The UK Access Management Federation
FOR EDUCATION AND RESEARCH

EDINBURGH'S TELFORD COLLEGE

Table of Contents

Executive Summary 1
Background Information 1
Access Management 2
Methodology 2
Project Experience 4
References 4

These case studies, prepared by organisations who participated in the JANET Shibboleth on Windows project, are provided for information purposes only and reflect the particular arrangements and experience of those concerned. In each case, the configuration, installation and implementation of the Shibboleth on Windows software will vary according to the type of infrastructure and technical resources involved.

Executive Summary

This case study describes the experiences at Edinburgh's Telford College (ETC) of deploying Shibboleth on Windows in a multiple domain environment. The work was undertaken as part of JANET(UK)'s Shibboleth on Windows[1] project.

Background Information

About the organisation

ETC is the largest FE college in the Lothians and one of the largest in Scotland. It has over 600 staff and 15,000-plus enrolled students. Three years ago it moved to a £70 million state of the art campus in north Edinburgh. ICT Support consists of two teams: Support Services, who are primarily concerned with first line and desktop support, and Development Services, whose role is server and network support and various pieces of project work.

Resources

[1] http://www.ja.net/development/middleware/shibboleth-on-windows.html

There were three engineers assigned on a part time basis to this project. The college's infrastructure is predominately a Microsoft Windows Server environment (principally Server 2003).

Current situation

Along with many organisations, access to external resources was an ad hoc mixture of ATHENS, institutional user ID and passwords, and IP addresses.

Access Management

Had you used any other forms of Access Management previously?

No.

What were the drivers for deploying Federated Access Management?

One of the major drivers was cost saving. With the contract for ATHENS ending and college budgets being reviewed any extra costs were viewed with suspicion. Also important was centralisation of access management, with Shibboleth access tied into the user's institutional login for which there are well-defined processes for provisioning and de-provisioning.

What services do you want to be federated?

Internal and external.

Are you working towards single sign-on (SSO)?

Currently only external resources are federated. We are currently running an identity management project alongside the Shibboleth project and one of its deliverables was SSO. We did not feel Shibboleth was a solution for SSO for all of our internal applications. This was partly down to lack of development expertise in this area.

However the feeling within ICT is the users' experience will be improved no matter what mechanisms deliver the SSO.

Methodology

How did you deploy Federated Access Management?

A decision was made in the college several years ago to use a Microsoft Server platform. Therefore the college was looking for a Microsoft based solution – Shibboleth on Windows provided this.

The LDAP/Directory system in ETC is based on Microsoft's Active Directory. There is one forest with three domains; a root domain and two sub-domains, one for staff and the other for students.

It was intended to install one IdP which would access both domains to retrieve the required attributes from the relevant domain.

Who was involved in the process within your organisation?

ICT & LRC Management co-ordinated the project. It was tested by ICT Development Services (3 engineers) and LRC staff.

What were your objectives for deploying Federated Access Management?

To allow continuing access to external resources without incurring extra costs; and to simplify and centralise user account management, whether to internal or external resources.

What were your experiences – what went well, what were the main challenges and how did you overcome them?

The hardware platform running the IdP is a legacy HP DL380. This was chosen as they are normally reliable servers and the load placed on the hardware by the IdP software was not seen to be particularly taxing. However, loading on the server will be monitored as the academic term gets underway and the service starts to be used in earnest.

The initial installation was straightforward with the IdP installed in the root domain and the LDAP lookup base search in the staff domain. Testing against testshib.org showed attributes being released correctly.

However, when trying to do cross-domain and cross-realm authentication, i.e. trying to login as a student when the default setting was the staff domain and realm, we ran into problems. The initial authentication of the users' logon is handled by Windows and hence uses Kerberos. This should not be a problem with a single domain and hence a single Kerberos realm allows the appropriate user to login. However with two domains, setting the Kerberos realm to default to one domain required a user in the other domain to have to enter their user name and full domain path, i.e. user1*@staff.int.ed-coll.ac.uk* rather than the much simpler *user1*. The user name and path also had to be in upper case.

After discussion with SDSS we decided with their help to implement LDAP as the user authentication. This involved installing and configuring the Virginia Tech LDAP authorisation module in Tomcat. Once that was configured the lookup would start searching at the top of the forest and continue into both domains to look for user information. Once the LDAP login was implemented we were able to lookup in both staff and student domains. From there on it was a case of adding our metadata to the UK federation and testing against their test system.

Once we had a live IdP there were a few configuration issues with service providers, mainly linked to the type and format of the attributes we release; however we have worked through the majority of them.

How long did it take?

Overall the project took two months although this was on a part-time basis, with some long breaks in the work due to holidays etc. and while climbing a steep learning curve. All going well it should be possible to install an IdP from scratch in a couple of days.

What were your training/support and roll-out experiences?

One member of the team attended a Netskills course – Federated Access Management: Core Skills for Identity Providers. The rest of the information was gleaned via the Internet2 wiki, the project wiki, and a great deal of help from the SDSS software developer, Rod Widdowson.

So far the roll-out has been uneventful; however it is still early days and the product will only really be fully tested when the academic year begins.

Do you have any hints/tips/gotchas to look out for and things you would do differently?

It would have been useful to have been more aware of the terminology used and the mechanics of the Shibboleth process. Basically, more reading about and around the topic before diving in!

What have been the actual benefits since deployment – improvements in end user experience; administration; convergence of internal/external systems. etc.?

Again, it is early days in the deployment; however, we have already seen some benefits. User administration has been simplified and centralised. Users are automatically given access to external resources with their college account; they do not have to ask or wait for another account to be created.

Are there any aspects of the process of deployment that could be made easier with centralised effort (i.e. JANET assistance)?

No, the deployment itself was straightforward. It was the college's particular infrastructure that caused issues.

Project Experience

Conclusions and Implications

The project itself was fairly straightforward with complication being added by the college's particular infrastructure. We could have deployed two IdPs, one for staff and another for students; however, this would have had the potential for confusion when using the federation's WAYF and would have meant double the administrative work on the servers.

Recommendations

Learn as much as possible about the terminology and the authentication/authorisation process used by Shibboleth, as this makes trouble shooting so much easier.

References

http://www.middleware.vt.edu/doku.php?id=middleware:opensource:LDAP

http://shibboleth.internet2.edu/

Copyright

For further enquiries, please contact JANET Service Desk on service@ja.net or 0870 850 2212.

The Shibboleth on Windows Installer was a JISC funded project.

Disclaimer

This case study is provided by JANET(UK) for general information purposes only and the JNT Association cannot accept any responsibility and shall not be liable for any loss or damage which may result from reliance on the information provided in it.