Details on Metadata Management
Stephanie Obodda - 2020-12-10 - 0 Comments - in Shibboleth Single Sign On

**Editing the Metadata**
The campus federation metadata is stored in subversion at:


Generally, any changes should be made locally and then pushed to the repository.

**Acquiring the Metadata from a new Campus Service Provider**
Once the sysadmins set up a new SP, they will turn it on and then the metadata for that new service provider should be available at the URL:

[sp.brown.edu]/Shibboleth.sso/Metadata

**Publishing the Metadata to the IdP servers.**
The scripts for managing the metadata are located on opel for production and quantum for QA in the directory:

/opt/local/shibboleth-metadata/

Update the copy of the unsigned metadata

```
./svn update
```

Make sure there were no conflicts, if so, resolve them first.

Then run

```
./publish_metadata.sh
```

This script will prompt you for which external server you want to deploy to, the certificate to use in the signing, and then will scp the signed file to the remote server to two locations, one a tomcat application that serves the metadata to all the campus federation, and two the remote idp directory. If no remote server is specified, the script will only deploy the metadata locally.
**Best Practices/Troubleshooting**
The best method for deploying metadata is to configure the new SP to use the qa IdP for authentication. Deploy the metadata to the QA servers and test.

If there is a global problem with the new campus metadata, none of the SPs should be able to authenticate. Revert to the last working version in subversion. And then locally diff the versions to figure out what went wrong.

If there is a typo in the new SP metadata (either through transcription or misconfiguration) other SPs should work and this one will fail to authenticate. Double check the metadata to make sure it was copied correctly, and if it is OK, then there is likely a misconfiguration on the SP end.

Once the metadata is debugged on QA, deploy to production. Make sure to remember the DR IdP at the P1 location (burns at the time of writing).

**Future Enhancements**
In the future, it would be better to further automate this process as there are far too many manual steps. Existing projects will need to be evaluated.

Tags

Business Systems