University of Edinburgh Grouper Page

Introduction/History

At the University of Edinburgh we chose Grouper as part of the implementation of an in-house Identity Management System. We needed a Group Management solution and after evaluating a few products, both commercial and free open source ones, we chose Grouper.

We originally deployed Grouper 1.5.0 to live in around 2012, and as part of that did an upgrade to 1.5.3. In 2015, we have upgraded Grouper to version 2.2.0, mainly to take advantage of the new UI and change based PSP.

Overall Grouper has been an invaluable addition to us, as it has "just worked" with a minimal amount of fuss, which is always a good sign in a piece of software!

Grouper Usage

We use Grouper for a few main reasons:

- We need a centrally provided group store which other systems can use as an authoritative source of group and membership information
- We need our Identity Management System to use groups to make decisions on which services to provision with identities.
- We need to provision an Open LDAP directory with groups for other systems and services to make use of centrally provided groups
- We need to optionally allow the creation of devolved adhoc groups which can be then used for other systems to make use of.

Grouper structure

Our Grouper top level (root) structure is as follows:

- Organisational Hierarchy - The organisational structure of the University
- Affiliation groups - Groups containing how identities are affiliated with the university, e.g. staff, undergraduate student etc
- Courses
- Programmes of Study - These are also attached to the Organisational Groups
- Adhoc groups - An area for devolved creation of groups
- Service groups - Service level groups to which individual identities can manually be added

Subject (Identity) Source

Grouper is set up to use our Identity Management System as a source of identities. This is set up as a simple query on the IDM database.

Grouper technical information

We run Grouper on two Red Hat Linux servers per environment, sitting behind a hardware load balancer. One of those servers is set up to run provisioning to Open LDAP (both can, only one does at any given time). Grouper UI and Web services are deployed into Tomcat, and have Apache in front connected via ModJK. We use Cosign for Single Sign-Onto the UI, which is provided via an Apache mod, the remote user is set and this is what Grouper is set to use. For SOAP web services we use standard authentication not hooked into SSO.

Database: Oracle 10g
Java: 1.8.x
Tomcat: 8.0.x (512MB->1GB memory)

Grouper SOAP Web Services

The Identity Management System uses the SOAP based Grouper API to perform CRUD operations on Groups and Memberships.

At the University of Edinburgh we use Oracle SOA, we have also provided Oracle SOA services which wrap some of the key read operations on Grouper, namely:

- Get group
- Get group members
- Is user member of group

(We do this to provide a suitable abstraction from the underlying implementing service, which should protect services in the event of upgrades which for example change the underlying API)

Grouper PSP

We use the Provisioning Service Provider to provision groups and memberships to our Open LDAP servers. It's safe to say this we found this the most complex part of setting up Grouper 2.2 (Grouper 1.6 setup was pretty straightforward), most of the examples provided for Grouper were using LDAP as the identity source, configuring grouper to use a database source for identities and provision LDAP was complex for us to set up and get right.

Additionally we found we had to give the PSP process a fair amount of memory to perform bulk provisioning.

Grouper Hook

We also have a grouper hook set up which we use to:

- Assign a GID to any new groups
- Tell the IDM about any changes to groups. The IDM can then tell other services about group changes.

Grouper sizing

On live at the moment we have roughly **600,000 identities**, **65,000 groups**, and **2,300,000 memberships**.

Future roadmap

The next step steps for Grouper are as follows:

- Grouper is to also provision our Active Directory service with groups. We're in the initial investigation steps on this, with plans to hopefully begin provisioning Grouper Groups to AD this year. Given the complexity of the Open LDAP provisioning setup, we will most likely spin off another separate Grouper instance specifically configured for Active Directory rather than bundle the two into a single instance.
- We will migrate the Grouper Database to Oracle 11g on new infrastructure