

Automatické přihlašování proti Active Directory (Windows Authentication)

Princip a protokoly

Automatické přihlášení je zapnuté jen tehdy, když jsou v konfiguraci nastavené obě volby ``LDAP:active = true`` a ``LDAP:automaticLogin = true``. Současné zapnutí ``LDAP:active`` a ``KeyCloak:active`` aplikace odmítne už při startu. Výchozím schématem ověření je pak Negotiate (balíček ``Microsoft.AspNetCore.Authentication.Negotiate``). Prohlížeč a server se přes něj domluví na protokolu Kerberos, a když to nejde, automaticky přejdou na NTLM. Aplikace zpracuje všechny tři typy identity, které mohou přijít: ``Kerberos``, ``NTLM`` i ``Negotiate``.

Aplikace běží na serveru Kestrel. Windows ověření proto provádí sama aplikace, ne IIS. Při nasazení pod IIS by ověření převzalo IIS a muselo by tam být zapnuté Windows Authentication. Ověření přes URL klíč (schéma ``URLKEY``) funguje dál. Pokud v požadavku klíč chybí, aplikace vyvolá výzvu k ověření přes Negotiate.

Požadavky na infrastrukturu (nejsou součástí kódu):

- server musí být členem domény,
- pro Kerberos musí být na účtu, pod kterým aplikace běží, zaregistrovaný SPN ``HTTP/<hostname>``. Bez něj se použije NTLM,
- adresa aplikace musí být v prohlížeči klienta v zóně Místní intranet (případně povolená politikou), jinak prohlížeč nepošle přihlašovací údaje automaticky,
- licence musí obsahovat modul ``ActiveDirectory``. Bez něj se automatické přihlášení nezdaří.

Získání a uložení uživatele při přihlášení

Po úspěšném Windows ověření převede ``ClaimsTransformation`` doménovou identitu na aplikačního uživatele. Volá k tomu

``UserActiveDirectoryManager.NtlmCheckAndSyncLoginAgainstActiveDirectory``. Pro každé připojení k AD z tabulky ``ActiveDirectories`` (připojení přes servisní účet) proběhne:

1. Dohledání uživatele v AD podle ``sAMAccountName``. Zkouší se jméno s doménou (``DOMENA\uzivatel``) i bez ní.
2. Zjištění členství ve všech AD skupinách, které jsou namapované na skupiny Infoportu.

3. Kontrola `LDAP:OnlyActiveDirectoryGroups`: pokud je volba zapnutá a uživatel není v žádné namapované AD skupině, nepřihlásí se a do DB se nezapíše.
4. Uložení do DB Infoportu:
 - neexistujícího uživatele aplikace založí (výchozí `RepositoryId = 1`),
 - existujícímu aktualizuje e-mail, jméno a příjmení podle AD,
 - dříve smazaného uživatele obnoví, pokud je v AD stále platný.
5. Synchronizace skupin a rolí: uživatele přidá do skupin Infoportu podle aktuálního členství v AD skupinách, nebo ho z nich odebere. Stejně upraví i roli `Repository` v příslušných repozitářích.
6. Kontrola přístupu do repozitáře a přihlášení:
 - pokud uživatel nemá přístup do svého aktuálního repozitáře, přepne se do prvního repozitáře, kam přístup má (přes vlastní claimy nebo členství ve skupině),
 - pokud takový repozitář neexistuje, aplikace ho odhlásí,
 - jinak se vytvoří aplikační přihlášení (`SignInAsync`, cookie `Identity.Application`).

Vztah k jobu na AD synchronizaci

Automatické přihlášení nevyžaduje, aby běžel job na synchronizaci AD (`SynchronizeADUsersJob`). Uživatel se založí, aktualizuje a zařadí do skupin přímo při přihlášení. K přihlášení stačí:

- licence s modulem `ActiveDirectory`,
- připojení k AD nastavené v administraci (Active Directory Manager),
- mapování AD skupin na skupiny Infoportu, rovněž nastavené ručně v administraci,
- dostupné AD v okamžiku přihlášení.

Job je doplňkový. Dávkově synchronizuje všechny členy namapovaných skupin, takže uživatelé existují v Infoportu dřív, než se poprvé přihlásí, a lze jim předem nastavovat práva. Změny v AD (odchody, změny členství) se díky němu promítnou i u uživatelů, kteří se nepřihlašují.

Omezení a známá rizika

- Výkon: převod identity proběhne při každém ověření požadavku přes Negotiate. Každý takový průchod znamená dotaz do AD, zápisy do DB a nové přihlášení. Při vyšší zátěži to může zatížit AD i databázi.
- Nedostupné AD: když se uživatele nepodaří dohledat (AD je nedostupné nebo chybí připojení), aplikační přihlášení se nevytvoří a uživatel zůstane jen s Windows identitou. V logu se objeví záznam „Transformation is needed, but it has not been done“.

Opravené nedostatky (říjen 2026)

- Přepnutí repozitáře při přihlášení (`ClaimsTransformation`): kvůli chybějícím složeným závorkám se uživatel považoval za úspěšně přepnutého, i když nebyl členem žádné skupiny repozitáře. Neoprávněný uživatel se proto neodhlásil. Zároveň se kontrolovala jen první skupina každého repozitáře. Oprava: přepnutí proběhne jen při skutečném členství a na odhlášení se čeká, než se dokončí.
 - Volba `OnlyActiveDirectoryGroups` (`UserActiveDirectoryManager`): podmínka zjišťovala jen to, jestli existuje nějaké mapování AD skupin, ne jestli je v nich uživatel. Do DB se tak zakládal kterýkoli doménový účet. Oprava: uživatel se přeskočí, pokud není členem žádné namapované AD skupiny.
-

V ručním LDAP přihlášení (`AccountController`) zůstává jedna drobnost: po nalezení skupiny se pokračuje v procházení dalších repozitářů. Uživatel se tak může přepnout vícekrát a platí poslední vhodný repozitář místo prvního.

Revision #1

Created 13 October 2026 10:26:54 by Jitka Kalíšová

Updated 13 October 2026 10:27:10 by Jitka Kalíšová