Použití shibbolethu pro autentizace ve WordPressu na webhosting.vse.cz

verze 2.0 – u nice URL pomocí htaccess je potřeba doplnit exclude pro Shibboleth.sso

Výhody

Jednotné přihlašování (Single-Sign-On) má dvě podstatné výhody:

* Uživatel zadá přihlašovací údaje jednou a může přistupovat k více službám. To mnoho uživatelů zatím neocení, pro mnohé bude důležitější výhodou to, že budou moci používat školní heslo (heslo do studijního systému).
* Poskytovatel služeb (v našem případě nainstalovaný WordPress) nemůže zcizit heslo. Tj. i když někdo úspěšně napadne instalaci WordPressu, tak se nedostane k heslům.

WordPress používá mixovanou autentizaci – část uživatelů se přihlašuje přes shibboleth a část uživatelů přes přihlašovací údaje uložené v lokální databázi WordPressu. Přihlašovací okno na adrese /wp-login.php po instalaci rozšíření pro Shibboleth vypadá takto:

Tj. jméno a heslo zadávají lokální uživatelé, uživatelé s přihlašováním přes Shibboleth kliknou na odkaz „Login with Shibboleth“. Lze nastavit automatické přihlašování pomocí Shibbolethu – odkazy na přihlášení uvedené na stránkách uživatele automaticky přesměrují na Shibboleth. Lokální uživatelé musí ručně zadat do URL cestu /wp-login.php a poté se jim zobrazí výše uvedený přihlašovací dialog.

Minimálně na začátku musí existovat jeden lokální účet – správce, který nastaví parametry pluginu a přiřadí práva aspoň jednomu uživateli vytvořenému přes Shibboleth. Nezkoušel jsem tohoto správce rušit, nepřipadá mi to jako správný nápad.

Nevýhody

Nelze se snadno odhlásit – je potřeba restartovat webový prohlížeč či vyčkat x hodin na vypršení platnosti přihlašovacích údajů. Většině uživatelů to asi nebude vadit, omezuje to správce, pokud se chtějí přepínat mezi účty. Lze to řešit přes anonymní (private) okna v prohlížeči.

Pro některé správce by mohlo být nevýhodou, že si uživatelé ze školy mohou vytvořit sami účet – nebudou moci nic vytvářet, neboť se přidělí práva Subscriber. Má to i výhodu – uživatel si sám založí účet a správce mu poté přiřadí správná práva (např. Author či Editor).

Postup nastavení

Nastavení autentizace se skládá z následujících kroků:

1. Záměr musíte dopředu sdělit správcům webhostingu na e-mail webhosting@vse.cz, neboť v konfiguraci shibbolethu je potřeba uvést každé doménové jméno (např. excel110.vse.cz), které bude používat ověřování pomocí shibbolethu.
2. Musíte stáhnout plugin Shibboleth z <https://cs.wordpress.org/plugins/shibboleth/>, rozbalit a nakopírovat na server do adresáře /wp-content/plugins
3. Povolit plugin a zkontrolovat, zda se do souboru .htaccess v domovském adresáři instalace WordPressu doplnili následující řádky:

AuthType shibboleth

Require shibboleth

1. Nice URL – pokud máte ve WordPressu hezká URL vytvářená pomocí rewrite v .htaccess, je potřeba doplnit výjimku pro Shibboleth.sso.\*, na osi.vse.cz vypadá příslušná část .htaccess takto:

# ignore Shibboleth.sso and index.php from rewrite

RewriteRule ^index\.php|Shibboleth\.sso.\*$ - [L,NC]

RewriteCond %{REQUEST\_FILENAME} !-f

RewriteCond %{REQUEST\_FILENAME} !-d

RewriteRule . /index.php [L]

1. Plugin je potřeba nakonfigurovat v **Setting -> Shibboleth**. V konfiguraci pluginu se nastavují následující položky (ukázky odpovídají webu excel110.vse.cz):

**Session Initiator URL**
hodnotu by měl vytvořit plugin, já mám <https://excel110.vse.cz/Shibboleth.sso/Login>

**Logout URL**
hodnotu by měl vytvořit plugin, já mám <https://excel110.vse.cz/Shibboleth.sso/Logout>

**Password Change URL**
Kde si uživatelé nastavují heslo. Uvedené stránka se zobrazí uživatelům přihlášeným přes Shibboleth při pokusu o změnu hesla. Já jsem nastavil <https://insis.vse.cz/auth/system/zmena_hesla.pl>

**Password Reset URL**
Pod přihlašovacím dialogem je volba pro obnovu hesla (lze v konfiguraci vypnout). Já jsem uvedl stránku pro obnovu hesla v InSISu (<https://insis.vse.cz/system/zahajeni_resetu.pl>), zobrazuje se všem.

**Shibboleth is default login**
Na úvodní stránce či v patičkách stránek bývá odkaz na přihlášení do WordPressu. Pokud se zaškrtne tato volba, tak se odkaz doplní o akci shibboleth (např. <https://excel110.vse.cz/wp-login.php?action=shibboleth>), která uživatele automaticky přesměruje z přihlašovací stránky WordPressu na přihlašovací stránku Shibboleth. Pokud je uživatel již přes shibboleth přihlášen (i u jiného služby), tak nemusí zadávat své přihlašovací údaje.
Pokud volba zaškrtnuta není, tak se všem zobrazí přihlašovací formulář a uživatelé s přihlášením přes Shibboleth musí kliknout na odkaz „Login with Shibboleth“.
U existujících instalací Wordpressu bych na začátku tuto volbu nechal odškrtnutou, po převedení uživatelů pod Shibboleth doporučuji zapnout.

**Shibboleth automatic login**
Nevím, k čemu tato volba je. Nenarazil jsem na rozdíly.

**User Profile Data**
Shibboleth po přihlášení předává WordPressu některé údaje. Nejdůležitější je **Username**, na základě něho se páruje uživatel v DB s uživatelem přihlášeným přes Shibboleth. Další se použijí při založení nového účtu, při zaškrtnutí Managed lze přepisovat hodnoty při každém přihlášení. Atributy by měly být nastaveny takto:

Username uid
First name givenName\_utf8
Last name sn\_utf8
Nickname uid *či* cn\_utf8
Display name cn\_utf8
Email address univerzitniEmail

Položka Username – hodnota uid znamená, že se použije školní uživatelské jméno, v mém případě je to pavlicek. Můžete použít ještě hodnotu eppn a uživatelské jméno bude poté ve tvaru pavlicek@vse.cz. Doporučuji preferovat variantu s uid.

**User Role Mappings**
Na základě atributů poskytnutých shibolethem lze přiřadit uživatelům přiřadit práva. Nedoporučuji používat, všechny přednastavené hodnoty jsem smazal.

**Default Role**
Nastavuji hodnotu Subscriber. Pokud nastavíte hodnotu (none), tak se nikdo přes shibboleth nepřihlásí a to včetně již založených účtů.

**Update User Roles**
**Odškrtnout** !!!!. Pokud byste nechali zaškrtnutu tuto volbu, tak i když uživateli změníte oprávnění např. na Editor, tak mu plugin při jeho příštím přihlášení nastaví roli zpět na defaultní, tj. Subscriber.

Nezapomeňte nastavení uložit.

Správa uživatelů

Správce může uživatele vytvořit dopředu či může nechat uživatele, aby se poprvé přihlásili a poté jim změnit práva (roli). Je zde ale důležité omezení – uživatelská jména ve WordPressu musí odpovídat školním. Pokud se používají odlišná či se na stejné uživatelské jméno hlásí někdo jiný, tak si správce musí dát nejdříve do pořádku uživatele.

Při větším nepořádku v uživatelích může být řešením používat jako username atribut eppn (tj. včetně @vse.cz). Poté starého uživatele smazat a při smazání převést příspěvky a nastavení na nový účet. Nevím, jak dobře to funguje.

Uživatel, který se hlásí přes shibboleth, se může přihlásit i lokálně, pokud zná heslo. Spíše to nedoporučuji, po převedení účtu pod shibboleth by měl správce dotyčnému nastavit nové náhodné heslo.