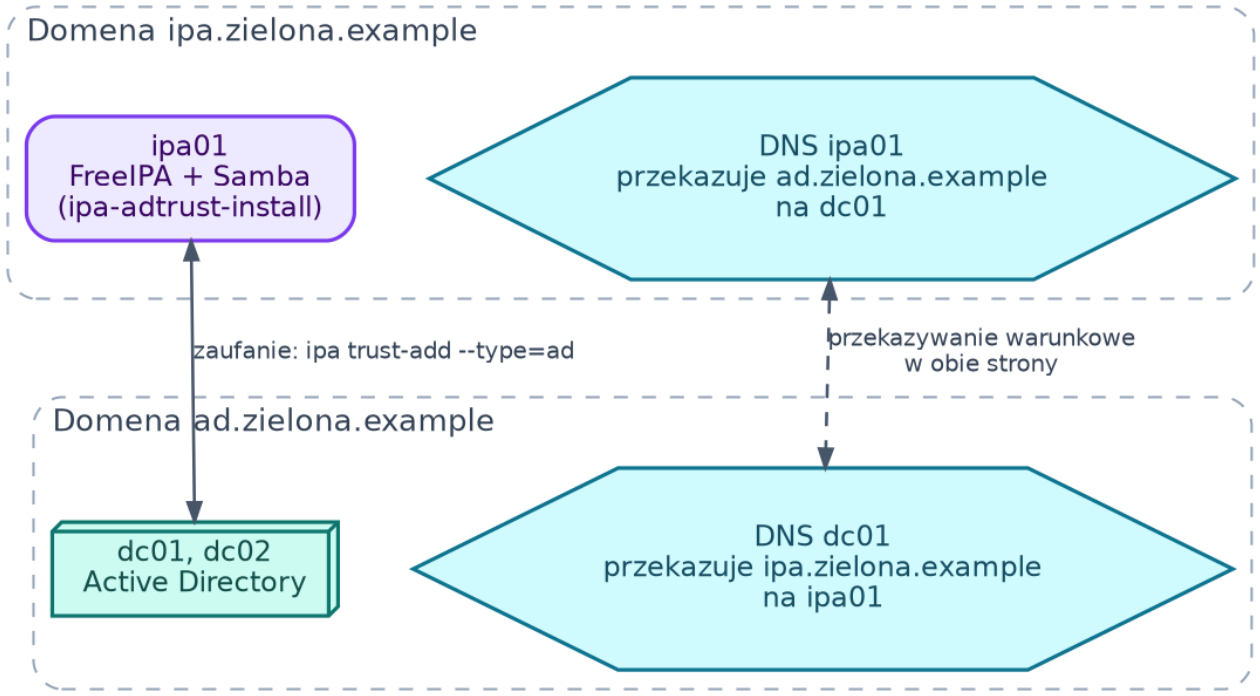
Skróty użyte na tej stronie (12)

Skrót	Co znaczy
AD	Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
HBAC	Host-Based Access Control: reguły FreeIPA mówiące, kto może się zalogować na który serwer
IdM	Identity Management: nazwa produktu Red Hata, płatnej i wspieranej wersji otwartego, darmowego FreeIPA
KDC	Key Distribution Center: serwer Kerberosa wydający bilety logowania
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)
POSIX	Portable Operating System Interface: wspólny zestaw zasad, dzięki któremu polecenie działa tak samo na różnych Uniksach
RHEL	Red Hat Enterprise Linux: komercyjna dystrybucja Linuksa
SID	w Oracle: System Identifier, nazwa instancji; w Windows: Security Identifier, numer konta
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
UID	User ID: numer użytkownika w Linuksie

Zanim zaczniemy

Komendy po stronie FreeIPA wykonujemy z CLI bash jako user z uprawnieniami sudo albo root na `ipa01`, z ważnym biletem `admin` (`kinit admin`). Konfiguracja DNS wymaga też dostępu administratora domeny AD do `dc01`.

Wymaganie	Jak sprawdzić
DNS FreeIPA rozwiązuje domenę AD	`dig +short ad.zielona.example` z `ipa01`
DNS AD rozwiązuje domenę FreeIPA	`dig +short ipa.zielona.example` z `dc01`
Zsynchronizowany zegar po obu stronach	`chronyc tracking` na `ipa01`, `w32tm /query /status` na `dc01`
Konto administratora domeny AD z prawem tworzenia zaufań	konto w grupie `Domain Admins` na `ad.zielona.example`
Otwarte porty między `ipa01` a `dc01`/`dc02`	445, 138, 139 (SMB/Netlogon), 389, 636 (LDAP), 88, 464 (Kerberos), 53 (DNS)



Dwie osobne domeny Kerberos, ipa.zielona.example i ad.zielona.example, połączone zaufaniem ipa trust-add, z DNS przekazującym zapytania wzajemnie w obie strony (kliknięcie otwiera pełny rozmiar)

Uważaj: zaufanie łączy dwie osobne domeny, nie scala ich w jedną. Konta AD po zestawieniu zaufania nadal zarządzane są w Active Directory, FreeIPA tylko rozpoznaje je i mapuje na lokalne UID/GID linuksów, o czym więcej w kroku 4.

Przebieg

1. Przekazywanie DNS w obie strony

Na `ipa01`, przekazanie zapytań o domenę AD do jej kontrolera:

```
ipa dnsforwardzone-add ad.zielona.example --forwarder=10.20.10.11 --forward-policy=only
```

Przykład:

```
Zone name: ad.zielona.example
Zone forwarders: 10.20.10.11
Forward policy: only
```

Po stronie AD, w konsoli DNS na `dc01`, zakładamy strefę przekazywania warunkowego (`Conditional Forwarder`) dla `ipa.zielona.example` wskazującą `10.20.10.53` (`ipa01`).

> **◫◫ ZRZUT EKRANU DO UZUPEŁNIENIA**
>
> Zrzut do uzupełnienia: konsola DNS Managera na `dc01`, węzeł „Conditional Forwarders" z nowo dodaną strefą `ipa.zielona.example` i adresem serwera `10.20.10.53`.

Uważaj: brakujące przekazywanie w jedną tylko stronę jest najczęstszą przyczyną, dla której `ipa trust-add` w kroku 3 kończy się błędem mimo poprawnie skonfigurowanej reszty. Obie strony muszą rozwiązywać nazwy drugiej domeny, zanim w ogóle spróbujemy zestawić zaufanie.

2. Przygotowanie serwera FreeIPA: ipa-adtrust-install

```
sudo ipa-adtrust-install --add-sids
```

Przykład:

```
Configuring cross-realm trusts for IPA server to work with trusted domains.
...
The ipa-adtrust-install command was successful
```

> **Pojęcie: ipa-adtrust-install.** Jednorazowa procedura instalująca na serwerze FreeIPA usługi wymagane przez zaufanie: pakiet `ipa-server-trust-ad`, komponent Samby udający kontroler domeny dla protokołów, których AD używa do komunikacji między domenami, oraz wtyczkę zgodności LDAP dla starszych klientów. Flaga `--add-sids` generuje identyfikatory SID dla istniejących już użytkowników i grup FreeIPA, operacja kosztowna przy dużej liczbie kont, więc przy tysiącach użytkowników warto ją zaplanować poza godzinami szczytu.

3. Zestawienie zaufania: ipa trust-add

```
ipa trust-add --type=ad ad.zielona.example --admin=Administrator --password
```

Przykład:

```
Active Directory domain administrator's password:
-----------------------------------------------------
Added Active Directory trust for realm "ad.zielona.example"
-----------------------------------------------------
  Realm name: ad.zielona.example
  Domain NetBIOS name: ZIELONA
  Domain Security Identifier: S-1-5-21-...
  Trust direction: Two-way trust
  Trust type: Active Directory domain
```

`--admin` wskazuje konto z uprawnieniami administratora domeny AD, podane hasło służy wyłącznie do jednorazowego zestawienia zaufania i nigdzie nie jest zapamiętywane przez FreeIPA.

4. Mapowanie ID: SID kontra POSIX

> **Pojęcie: mapowanie ID (ID mapping).** Sposób, w jaki FreeIPA i SSSD wyliczają lokalny UID/GID dla konta, które fizycznie istnieje tylko w Active Directory, nieposiadającym własnego pojęcia UID linuksowego.

Wariant	Kiedy używamy	Jak działa
Mapowanie z SID (domyślne, `ipa-ad-trust`)	AD nie ma wypełnionych atrybutów POSIX (`uidNumber`, `gidNumber`)	SSSD sam wylicza UID/GID z zakresu przypisanego do SID konta, spójnie na każdym linuksie

Wariant	Kiedy używamy	Jak działa
Atrybuty POSIX z AD (`ipa-ad-trust-posix`)	administrator AD już wcześniej ręcznie wypełnił `uidNumber`/`gidNumber` w schemacie AD	SSSD używa tych wartości wprost, bez własnego wyliczania

Zielona nie wypełniała nigdy atrybutów POSIX w AD, więc zostaje przy domyślnym mapowaniu z SID, ustawionym już w kroku 3 bez dodatkowych flag.

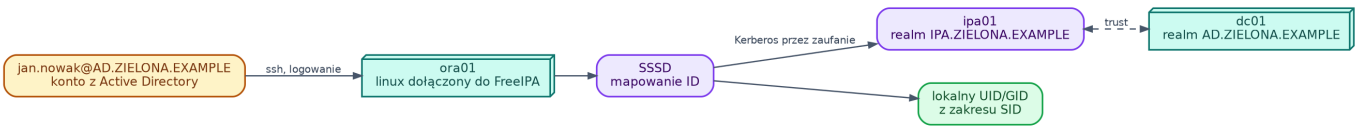
5. Logowanie kontem AD na linuksie

Po zaufaniu i dołączeniu hosta do FreeIPA (patrz FreeIPA po `ipa-client-install`) konto z AD loguje się w pełni kwalifikowaną nazwą, z realmem AD:

```
id kasia.wisniewska@ad.zielona.example
```

Przykład:

```
uid=1979400512(kasia.wisniewska@ad.zielona.example) gid=1979400513(domain
users@ad.zielona.example)
groups=1979400513(domain users@ad.zielona.example)
```



Droga logowania konta AD na linuksie: żądanie idzie przez SSSD do FreeIPA, a stamtąd przez zaufanie do kontrolera domeny AD (kliknięcie otwiera pełny rozmiar)

Dostęp do konkretnego hosta wciąż zawężamy regułą HBAC, tak jak dla kont FreeIPA, wskazując w niej grupę zewnętrzną powiązaną z grupą AD:

```
ipa group-add-member zielona-linux-admins --external "ZIELONA\\administratorzy_linux"
```

Weryfikacja

```
ipa trust-status ad.zielona.example
```

Przykład:

```
CIFS server credentials:
Kerberos:  OK
LDAP: OK
```

```
id kasia.wisniewska@ad.zielona.example
```

```
kinit kasia.wisniewska@AD.ZIELONA.EXAMPLE
```

Przykład potwierdzający, że KDC FreeIPA przekazał żądanie dalej do AD zamiast zwrócić błąd:

```
Password for kasia.wisniewska@AD.ZIELONA.EXAMPLE:
```

Wycofanie zmian

```
ipa trust-del ad.zielona.example
```

Przykład:

```
Deleted trust "ad.zielona.example"
```

Uważaj: usunięcie zaufania nie usuwa reguł HBAC ani grup zewnętrznych powiązanych z kontami AD, zostają jako martwe wpisy odwołujące się do już nieistniejącej domeny. Porządkujemy je ręcznie, jeśli zaufanie usuwamy na stałe, a nie tylko na czas naprawy.

Gdy coś nie zadziała

Objaw	Przyczyna	Naprawa
`ipa trust-add` kończy się błędem rozpoznania domeny AD	DNS nie przekazuje zapytań w jedną albo obie strony	`dig +short ad.zielona.example` z `ipa01` i `dig +short ipa.zielona.example` z `dc01`, poprawiamy przekazywanie z kroku 1
`ipa trust-add` kończy się błędem uwierzytelnienia mimo poprawnego hasła administratora AD	zegar `ipa01` rozjechany z `dc01` o więcej niż limit Kerberosa	`chronyc tracking` na `ipa01`, porównujemy z czasem na `dc01`
`id uzytkownik@ad.zielona.example` nie zwraca żadnego wyniku	host linuksowy nie ma jeszcze uruchomionej usługi `sssd` z widoczną domeną zaufaną	`sudo systemctl restart sssd`, `sudo sss_cache -E`, ponawiamy

Objaw	Przyczyna	Naprawa
Logowanie działa, ale użytkownik trafia bez żadnych grup lokalnych	reguła HBAC albo grupa zewnętrzna nie obejmuje tego konta	sprawdzamy przynależność w AD, poprawiamy grupę zewnętrzną z kroku 5

Powiązane: FreeIPA: jedno logowanie dla wszystkich linuksów · Instalacja serwera FreeIPA na ipa01 · FreeIPA · Dołączenie do domeny AD przez realmd

Źródła: docs.redhat.com, „Installing trust between IdM and AD", RHEL 9, rozdział „Setting up a trust" · freeipa.org/page/Active_Directory_trust_setup · `man ipa-adtrust-install` · `man ipa-trust-add` (dokumentacja polecenia `ipa trust-add`)