Реализация IdP сервиса на базе АБИС «РУСЛАН»

Усманов Рустам Тимурович, заместитель директора, Институт корпоративных библиотечно-информационных систем Санкт-Петербургского государственного политехнического университета

Излагается опыт создания поставщика идентификационных данных на основе базы данных читателей АБИС «РУСЛАН». Рассказывается о применении свободного программного обеспечения JBoss Enterprise Application Platform, Shibboleth, OpenLDAP.

С увеличением количества различных электронных информационных ресурсов, доступных пользователям библиотек, возрастает и количество проблем, связанных с их использованием не только в стенах библиотеки, но и из любых узлов Интернет. К таким проблемам можно отнести:

- утомительность регистрации в большом количестве информационных систем;
- необходимость управления большим количеством учётных записей пользователя (хранение паролей, актуализации данных);
- обезличенный доступ (там где это не требуется) при авторизации по IP-адресам организации;
- невозможность доступа с незарегистрированных у поставщика ресурса IP-адресов (смена адресов, необходимость доступа с любого адреса);
- риски нарушения законодательства о защите персональных данных.

Одним из способов решения такого рода проблем является использование технологий федеративной авторизации с использованием протокола SAML [1].

В конце 2013 года в Фундаментальной библиотеке Санкт-Петербургского государственного политехнического университета была успешно реализована разработки программного комплекса для поставщика идентификационных данных с использованием одной из реализаций протокола SAML – Shibboleth.

Основной задачей, которую приходится решать при развёртывании поставщика идентификационных данных, является привязка поставщика к источнику этих идентификационных данных. Такая привязка может осуществляться различными способами с использованием различных механизмов доступа к данным. Одним из таких механизмов, поддерживаемых Shibboleth, является протокол LDAP. Наличие положительного опыта работы с реализациями LDAP – клиентами и серверами – предопределило выбор именно этого механизма для осуществления связи с источником данных.

В нашем случае источником идентификационных данных является АБИС «РУСЛАН». Доступ к данным, в т.ч. к учётным данным читателей, этой АБИС осуществляется по протоколу Z39.50. Таким образом, задача привязки к источнику данных свелась к задаче построения шлюза LDAP-Z39.50, являющемуся одновременно сервером LDAP и клиентом Z39.50.

В качестве сервера LDAP было выбрано популярное свободное программное обеспечение OpenLDAP, поддерживающее механизм выполнения произвольных программ для связи с унаследованными источниками данных (базы данных типа shell). В тоже время наличие положительного опыта работы с клиентом Z39.50 PHP/YAZ (также свободное программное обеспечение) позволило использовать этот клиент в роли вышеуказанной произвольной программы.

Схема построенной информационной системы представлена на рис.1

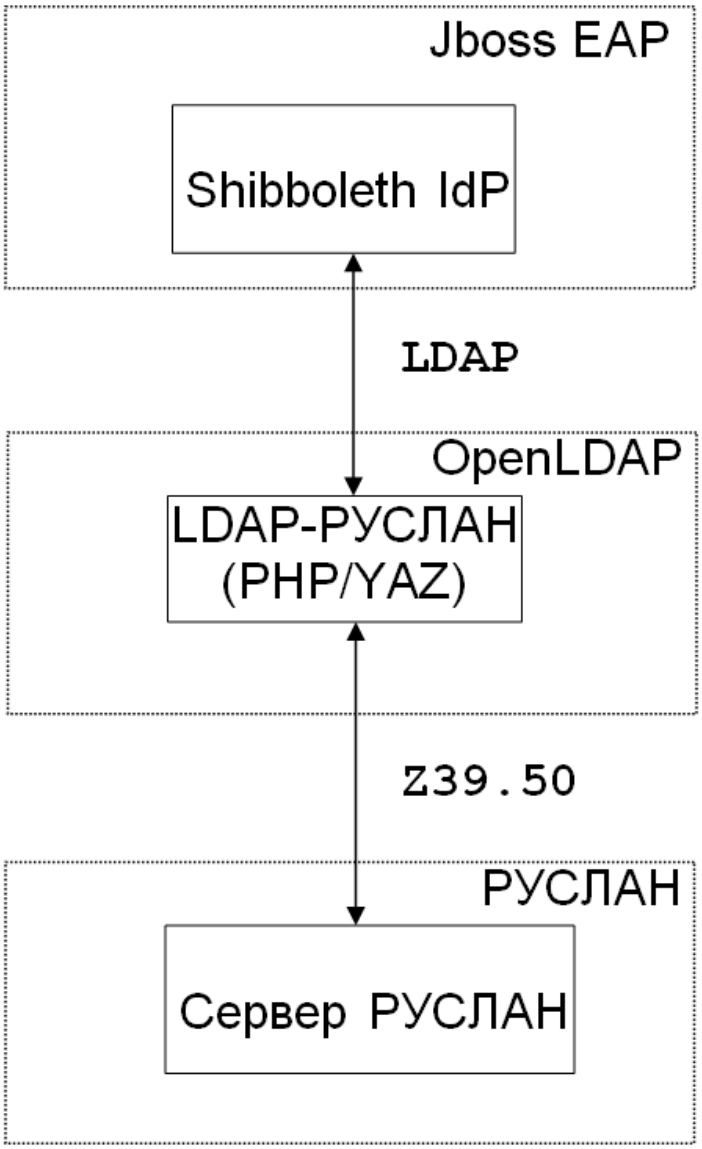

Рис.1. Схема реализации поставщика идентификационных данных

Разработанный шлюз LDAP-РУСЛАН стал центральной частью информационной системы. Большая часть времени была потрачена на конфигурирование и настройку параметров системы. Следует отметить, что при использовании БД типа shell в OpenLDAP и ОС Linux некоторые неудобства доставляют инструменты упреждающей защиты типа SELinux и AppArmor – приходится дополнительно разрабатывать соответствующие политики безопасности.

Реализация поставщика идентификационных данных в Фундаментальной библиотеке Санкт-Петербургского государственного политехнического уни-

верситета и его включение в федерацию ФЕДУРУС позволяет зарегистрированным читателям библиотеки в настоящее время получать дополнительные удобства при использовании следующих внутренних и внешних ресурсов:

- Электронная библиотека СПбГПУ;
- Портал АРБИКОН;
- ЭБС Айбукс;
- EBSCO;
- Web of Science.

Они могут получать доступ к этим ресурсам после однократной авторизации с использованием пароля и идентификатора, выданного им как пользователям Фундаментальной библиотеки.

Это же решение может быть применено во всех библиотеках, использующих АБИС «Руслан» для автоматизации, а также имеющих подписку на внешние базы данных. Отметим, что все ведущие поставщики научных баз данных поддерживают рассмотренный выше механизм идентификации для работы с поставляемыми ресурсами.

Список использованных источников

1. **Порхачев, Василий Александрович.** Сервисы Федеративной авторизации – пути развития [Электронный ресурс] / В.А. Порхачев .— Электрон. дан. (1 файл : 1.1 Мб) // XI международная научно-практическая конференция и выставка «Корпоративные библиотечные системы: технологии и инновации» [Электронный ресурс] : 24-30 июня 2013 г., Санкт-Петербург — Вильнюс — Клайпеда : [сайт] / Ассоциация региональных библиотечных консорциумов (АРБИКОН); Санкт-Петербургский государственный политехнический университет; Российская библиотечная ассоциация; Министерство образования и науки Российской Федерации .— СПб., 2013 .— (Основная программа) .— Свободный доступ из сети Интернет (чтение, печать, копирование) .— Презентация .— Adobe Acrobat Reader 6.0 .— <URL:http://arbicon.ru/conference/media/uploads/arbicon2013/materials/%D0%A1%D0%B5%D1%80%D0%B2%D0%B8%D1%81%D1%8B%20%D0%A4%D0%B5%D0%B4%D0%B5%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B9%20%D0%B0%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D0%B8%20%E2%80%93%20%20%D0%BF%D1%83%D1%82%D0%B8%20%D1%80%D0%B0%D0%B7%D0%B2%D0%B8%D1%82%D0%B8%D1%8F%20%D0%9F%D0%BE%D1%80%D1%85%D0%B0%D1%87%D0%B5%D0%B2.pdf>.