Generalizing B-Fabric towards an Infrastructure for Collaborative Research in Switzerland

Deliverable No D4:

Specification for Authentication via SwitchAAI Shibboleth

June 2010

Document Information

Project	
Project Title	Generalizing B-Fabric towards an Infrastructure for Collaborative Research in Switzerland
Project Start	01.06.2009
Project Sponsor	SWITCH (AAA/SWITCH Project)
Project Number	UZH.5

Document	
Title	Specification for Authentication via SwitchAAI Shibboleth
Date	
Author(s)	Fuat Akal, Can Türker
Total Number of Pages	
File Name	D4.docx
Key words	authentication, shibboleth

Table of Contents

Summary

B-Fabric has its own user management scheme including authorization and authentication. This requires that scientists (referred as users of B-Fabric) must register and create a B-Fabric account before using B-Fabric. In order to facilitate collaboration among users, we envision a dual login mechanism which also allows users log into B-Fabric with their Switch AAI/Shibboleth accounts as well as with their B-Fabric accounts.

Users may benefit from this support in several ways. First, users who already have a Switch AAI/Shibboleth account will not require anymore to explicitly register with B-Fabric and thus to take care of an additional account - for which they have to remember their login name and password. Second, any user with an existing Switch AAI/Shibboleth account will automatically have access to data that is public for the B-Fabric community. In other words, all users with a Switch AAI/Shibboleth account (currently these are more or less all members of Swiss academic institutions) will implicitly become a part of the B-Fabric community. Third, users may access several B-Fabric instances - possibly managed by different institutions - with the same login and password and thus increase the potential of collaboration.

This document describes the details of the dual login mechanism envisioned.

1 Introduction

B-Fabric provides and maintains a local user database to manage authentication and authorization of its users. The Switch AAI/Shibboleth-based authentication requires an extension and adaption of the current B-Fabric architecture with respect to the user management and service provision. In order to achieve this, we envision a dual login mechanism for B-Fabric. Users can either login with their B-Fabric or Shibboleth accounts. The login process is explained in details in the following section.

For two practical reasons, it is not possible to use only Shibboleth accounts to use all functionality provided by B-Fabric.

- First, the metadata about the user provided by identity providers is not complete enough to use all B-Fabric services. For instance, detailed address information is required for project requests, service billing or door key ordering (to physically access the FGCZ lab).

- Second, there are users that do not have Shibboleth accounts, e.g., academic users from other countries or external customers from companies.

Due to the above mentioned reasons, a simple elimination or complete replacement of the current user management of B-Fabric is not feasible, at least for the B-Fabric deployment at FGCZ where some applications require detailed personal user information and where users might not have Shibboleth accounts.

2 B-Fabric Login Process

Figure 1 illustrates how the login process will be performed with B-Fabric. Each B-Fabric user has two options to log into B-Fabric.

If a user has his own B-Fabric account already, he may choose to login with it as the first option. Once he logs in, he will be authorized with the privileges of that user.

The second option is to use a Shibboleth account. Here we must note that, the complete list of institutions from which a user can log in via Shibboleth accounts have not been determined yet. We, at the moment, foreseen only Swiss educational institutions are the allowed identity providers. If Shibboleth login is granted, the login process continues with further steps.

1. If this user has used B-Fabric before and also logged in by using his Shibboleth account, it is likely that his Shibboleth account has been mapped to his local B-Fabric account

already. If this is the case, the user is granted with the privileges of the mapped user.

2. If no mapping exists between the Shibboleth account and any of the local B-Fabric accounts, B-Fabric checks if there is any candidate account in its database which can be mapped to the user's Shibboleth account. Candidates are searched through e-mail addresses.
    a. If a matching account over e-mail addresses is found, the mapping is done automatically by B-Fabric by adding that user's unique Shibboleth ID to the B-Fabric user database. Once the user is mapped to the B-Fabric account, he is authorized as the mapped user.
    b. If no candidate is found, B-Fabric asks the user whether he has already a B-Fabric account under a different e-mail address?
        i. If yes, B-Fabric requires the user to login into B-Fabric with his B-Fabric account and redirects the user to a form where the user can manually couple his B-Fabric account with his Shibboleth account.
        ii. If the user has no B-Fabric account yet, he is asked whether he wants to have one?
            1. If yes, B-Fabric creates an account for the user by taking the received attributes of the authenticated Shibboleth account and does the mapping between the B-Fabric and Shibboleth accounts. At this point, user might also enter further information about himself which does not exist among the Shibboleth attributes.
            2. Otherwise, the user will be authorized with the privileges of the built-in *guest* account. The guest account only allows access to public data.

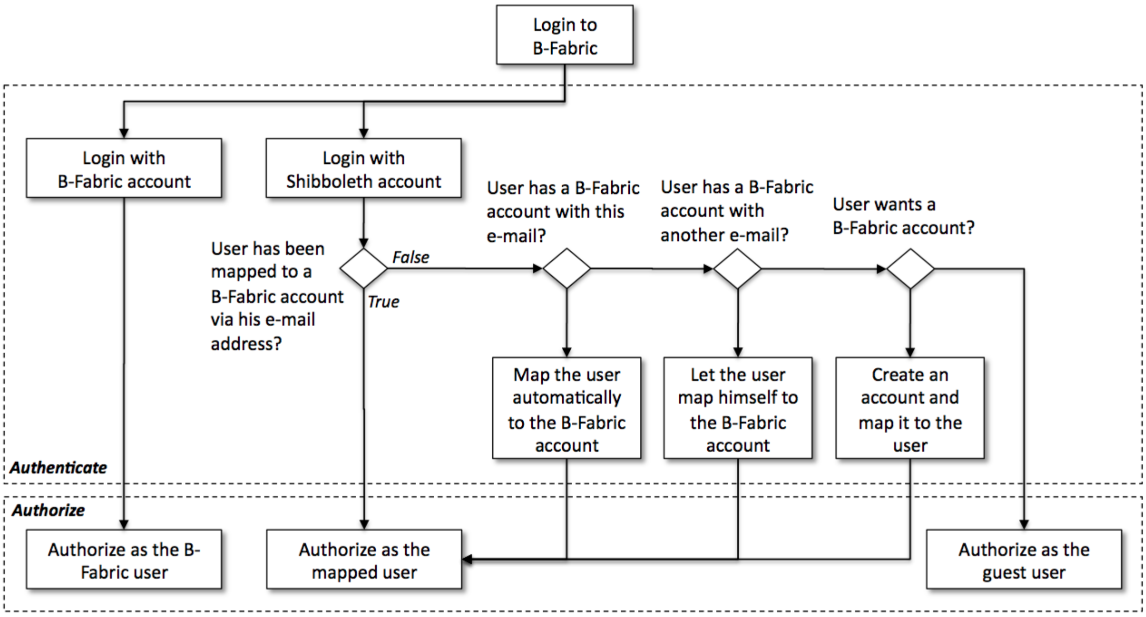
Login to B-Fabric
Login with B-Fabric account
Login with Shibboleth account
User has been mapped to a B-Fabric account via his e-mail address?
False
True
User has a B-Fabric account with this e-mail?
User has a B-Fabric account with another e-mail?
User wants a B-Fabric account?
Map the user automatically to the B-Fabric account
Let the user map himself to the B-Fabric account
Create an account and map it to the user
Authenticate
Authorize
Authorize as the B-Fabric user
Authorize as the mapped user
Authorize as the guest user

Figure 1 B-Fabric Login Process

3 Securing B-Fabric Resources with Shibboleth

B-Fabric uses the Glassfish application server as servlet container. That is, in order to secure B-Fabric via Shibboleth, an Apache Web server must be set up to front end the Glassfish server. Figure 2 shows the overview of the architecture. Also note that, we chose Glassfish over Tomcat (which is typically used servlet container with Shibboleth) due to robustness reasons.

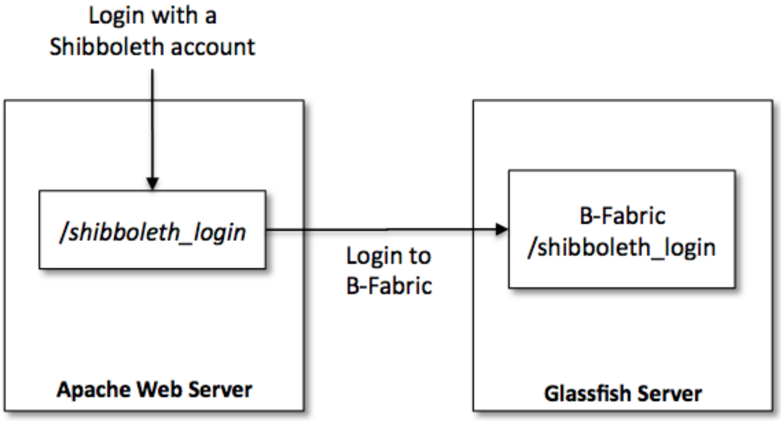

Figure 2 Securing B-Fabric Resources with Shibboleth

When a user wants to log in to B-Fabric with his Shibboleth account, he is directed to "*/shibboleth_login*" location defined in the Apache Web server. It is a Shibboleth protected location. It is also configured to forward incoming requests to the back-end Glassfish server by using the Apache JServ Protocol (AJP) which is a binary protocol that can conduct inbound requests from a web server through to an application server which sits behind the web server. With this configuration, all incoming requests to "*/shibboleth_login*" location in the Apache Web server are forwarded to "*/shibboleth_login*" location in the Glassfish server. Once the user is authenticated, post-authentication process is performed as explained in Section 2.

4 Needed B-Fabric Adaptations

With the support for Shibboleth based authentication the following adaptations and extensions of B-Fabric have to be carried out:

- Adapt/extend the database schema to capture the additional information regarding Shibboleth accounts.
- Adapt/extend the corresponding Java Entity Bean "User" and Session Bean "UserManager" to handle the additional information.
- Adapt/extend the Web Frontend to create and edit users in a way that users can also couple/decouple their B-Fabric accounts with/from their Shibboleth accounts, if they have any.
- Adapt/extend the Web Frontend to login into B-Fabric to provide dual-login.
- Write methods to detect and automatically couple Shibboleth and B-Fabric accounts
- Write methods and a new Web frontend screen for coupling a Shibboleth account with a B-Fabric account manually by users in case user has a Shibboleth account with a different e-mail address than what is known to B-Fabric.
- Implement the login handling workflow described in Section 2
- Install and configure an Apache Web server to front end the Glassfish application server.

5 Conclusion

With the support for Shibboleth based authentication having added, B-Fabric will be a more commonly used platform for collaboration among life sciences researchers (users) from Swiss academic institutions. Users with a Shibboleth account will be a part of the B-Fabric community. Such users will be able to access at least all public B-Fabric resources without having B-Fabric accounts. Furthermore, in case of several instances of B-Fabric hosted by several different institutions, users will only need a single account to access available data.