# Graylog: logowanie kontem z Active Directory

**Typ: procedura** **Dotyczy: Graylog 7.1, Active Directory na dc01/dc02** **Czas: ~30 min**

*Efekt: logowanie do Graylogu kontem domenowym z Active Directory, bez zakładania konta lokalnego dla każdej nowej osoby. Po drodze sprawdzamy uczciwie, gdzie kończy się darmowa wersja Open, a zaczyna płatny Enterprise.*

**Skróty użyte na tej stronie (8)**

| Skrót | Co znaczy |
|---|---|
| **AD** | Active Directory: katalog Microsoftu z kontami użytkowników, komputerów i grup w firmie |
| **CA** | Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty |
| **IT** | Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy |
| **JRE** | Java Runtime Environment: środowisko uruchomieniowe Javy, potrzebne do odpalenia programów napisanych w tym języku, jak sam Graylog |
| **JVM** | Java Virtual Machine: maszyna wirtualna, w której działają programy w Javie |
| **LDAP** | Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA) |
| **LDAPS** | LDAP szyfrowany TLS, zwykle port 636 |
| **TLS** | Transport Layer Security: szyfrowanie połączeń, np. w HTTPS |

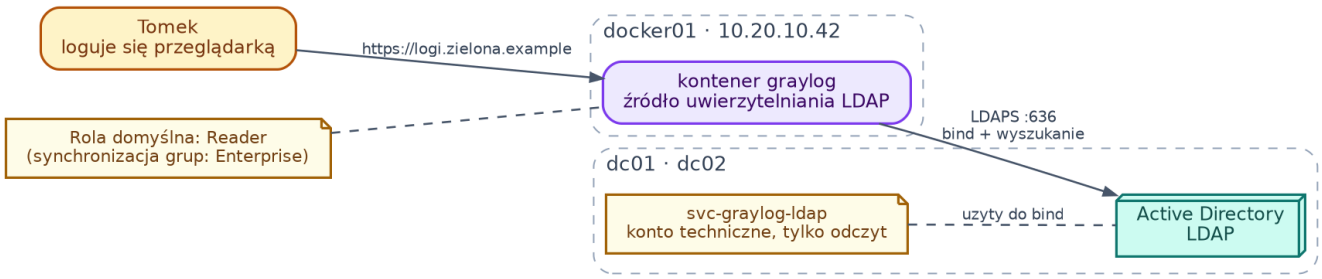
# Zanim zaczniemy

**Z ŻYCIA WZIĘTE**

Ola dostaje dostęp do Graylogu, żeby sama sprawdzała logi swoich aplikacji zamiast pytać za każdym razem zespół IT. Loguje się tym samym kontem domenowym, którym otwiera pocztę i loguje się do komputera, bez osobnego hasła do zapamiętania i bez maila z tymczasowym hasłem, który trzeba zmienić przy pierwszym logowaniu.

**Pojęcie: LDAP.** Protokół odpytywania katalogu z kontami, grupami i innymi obiektami organizacyjnymi, opisany szerzej przy okazji Gitea na stronie Logowanie kontem z Active Directory. Active Directory na `dc01` i `dc02` udostępnia swoje dane właśnie przez LDAP, a Graylog, zamiast trzymać osobną bazę haseł, o każdym logowaniu pyta katalog, czy takie konto istnieje i czy podane hasło jest poprawne.

**Pojęcie: usługa uwierzytelniania (authentication service).** Konfiguracja w Graylogu opisująca, jak i gdzie łączyć się z katalogiem: adres serwera, poświadczenia konta technicznego do wyszukiwania, filtr określający, które konta wolno logować, i rolę, jaką dostają automatycznie po pierwszym logowaniu.




*Graylog łączy się z Active Directory na dc01 po LDAPS przez konto techniczne, a każde zsynchronizowane konto dostaje tę samą rolę domyślną (kliknięcie otwiera pełny rozmiar)*

| Wymaganie | Uwaga |
|---|---|
| Konto techniczne w AD do bind LDAP | zakładamy w kroku 1, prawo tylko do odczytu katalogu |
| LDAPS na porcie 636 osiągalny z `docker01` do `dc01`/`dc02` | sprawdzamy zaporą, zanim zaczniemy konfigurację w Graylogu |
| Certyfikat firmowego CA zaufany przez JVM wewnątrz kontenera | bez tego kroku 4 połączenie LDAPS kończy się błędem certyfikatu |
| Decyzja, jaką rolę domyślną dostają zsynchronizowane konta | patrz sekcja niżej o różnicy między Open i Enterprise |

**Uważaj:** konto techniczne wskazane przy uwierzytelnianiu systemowym powinno mieć wyłącznie prawo odczytu katalogu, na tej samej zasadzie najmniejszych uprawnień, na jakiej opieramy konta monitorujące bazy danych. Graylog nie potrzebuje żadnego prawa zapisu w Active Directory do samego uwierzytelniania użytkowników.

# Co jest w Open, a co wymaga Enterprise

To rozróżnienie decyduje, jak dokładnie skonfigurujemy krok 3, więc sprawdzamy je, zanim usiądziemy do formularza. Samo uwierzytelnianie LDAP i Active Directory, czyli sprawdzenie loginu i hasła w katalogu, jest częścią darmowego Graylog Open i działa dokładnie tak, jak opisuje ta strona.

Synchronizacja grup, czyli automatyczne mapowanie grup z Active Directory na role albo zespoły (teams) wewnątrz Graylogu, jest funkcją wyłącznie Graylog Enterprise: dokumentacja producenta wprost zaznacza przy tym ekranie, że wymaga ważnej licencji Enterprise. W wersji Open każde konto zsynchronizowane z katalogu dostaje jedną, tę samą rolę domyślną skonfigurowaną w polu „Default Roles", niezależnie od tego, do jakich grup faktycznie należy w Active Directory.

W praktyce w Zielonej oznacza to, że wszyscy logujący się przez LDAP dostają w Open rolę `Reader` (obowiązkową, bez niej nikt nie otworzy interfejsu), a podniesienie kogoś do roli `Admin` wykonujemy ręcznie, z poziomu System → Users, po pierwszym zsynchronizowaniu jego konta. To jeden dodatkowy klik na osobę, nie automatyzacja przez grupę, ale wciąż mniej pracy niż zakładanie całego konta lokalnego od zera.

# Przebieg

## 1. Konto techniczne w Active Directory

Zakładamy konto techniczne do bind LDAP, z hasłem nieulegającym wygaśnięciu i bez prawa jego zmiany przez samo konto:

```
New-ADUser -Name "svc-graylog-ldap" `
  -SamAccountName "svc-graylog-ldap" `
  -UserPrincipalName "svc-graylog-ldap@ad.zielona.example" `
  -Path "OU=KontaTechniczne,DC=ad,DC=zielona,DC=example" `
  -AccountPassword (Read-Host -AsSecureString "Haslo konta") `
  -Enabled $true `
  -PasswordNeverExpires $true `
  -CannotChangePassword $true
```

# 2. Zaufanie do firmowego CA w JVM

Graylog działa na maszynie wirtualnej Javy (JVM), a JVM ma własny magazyn zaufanych certyfikatów, niezależny od systemowego magazynu hosta. Certyfikat CA Zielonej musi trafić właśnie tam, inaczej połączenie LDAPS kończy się błędem certyfikatu mimo poprawnej reszty konfiguracji. Najpierw sprawdzamy, gdzie w obrazie leży JRE:

```
docker exec graylog printenv JAVA_HOME
```

Przykład:

```
/usr/lib/jvm/temurin-17-jre
```

Kopiujemy certyfikat do kontenera i dokładamy go do magazynu `cacerts` tym samym `keytool`, którego używa sam Graylog, wskazując ścieżkę wyliczoną w poprzednim kroku:

```
docker cp CA-Zielona.crt graylog:/tmp/ca-zielona.crt
docker exec graylog keytool -importcert -trustcacerts -noprompt \
  -alias ca-zielona \
  -file /tmp/ca-zielona.crt \
  -keystore "$(docker exec graylog printenv JAVA_HOME)/lib/security/cacerts" \
  -storepass changeit
docker restart graylog
```

> Po przenosinach urzędu według strony Przenosiny urzędu z dc01 bez przerwy: dwa urzędy równolegle i wygaszenie CA-Zielona dokładamy tu w ten sam sposób zaufanie do `Zielona-Root-CA`, a `CA-Zielona.crt` zostaje obok do wygaszenia starego urzędu.

**Uważaj:** `changeit` to domyślne hasło magazynu `cacerts` w niemal każdej dystrybucji Javy, nie hasło specyficzne dla Graylogu. Jeśli obraz zmienił je przy budowaniu, `keytool` zgłosi błąd złego hasła i sprawdzamy je w dokumentacji obrazu, zamiast zgadywać kolejne wartości.

> Import przez `keytool` do działającego kontenera zmienia plik `cacerts` wewnątrz warstwy kontenera, a nie na dysku hosta. Przy każdym odtworzeniu kontenera (`docker compose up -d` po zmianie tagu obrazu albo `docker compose down`) certyfikat znika i LDAPS znów kończy się błędem `unable to find valid certification path`. Taki import traktujemy jako szybki test, a na stałe robimy trwały magazyn zaufania z poniższego podkroku.

## Trwały magazyn zaufania: truststore w katalogu danych

Przygotowujemy kopię magazynu z dopisanym CA Zielonej i zapisujemy ją w katalogu danych Grayloga, który i tak jest wolumenem na hoście (`/docker/apps/graylog/graylog`). Certyfikat `/tmp/ca-zielona.crt` jest już w kontenerze z poprzedniego polecenia.

```
docker exec graylog sh -c 'cp "$JAVA_HOME/lib/security/cacerts" /tmp/truststore.jks && keytool -importcert -trustcacerts -noprompt -alias ca-zielona -file /tmp/ca-zielona.crt -keystore /tmp/truststore.jks -storepass changeit'
docker cp graylog:/tmp/truststore.jks /docker/apps/graylog/graylog/truststore.jks
```

Plik musi należeć do użytkownika Grayloga (numery sprawdzamy tak, jak w kroku z `chown` na stronie Instalacja Grayloga w Dockerze: Graylog, MongoDB i OpenSearch):

```
sudo chown NumerUID:NumerGID /docker/apps/graylog/graylog/truststore.jks
```

W `compose.yaml`, w usłudze `graylog`, dopisujemy do `environment` zmienną, która wskazuje JVM własny magazyn zamiast domyślnego:

```
    environment:
      - GRAYLOG_SERVER_JAVA_OPTS=-Xms1g -Xmx1g -server -XX:+UseG1GC -XX:-OmitStackTraceInFastThrow -Djavax.net.ssl.trustStore=/usr/share/graylog/data/truststore.jks -Djavax.net.ssl.trustStorePassword=changeit
```

Zmienna zastępuje domyślne opcje JVM obrazu, dlatego wpisujemy w niej od razu także opcje pamięci (wartości `-Xms` i `-Xmx` dopasowujemy do swojej instalacji, jak na stronie Graylog: częste problemy). Magazyn jest kopią systemowego `cacerts` z jednym dopisanym certyfikatem, więc inne połączenia TLS Grayloga nadal działają. Po zmianie odtwarzamy kontener: `docker compose up -d graylog`. Teraz certyfikat przeżywa każde odtworzenie, bo leży na hoście. Po aktualizacji obrazu Grayloga odświeżamy kopię `cacerts`, żeby nie zostać ze starą listą zaufanych urzędów.

# 3. Konfiguracja usługi uwierzytelniania w interfejsie

W System → Authentication → Create service → Active Directory wypełniamy formularz zgodnie z tabelą.

| Pole | Wartość w Zielonej | Uwaga |
|---|---|---|
| Title | `AD Zielona` | dowolna, widoczna tylko w panelu administracyjnym |

| Pole | Wartość w Zielonej | Uwaga |
|---|---|---|
| Server Address | `dc01.ad.zielona.example:636` | drugi kontroler `dc02` dopisujemy jako kolejny adres, jeśli formularz na to pozwala |
| Security Options | LDAPS | port 636, ruch szyfrowany od razu przy nawiązaniu połączenia |
| System User DN | `CN=svc-graylog-ldap,OU=KontaTechniczne,DC=ad,DC=zielona,DC=example` | konto techniczne z kroku 1 |
| System Password | hasło konta technicznego | to samo hasło co przy `New-ADUser` |
| Search Base DN | `OU=Uzytkownicy,DC=ad,DC=zielona,DC=example` | jednostka organizacyjna z kontami pracowników |
| Search Pattern | `(&(objectClass=user)(sAMAccountName={0}))` | `{0}` zastępuje login wpisany na ekranie logowania |
| Name Attribute | `sAMAccountName` | login w starym formacie, ten sam co do stacji Windows |
| Full Name Attribute | `displayName` | imię i nazwisko wyświetlane w interfejsie |
| Email Attributes | `mail` | adres do powiadomień |
| Default Roles | `Reader` | obowiązkowe: bez roli Reader zsynchronizowane konto nie otworzy interfejsu |

**◫ ZRZUT EKRANU DO UZUPEŁNIENIA**

Zrzut do uzupełnienia: ekran System → Authentication po dodaniu usługi, wiersz „AD Zielona" ze statusem Aktywna i typem Active Directory.

# Weryfikacja

Testujemy logowanie kontem domenowym na ekranie logowania Graylogu, używając loginu `ola.wisniewska` i hasła domenowego, zamiast konta `admin`.

Sprawdzamy z poziomu interfejsu, że konto rzeczywiście trafiło na listę użytkowników, w System → Users, z kolumną „Client" pokazującą nazwę usługi `AD Zielona` zamiast „internal".

**◫ ZRZUT EKRANU DO UZUPEŁNIENIA**

Zrzut do uzupełnienia: ekran System → Users po pierwszym logowaniu Oli przez LDAP, z widocznym kontem `ola.wisniewska` i źródłem `AD Zielona`.

# Wycofanie zmian

Wyłączenie usługi uwierzytelniania bez usuwania importowanych kont, gdy chcemy tymczasowo wrócić do logowania lokalnego: w System → Authentication odznaczamy „Enable service" przy usłudze `AD Zielona`, zamiast ją usuwać.

Pełne usunięcie usługi: w System → Authentication, przy usłudze `AD Zielona`, wybieramy „Delete service". Konta, które zdążyły się już zalogować, zostają na liście użytkowników jako konta bez działającego źródła uwierzytelniania, aż administrator usunie je ręcznie.

# Gdy coś nie zadziała

| Objaw | Przyczyna | Co robimy |
|---|---|---|
| `LDAP Result Code 49 Invalid Credentials` w logu Graylogu | zły System User DN albo hasło konta technicznego | sprawdzamy DN i hasło komendą `ldapsearch` z hosta `docker01` przed poprawką w Graylogu |
| `unable to find valid certification path to requested target` | certyfikat firmowego CA niezaufany w magazynie `cacerts` | wykonujemy krok 2, dokładamy CA do keystore i restartujemy kontener |
| LDAPS działał, a po odtworzeniu kontenera znów zgłasza błąd certyfikatu | CA zaimportowane `keytool` do działającego kontenera zniknęło razem ze starym kontenerem | przechodzimy na trwały truststore z kroku 2 (`GRAYLOG_SERVER_JAVA_OPTS` i plik na hoście) |
| Konto istnieje w AD, ale logowanie odrzucone | Search Pattern bez `{0}` albo konto poza jednostką organizacyjną wskazaną w Search Base DN | sprawdzamy, czy `{0}` jest we wzorcu i czy konto rzeczywiście leży pod wskazanym `OU` |
| Konto loguje się, ale widzi tylko odczyt, mimo że powinno być administratorem | brak synchronizacji grup w wersji Open, opisany wyżej | podnosimy rolę ręcznie w System → Users, albo rozważamy licencję Enterprise przy większej liczbie takich wyjątków |

**Powiązane:** Instalacja Grayloga w Dockerze: Graylog, MongoDB i OpenSearch · Logowanie kontem z Active Directory · Active Directory: konta, grupy, jednostki organizacyjne

**Źródła:** go2docs.graylog.org, rozdział „Active Directory and LDAP Authentication" · graylog.org, „Graylog Feature List" (Open vs Enterprise) · community.graylog.org, wątek o imporcie certyfikatu do magazynu Javy w kontenerze Graylog

---

Revision #23
Created 2026-09-28 16:57:56 UTC by Tomasz Konieczny

Updated 2026-10-26 14:15:38 UTC by Tomasz Konieczny