Zabbix: logowanie kontem z Active Directory

Typ: procedura **Dotyczy: Zabbix 7.0 LTS, Active Directory na dc01/dc02**

Czas: ~35 min

Efekt: logowanie do Zabbixa kontem domenowym z Active Directory, z automatycznym założeniem konta i nadaniem roli osobom z grupy `GG_Zabbix_Admin`, bez ręcznego zakładania kont lokalnych dla każdej nowej osoby.

Skróty użyte na tej stronie (4)

Skrót	Co znaczy
JIT	Just In Time: mechanizm zakładający albo aktualizujący konto użytkownika automatycznie w chwili pierwszego udanego logowania, zamiast wymagać ręcznego założenia konta z wyprzedzeniem
LDAP	Lightweight Directory Access Protocol: protokół do odpytywania katalogu użytkowników (AD, FreeIPA)
LDAPS	LDAP szyfrowany TLS, zwykle port 636
LTS	Long Term Support: wersja z długim wsparciem poprawkami

Zanim zaczniemy

Z ŻYCIA WZIĘTE

Tomek dostaje dostęp do Zabbixa drugiego tygodnia pracy. Zamiast czekać, aż ktoś założy mu konto lokalne w bazie Zabbixa i wyśle hasło mailem, loguje się od razu tym samym kontem domenowym, którym loguje się do komputera i do poczty, a Zabbix sam rozpoznaje po jego grupie w Active Directory, że powinien dostać rolę administratora.

Pojęcie: LDAP. Protokół odpytywania katalogu z kontami, grupami i innymi obiektami organizacyjnymi. Active Directory na `dc01` i `dc02` udostępnia swoje dane właśnie przez LDAP : Zabbix, zamiast trzymać osobną bazę haseł dla każdego użytkownika, o każdym logowaniu

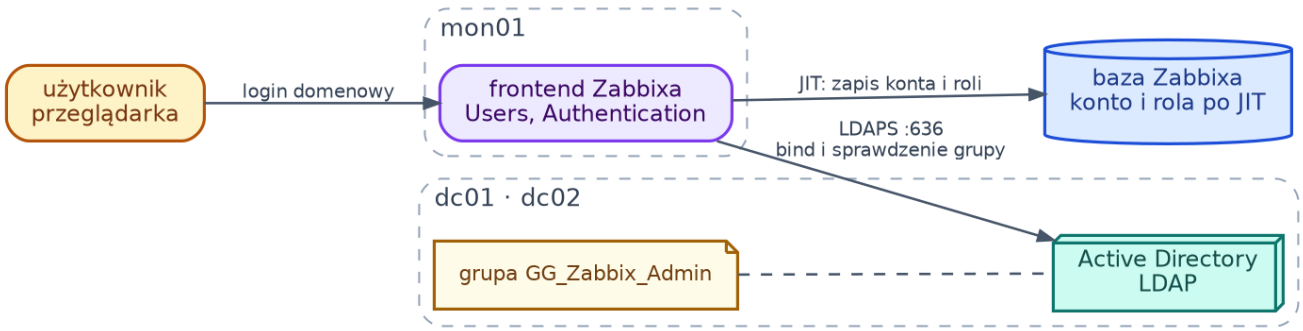
pyta katalog, czy takie konto istnieje, czy podane hasło jest poprawne, i do jakich grup to konto należy.

Pojęcie: provisioning JIT (just in time). Mechanizm w Zabbiksie, sprawdzony w dokumentacji dla wersji 7.0, automatycznie zakładający albo aktualizujący konto użytkownika Zabbixa w chwili pierwszego udanego logowania przez LDAP, na podstawie grup, do których to konto należy w katalogu. Bez JIT provisioningu administrator musiałby ręcznie założyć w Zabbiksie konto dla każdej osoby, zanim ta osoba w ogóle mogłaby się zalogować, nawet jeśli LDAP samo uwierzytelnianie hasła już obsługuje.

Konfigurację wykonujemy zalogowani do frontendu Zabbixa kontem `Admin` z uprawnieniami Super Admin. Ścieżki klikania w interfejsie zapisujemy jako osobne bloki tekstu, zrzuty ekranu dostarcza autor po konfiguracji.

Wymaganie	Uwaga
Konto techniczne w AD do bind LDAP	zakładamy w kroku 1, prawo tylko do odczytu katalogu
Grupa `GG_Zabbix_Admin` w AD	zakładamy w kroku 1, osoby w tej grupie dostają rolę Super Admin
LDAPS na porcie 636 osiągalny z `mon01` do `dc01`/`dc02`	sprawdzamy zaporą, zanim zaczniemy konfigurację w Zabbiksie
Certyfikat firmowego CA zaufany przez system operacyjny `mon01`	bez niego połączenie LDAPS kończy się błędem certyfikatu

Uważaj: konto techniczne wskazane przy bind LDAP powinno mieć wyłącznie prawo odczytu katalogu, na tej samej zasadzie najmniejszych uprawnień, na jakiej opieramy konta monitorujące bazy danych opisane na stronie Monitorowanie typowych usług. Zabbix nie potrzebuje żadnego prawa zapisu w Active Directory do samego uwierzytelniania użytkowników.



Frontend Zabbixa łączy się z Active Directory na dc01 po LDAPS, a provisioning JIT zapisuje konto i rolę na podstawie grupy GG_Zabbix_Admin (kliknięcie otwiera pełny rozmiar)

Przebieg

1. Konto techniczne i grupa 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-zabbix-ldap" `
  -SamAccountName "svc-zabbix-ldap" `
  -UserPrincipalName "svc-zabbix-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
```

Zakładamy grupę dla administratorów Zabbixa, zgodnie z konwencją nazw grup domenowych Zielonej opisaną na stronie Struktura OU Zielonej i delegowanie uprawnień:

```
New-ADGroup -Name "GG_Zabbix_Admin" -GroupScope Global -GroupCategory Security -Path
"OU=Grupy,DC=ad,DC=zielona,DC=example"
```

Dodajemy Tomka do grupy:

```
Add-ADGroupMember -Identity "GG_Zabbix_Admin" -Members "tomek.kowalski"
```

2. Dodanie serwera LDAP: Users → Authentication → LDAP settings

```
Users → Authentication → LDAP settings → Servers → Create LDAP server
Nazwa: AD Zielona
```

```
Host: dc01.ad.zielona.example
Port: 636
Base DN: DC=ad,DC=zielona,DC=example
Search attribute: sAMAccountName
Bind DN: ZIELONA\svc-zabbix-ldap
Bind password: (hasło konta z kroku 1)
Zaznaczone: Advanced configuration, Enable connection encryption (LDAPS)
```

> **Pojęcie: Base DN.** Punkt w drzewie katalogu, od którego Zabbix zaczyna szukać kont i grup. U nas to cała domena `ad.zielona.example`, bo konta użytkowników i grupy `GG_*` leżą w różnych jednostkach organizacyjnych pod tym samym korzeniem.

> **Pojęcie: search attribute.** Atrybut LDAP, po którym Zabbix dopasowuje login wpisany na ekranie logowania do konkretnego konta w katalogu. `sAMAccountName` to nazwa konta w starym formacie `ZIELONA\jan.nowak`, dokładnie ta, której pracownicy Zielonej używają już do logowania na stacjach roboczych.

3. Włączenie provisioningu JIT: zakładka Provisioning

```
Users → Authentication → LDAP settings → Servers → AD Zielona → Provisioning
Enable JIT provisioning: zaznaczone
Group configuration: memberOf
Group name attribute: cn
User group membership attribute: memberOf
User name attribute: givenName
User last name attribute: sn
```

> **Pojęcie: memberOf.** Atrybut konta użytkownika w Active Directory, zawierający listę grup, do których to konto należy. Wybranie metody `memberOf` w provisioningu oznacza, że Zabbix odczytuje grupy wprost z tego atrybutu konta, zamiast osobno przeszukiwać obiekty grup w katalogu.

4. Mapowanie grup na role: tabela Group mapping

```
Users → Authentication → LDAP settings → Servers → AD Zielona → Provisioning → Group mapping →
Create group mapping
Group pattern DN: CN=GG_Zabbix_Admin,OU=Grupy,DC=ad,DC=zielona,DC=example
User group: Zabbix administratorzy
Role: Super admin role
```

Powtarzamy dla zwykłych użytkowników, jeśli chcemy, żeby dowolna osoba z domeny mogła się zalogować z ograniczoną rolą:

```
Group pattern DN: CN=Domain Users,CN=Users,DC=ad,DC=zielona,DC=example
User group: Zabbix uzytkownicy
Role: User role
```

Uważaj: kolejność wpisów w tabeli mapowania ma znaczenie tylko wtedy, gdy jedno konto pasuje do kilku wzorców naraz. Osoba należąca jednocześnie do `GG_Zabbix_Admin` i do `Domain Users` dostaje sumę uprawnień z obu dopasowanych grup, nie tylko z pierwszej pasującej reguły.

5. Mapowanie danych kontaktowych: zakładka Media type mapping

```
Users → Authentication → LDAP settings → Servers → AD Zielona → Provisioning → Media type
mapping → Create media type mapping
Media type: Email
Attribute: mail
```

Dzięki temu adres e-mail wpisany w Active Directory trafia od razu do profilu nowo założonego konta Zabbixa, bez ręcznego uzupełniania go po pierwszym logowaniu.

6. Włączenie LDAP jako sposobu logowania: zakładka Authentication

```
Users → Authentication → Authentication
Default authentication: LDAP
Deprovisioned users group: Disabled
```

> **Pojęcie: grupa deprowizjonowanych użytkowników.** Grupa Zabbixa, do której provisioning JIT przenosi konto, gdy przy kolejnym logowaniu okazuje się, że dana osoba nie należy już do żadnej zmapowanej grupy w Active Directory, na przykład po odejściu z zespołu Oli. Wskazujemy tu grupę o statusie `Disabled`, żeby takie konto od razu traciło dostęp, zamiast wisieć aktywne z ostatnią przypisaną rolą.

Weryfikacja

Wylogowujemy się z konta `Admin` i logujemy testowo kontem `tomek.kowalski` z hasłem domenowym:

```
Login: tomek.kowalski
Password: (hasło domenowe Tomka)
```

Sprawdzamy we frontendzie, że konto zostało założone automatycznie z właściwą rolą:

```
Users → Users → tomek.kowalski
```

Przykład:

```
Username: tomek.kowalski
User type: Super Admin
User groups: Zabbix administratorzy
```

◫ ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran `Users → Users` z widocznym wierszem `tomek.kowalski`, kolumną `User type` ustawioną na `Super Admin` i kolumną `Groups` pokazującą `Zabbix administratorzy`, założonym automatycznie po pierwszym logowaniu LDAP.

Jeśli chcemy sprawdzić provisioning bez czekania na kolejne logowanie danej osoby, uruchamiamy je ręcznie:

```
Users → Users → tomek.kowalski → Provision now
```

Częste błędy

Objaw	Przyczyna	Co robimy
Logowanie LDAP zwraca „Login name or password is incorrect" dla poprawnego hasła	zły `Bind DN` albo hasło konta technicznego, Zabbix w ogóle nie może przeszukać katalogu	testujemy bind osobno narzędziem `ldapsearch` z hosta `mon01`, poprawiamy dane w konfiguracji serwera LDAP
Konto zakłada się, ale zawsze z rolą `User`, nigdy `Super Admin`	wzorzec `Group pattern DN` w mapowaniu grup nie pasuje do rzeczywistego DN grupy `GG_Zabbix_Admin`	sprawdzamy dokładny DN grupy przez `Get-ADGroup GG_Zabbix_Admin`, poprawiamy wzorzec
Połączenie z LDAP kończy się błędem certyfikatu	certyfikat CA Zielonej niezaufany przez system operacyjny `mon01`	kopiujemy `CA-Zielona.crt` do `/etc/pki/ca-trust/source/anchors/` i wykonujemy `sudo update-ca-trust`, zgodnie ze stroną Certyfikaty SSL, wystawienie, konwersja, weryfikacja
Osoba usunięta z grupy `GG_Zabbix_Admin` nadal ma uprawnienia administratora w Zabbiksie	provisioning JIT uruchamia się dopiero przy kolejnym logowaniu, nie od razu po zmianie w AD	dla pilnych przypadków wyłączamy konto ręcznie w `Users → Users`, zamiast czekać na naturalne wygaśnięcie sesji

> 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.

Ćwiczenia

1. Osoba należy jednocześnie do grup `GG_Zabbix_Admin` i `Domain Users`, obie zmapowane w tabeli grup na różne role. Jaką rolę dostanie po zalogowaniu?

Odpowiedź

Dostanie sumę uprawnień z obu dopasowanych grup, nie tylko z pierwszej reguły na liście. W praktyce, jeśli jedna z dopasowanych ról to Super Admin, konto końcowo działa z uprawnieniami Super Admin, bo to najszersza z przypisanych ról.

1. Dlaczego samo włączenie LDAP jako `Default authentication` bez skonfigurowania provisioningu JIT nie wystarczy, żeby nowa osoba mogła się zalogować pierwszy raz?

Odpowiedź

Bez provisioningu JIT LDAP obsługuje wyłącznie sprawdzenie hasła, ale konto użytkownika w bazie Zabbixa musi istnieć, zanim ktokolwiek się nim zaloguje. Administrator musiałby więc ręcznie założyć konto w Zabbiksie dla każdej nowej osoby, dokładnie ten ręczny krok, który provisioning JIT eliminuje.

Powiązane: Instalacja serwera Zabbix z pakietów na Rocky Linux 9 · Struktura OU Zielonej i delegowanie uprawnień · Monitorowanie typowych usług

Źródła: Authentication, dokumentacja Zabbix · LDAP, dokumentacja Zabbix · Just-in-Time user provisioning explained, blog Zabbix

---

Revision #24
Created 2026-09-28 16:57:52 UTC by Tomasz Konieczny
Updated 2026-10-26 14:09:43 UTC by Tomasz Konieczny