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.

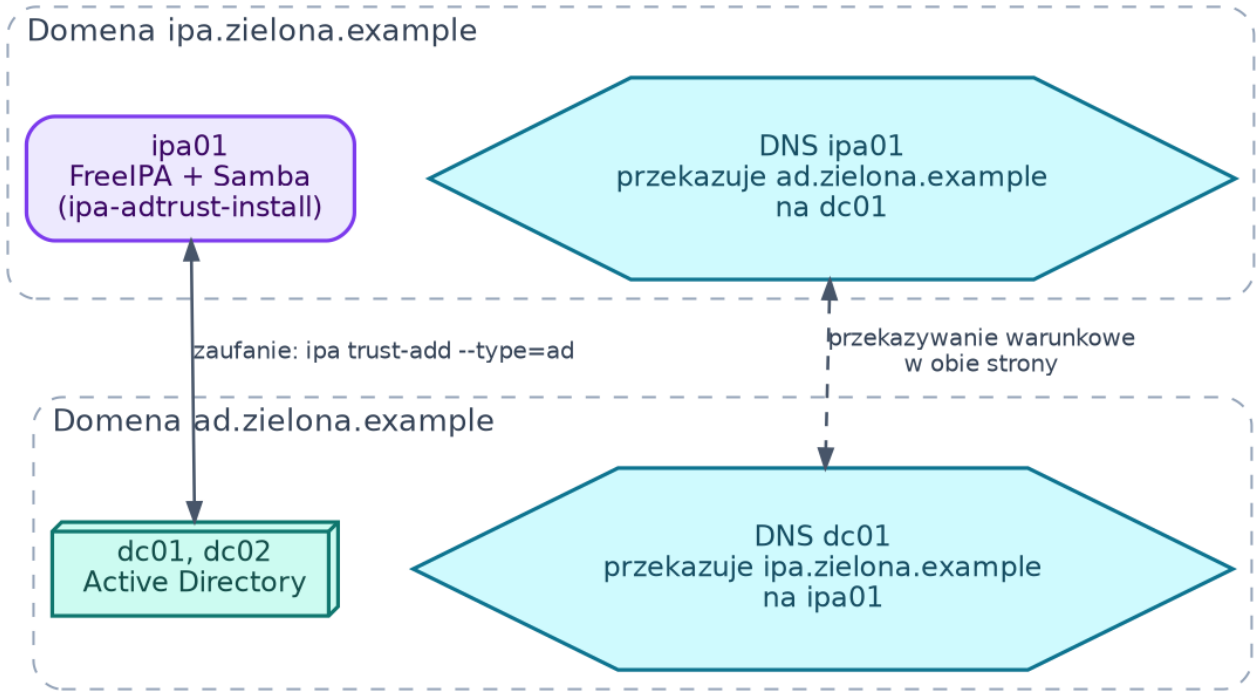
Skróty użyte na tej stronie (12)

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.

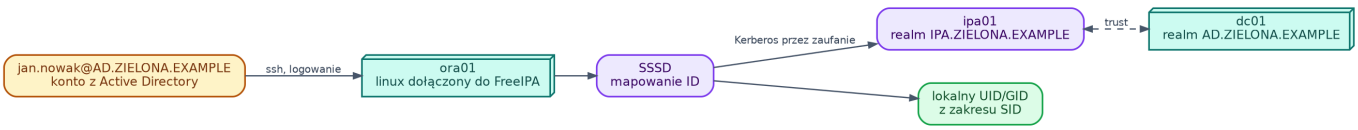
5. Logowanie kontem AD na linuksie

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`)

Revision #22
Created 2026-09-28 17:15:43 UTC by Tomasz Konieczny
Updated 2026-10-26 14:14:52 UTC by Tomasz Konieczny