Kontrola dostępu do zasobów w systemie dLibra

Informacje ogólne

Kontrola dostępu do systemu dLibra składa się z dwóch etapów:

1. etapu **uwierzytelnienia**, na którym określana jest tożsamość użytkownika,
2. etapu **autoryzacji**, na którym to etapie następuje sprawdzenie, czy dany użytkownik ma prawo dostępu do żądanego zasobu.

Etapy te opisano szczegółowo poniżej.

Uwierzytelnienie

W systemie dLibra możliwe są następujące sposoby autentykacji:

- *Uwierzytelnienie podstawowe* - użytkownik wprost podaje nazwę użytkownika i hasło. Hasło użytkownika może być przechowywane w systemi dLibra lub na zewnętrznym serwerze LDAP.
- *Uwierzytelnienie IP* - użytkownik podaje tylko nazwę użytkownika, przy czym korzysta z komputera, którego adres sieciowy spełnia reguły dostępu bez hasła dla danego użytkownika. Reguły te muszą być wcześniej zdefiniowane w systemie dLibra przez administratora.
- *Uwierzytelnienie SSO (dostępna tylko w aplikacji czytelnika)* - identyfikator użytkownika pobierany jest z zewnętrznego systemu Single Sign-On na podstawie "biletu" SSO przekazanego przez użytkownika w żądaniu HTTP.

Autoryzacja

Po ustaleniu tożsamości użytkownika odbywa się określenie poziomu uprawnień danego użytkownika do żądanego zasobu. Możliwe są następujące poziomy uprawnień (na poziomie wydania publikacji):

- brak uprawnień,
- prawo przeglądania - prawo do odczytania wszystkich *opublikowanych* wydań publikacji,
- prawo odczytu - prawo do odczytania wszystkich wydań publikacji,
- prawo zarządzania - prawo do zarządzania publikacją (np. tworzenia nowego wydania lub przyznania praw dostępu).

Pozytywna weryfikacja uprawnień może odbyć się w jeden z następujących sposobów:

- *Autoryzacja bezpośrednia* - użytkownik, bądź jedna z grup do których on należy, ma wprost przyznane odpowiednie prawo do danego zasobu (zazwyczaj prawo przeglądania).
- _Autoryzacja implikowana_ - użytkownik, bądź jedna z grup do których on należy, ma przyznane do danego zasobu uprawnienie wyższego poziomu, niż uprawnienie pożądane. Dla przykładu: wymagane jest prawo przeglądania, a użytkownik czy też grupa ma prawo odczytu.

Członkiem danej grupy użytkownik może zostać albo poprzez przypisanie do tej grupy przez administratora, albo - w przypadku *dynamicznych grup LDAP (p atrz Podręcznik Administratora)* - na podstawie atrybutów jakie są przypisane użytkownikowi w zewnętrznym serwerze LDAP.

Przykładowe scenariusze

Poniżej przedstawiono kilka przykładowych scenariuszy opisanych powyżej mechanizmów autentykacji i autoryzacji.

1. Biblioteka cyfrowa z publikacjami dostępnymi bez ograniczeń

Opis: Biblioteka cyfrowa gromadzi zbiory, do których dostęp mogą mieć wszyscy użytkownicy Internetu.
Sposób konfiguracji: *Użytkownicy publiczni* mają przyznane *prawo przeglądania* dla wszystkich opublikowanych wydań. Nie potrzebują identyfikatora ani hasła żeby móc korzystać z gromadzonych zasobów.

2. Biblioteka cyfrowa z wydzielonymi zbiorami o ograniczonym dostępie

Opis: Biblioteka cyfrowa gromadzi zbiory, do których dostęp mogą mieć wszyscy użytkownicy Internetu oraz zbiory, których treść powinna być dostępna tylko z komputerów o określonych adresach IP (np. z czytelni).
Sposób konfiguracji: Dla zbiorów dostępnych bez ograniczeń konfigurowany jest tak jak w *scenariuszu 1*. Poza tym stworzony jest specjalny użytkownik o nazwie "Czytelnia", którego hasło zna tylko administrator. Użytkownik "Czytelnia" ma skonfigurowane reguły dostępu bez hasła z adresów IP komputerów znajdujących się w czytelni. Użytkownik "Czytelnia" ma przyznane *prawo przeglądania*dla zbiorów o ograniczonym dostępie. Użytkownicy komputerów w czytelni są poinstruowani, żeby w przypadku pytania o nazwę użytkownika i hasło podać nazwę "Czytelnia", a pole "hasło" pozostawić puste (tak na prawdę jego wartość jest w takiej sytuacji po prostu ignorowana). Użytkownicy o nazwę użytkownika pytani są tylko raz na początku każdej sesji. Próby takiego dostępu bez hasła z komputerów spoza wyznaczonego zakresu adresów IP nie powiodą się. Konieczne będzie wtedy podanie prawidłowego hasła użytkownika "Czytelnia".

3. Biblioteka cyfrowa dostępna dla wszystkich w sieci wewnętrznej

Opis: Biblioteka cyfrowa gromadzi zbiory, do których dostęp mogą mieć wszyscy użytkownicy sieci wewnętrznej.
Sposób konfiguracji 1: *Użytkownicy publiczni* mają przyznane *prawo przeglądania*dla wszystkich opublikowanych wydań. Nie potrzebują identyfikatora ani hasła żeby móc korzystać z gromadzonych zasobów. Biblioteka cyfrowa udostępniana jest tylko w sieci wewnętrznej przy pomocy zewnętrznych mechanizmów kontroli dostępu (firewalle itp.).
Sposób konfiguracji 2: *Użytkownicy publiczni nie* mają przyznanego *prawa przeglądania*dla żadnego z opublikowanych wydań. Stworzona jest specjalna grupa "Intranet" skonfigurowana i wykorzystywana analogicznie do scenariusza 2. **Uwaga:** W przypadku takiej konfiguracji użytkownicy publiczni mają dostęp do metadanych obiektów cyfrowych - blokowany jest tylko dostęp do treści.

4. Biblioteka cyfrowe ze ścisłą kontrolą dostępu

Opis: Biblioteka cyfrowa gromadzi zbiory, do których dostęp mogą mieć tylko wybrani użytkownicy.
Sposób konfiguracji: Należy założyć konta dla poszczególnych użytkowników i wprost przyznawać im właściwe uprawnienia do poszczególnych zasobów.

Mechanizm wykrywania prób nielegalnego dostępu

System dLibra posiada wbudowany mechanizm wykrywania prób nielegalnego dostępu. Jeżeli z jednego komputera (jednego adresu IP) nastąpi 5 kolejnych nieudanych prób autentykacji danego użytkownika, a odstęp między każdymi dwiema kolejnymi próbami będzie mniejszy niż 20 minut, to adres IP z którego nastąpiły próby autentykacji zostanie automatycznie dodany do listy adresów blokowanych dla tego użytkownika. Listą taką zarządza administrator biblioteki cyfrowej.