DrupalShibboleth

Elgondolás

A Drupal saját maga szereti kezelni a felhasználóit - adatbázisban -, de az azonosítás moduláris. A felhasználó beállításai a Drupal saját adatbázisában vannak, a Shibboleth modul csak a felhasználó azonosítóját adja meg.

Felhasználó létrehozása

Az IdP-nek azonosítania kell tudnia a felhasználót, tehát valamilyen központi adatbázisban léteznie kell.

Ha egy olyan felhasználó jelentkezik be a Drupalba, aki még korábban nem jelentkezett be (pontosabban ha a Shibboleth-en keresztül megkapott azonosító még nem létezik), akkor a modul létrehoz egy új Drupal felhasználót. A felhasználó jelszava egy olyan véletlenszerűen generált megfelelően hosszú karakter sorozat, amely egyaránt tartalmazhat kis- és nagybetűket, valamint számokat. Alapesetben a felhasználó számára a jelszó változtatása tiltott, így a hagyományos úton (felhasználó név/ jelszó párossal) nem tud. A későbbiekben a jelszó változtatásának joga azonban egyénileg, vagy csortosan kioszthatóezzel engedélyezve a két authentikáció párhuzamos használatát. Néhány felhasználói beállítás kezdeti értéke származhat a Shibboleth-től kapott attribútumokból:

- teljes név
- email cím

(Ez utóbb funkciót az implementáció nem tartalmazza, ugyanis a különböző Shibboleth beállításoknak megfelelően rendszerenként más információk állnak rendelkezésre. Ennek kezelése a modul jövőbeli fejlesztései közé tartozik.)

A felhasználói attribútumok változtatása az IdP-ben nem terjed át a Drupalra (leszámítva természetesen a felhasználói azonosítót), az Drupalban található attribútumok megváltoztathatók, ha ezt az oldal konfigurációja megengedi.

Az újonnan létrejött felhasználó alap jogosultságokkal rendelkezik, ezután az adminisztrátor további jogokat biztosíthat számára.

Felhasználó törlése

A felhasználót a központi adatbázisból kell törölni, ezáltal megszűnik a hozzáférése a Drupalhoz. A Drupal azonosítója és beállításai azonban megmaradnak, ami az alábbi következményekkel jár (Vigyázat! Ha korábban egedélyeztük számára a jelszavas belépést, akkor azt külön le kell tiltani!):

- ha újra kiosztják a felhasználó azonosítóját, akkor a régi beállítások lesznek érvényesek
- lehetséges privát üzenetet küldeni a felhasználó email címére
- a törölt felhasználó mindaddig be tud lépni, amíg a Drupal által használt cookie érvényes, ezért célszerű memóriában tárolt cookie-kat használni (ld.: Drupal modul konfiguráció)

A fenti problémákat csak úgy lehet megoldani, ha egy alkalmazás a törölt felhasználók státuszát inaktiválja a Drupalban (és a hasonló elven felépülő többi rendszerben is).

Shibboleth konfiguráció

Be kell állítani a RequestMap-et az adott virtuális szerver adott könyvtárára, majd az Apache-nak a megfelelelő `Directory` vagy `Location` blokkjában be kell kapcsolni a Shibboleth azonosítást.

> **Info**
>
> Lazy sessiont kell beállítani akkor, ha azt szeretnénk, hogy
>
> • anonymous módon hozzáférhető legyen a Drupal (pl. csak olvasásra)
> • az adminisztrátor be tudjon jelentkezni jelszóval.

Bővebben lásd: Required Session

Drupal Shibboleth modul

Amennyiben lehetővé szeretnéd tenni, hogy a rendszered felhasználói Shibboleth-en keresztül is azonosíthassák magukat, nem kell mást tenned, mint hogy a meglévő Drupal rendszeredhöz hozzáadjad a Drupal Shibboleth modul-t (shib_auth).

A Drupal Shibboleth modul angol nyelvű dokumentációja itt található

Figyelem

A szócikk további része lehetséges, hogy elavult, az angol nyelvű dokumentáció az érvényes!

Telepítés

1. Telepítsd a **userprotect** modult
   1. Töltsd le a rendszerünknek megfelelő verzióhoz tartozó **userprotect** modult a project honlapjáról!
   2. Kövesd a modullal együtt érkező README.txt utasításait a telepítéshez!
2. Telepítsd a **shib_auth** modult
   1. Töltsd le a rendszerünknek megfelelő verzióhoz tartozó **shib_auth** modult a project honlapjáról!
   2. Másold be a tömörítve érkező fájlokat a rendszered **modules/shib_auth** könyvtárába. (Ez elsősorban a <drupal telepítési könyvtára>/modules/shib_auth útvonalon érhető el, azonban néha - főként multisite alkalmazások esetén - ettől eltérő is lehet.)
   3. A portál adminisztrációs felületén keresztül (Administer/Site Building/Modules) engedélyezd a **shib_auth** modult! Amennyiben ezt a rendszer nem egedélyezné, bizonyosodj meg róla, hogy a Drupal verziójához tartozó modult töltötted-e le, valamint hogy a függőségként szereplő modulok be vannak-e már kapcsolva!

Konfiguráció

A modul telepítője elvégezi a szükséges beállítások és módosítások többségét, így neked már nincs sok tennivalód. Az egyetlen elengedhetetlen beállítás a modul (Administer/User management/Shibboleth authentication module settings útvonalon elérhető) adminisztrációs oldalán található, ahol megadható a a WAYF *localhost*-ra mutató útvonala. (például: */Shibboleth.sso/WAYF/NIIF-WAYF*)

Ajánlott a settings.php-ben (pl.: <drupal telepítési könyvtára>/sites/default/settings.php) a cookie-k élettartamát 0-ra csökkenteni. *ini_set('session.cookie_lifetime', 0);*

Használat

A modul működése automatikus. A felhasználók a modul által létrehozott block-ban található url-re kattintva (*lazy-session*) vagy automatikusabn, az oldal betöltése közben (*required session*) authentikálják magukat a hozzájuk tartozó, a szerver által megbízhatónak tartott IdP-nél. A

rendszer a apache modul által kapott információk alapján, az első bejelentkezés során létrehoz egy, a felhasználóhoz tartozó Drupal accountot, amihez egy véletlenszerű jelszót társít. Mivel a felhasználó ezt nem ismeri, így ezzel nem, kizárólag Shibboleth-es azonosítás segítségével tud belépni.

> **Info**
>
> Amennyiben engedélyezni szeretnéd egy felhasználónak vagy csoportnak a Shibboleth-es belépésen túl a jelszavas azonosítást **IS**, nincs más dolgod, mint:
>
> • a felhasználónak, vagy csoportnak a jogosultságokat kezelő oldalon engedélyezni a jelszavának átállítását
> • majd ezt követően:
> • beállítani neki egy jelszót és ezt közölni vele, vagy
> • rávenni, hogy egy Shibboleth-es belépést követően adjon meg magának egy jelszót.

Admin felhasználó bejelentkezése

Érdemes egy, a Shibboleth-től elkülönítve kezelt adminisztrátort is létrehoznod (például a telepítés során), hogy a rendszer az IdP-től függetlenül is használható maradjon, vagy hogy például szükség esetén magát a shib_auth modult is el lehessen távolítani.

Mivel a modul kikapcsolja a főoldalon megjelenő **user login** blokkot, így azon keresztül nem lehetséges a username/password alapú belépés. (Ez a blokk opcionálisan visszakapcsolható.) Ahhoz hogy mégis be tudj lépni töltsd be a <Drupal CMS elérhetősége>/?q=user oldalt anélkül, hogy Shibboleth-en keresztül authentikáltad volna magad.

Required session

Lehetőség van arra is, hogy a felhasználók Shibboleth-en keresztüli authentikációját kötelezően megköveteld az oldal valamennyi megtekintése előtt. Ebben az esetben azonban nem lehetséges a nem shib_auth-on keresztüli belépés, így amíg ez a kényszer fenn áll, nem megoldható, hogy adminisztrátorként lépj be.

Változat #3
cziernorbert hozta létre 2026-04-14 13:22:52 CEST
cziernorbert frissítette 2026-04-17 12:49:11 CEST