Cardiff Grouper Project Page

Grouper at Cardiff University

Cardiff University introduced Grouper into an existing Identity and Access Management infrastructure in 2009. This work was in part funded by the Joint Information Systems Committee (JISC) under project Cuckoo. It is used as a centrally supported tool to manage:

- Automatically provisioned groups where the data required to calculate membership exists in corporate systems of record
- Manually managed groups

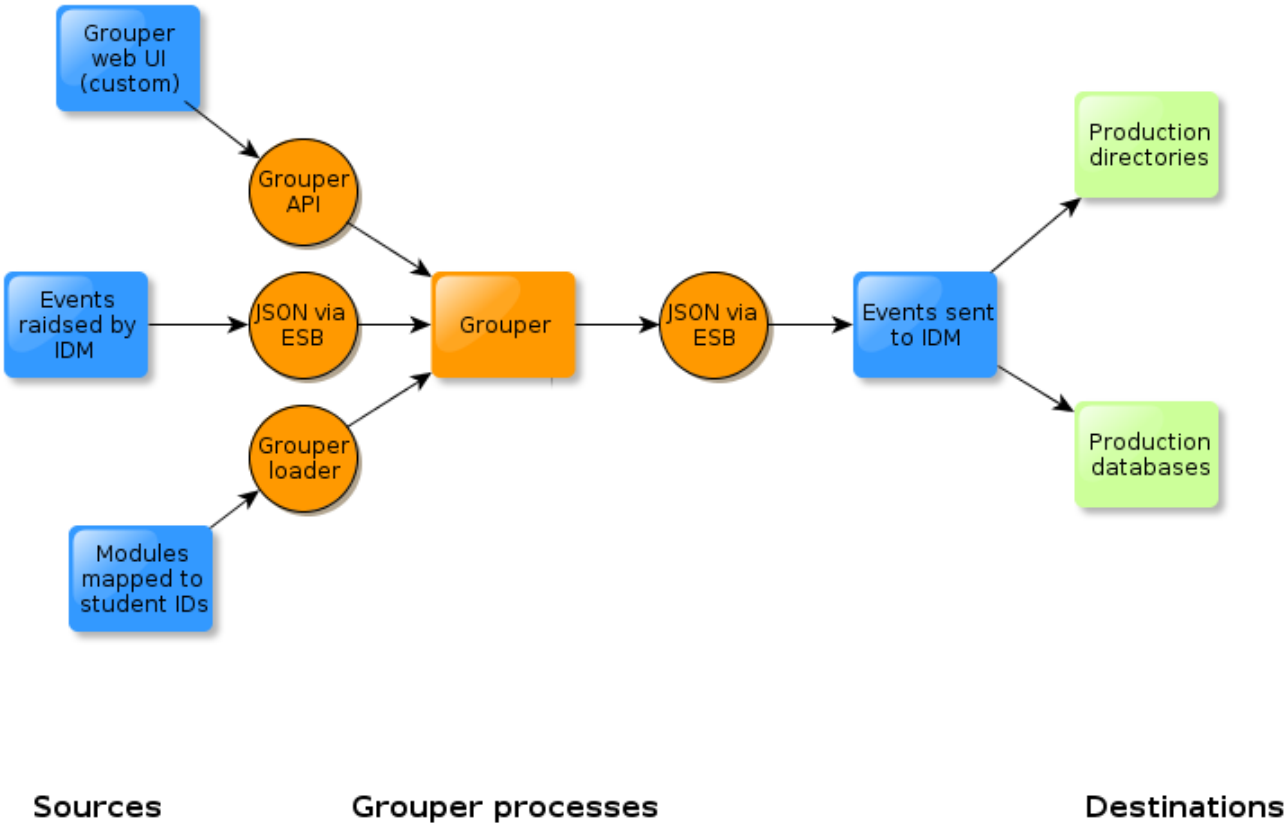
Groups are stored in Grouper and provisioned from Grouper into 4 LDAP directories, which are used by scores of applications for authentication and authorisation. We have more than 1,500 centrally managed groups organised in a hierarchical group structure which mirrors the organisational structure. We use nesting of group memberships extensively in Grouper and in the LDAP directories to keep the number of direct memberships down. We have 95,000 direct memberships within Grouper, and 175,000 indirect memberships. Our largest group has a membership of >30,000 indirect members.

Data processing through Grouper

Our IDM infrastructure favours event based processing over batch. We use an Enterprise Service Bus to provide interfaces between different systems, and ActiveMQ to manage queueing for asynchronous event processing. An ESB interface was written to enable events to be propagated to and from Grouper. This was contributed to Grouper and now forms part of the Grouper release. The IDM system calculates group membership using Drools rulesets, and sends changes of membership to Grouper for processing. Membership changes are then sent from Grouper to the IDM system using the changelog daemon and the ESB interface, and executed in one LDAP directory. Membership changes are then propagated to other directories using the existing infrastructure.

A user-targeted web interface is also provided for technical users, enabling the management of groups to be delegated. This is a custom interface, built on Spring webflow and Spring MVC, as the Grouper administrative UI was considered inappropriate for this use.

We are starting to roll out module groups for students. This data is not stored in the IDM system, and so is sourced from an intermediate set of data tables which are maintained by cron jobs. They are loaded using Grouper Loader and refreshed daily. This will add a further 4,500 groups and 153,500 direct memberships.



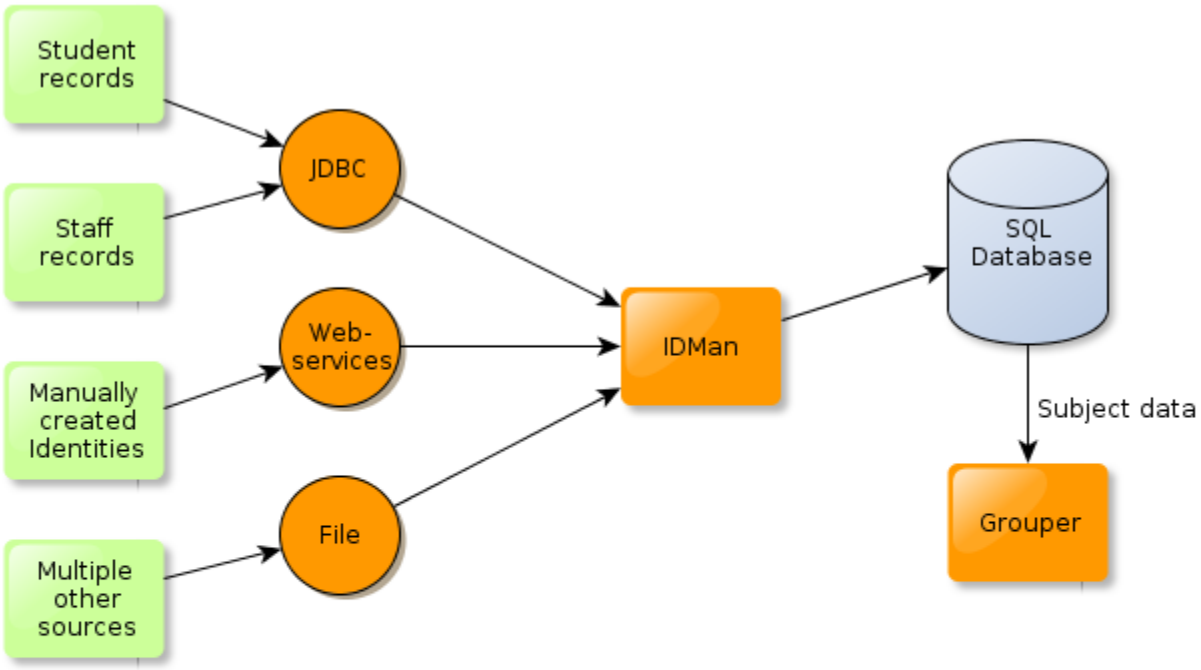
The groups in production directories are available for use by scores of systems, including:

- Filesystems for ACLs
- Applications made available through Zenworks
- Wikis
- Portal

- Other web applications which consume LDAP groups
- Mail listserver
- Shibboleth

Grouper subject source

Our identity management system presents a consolidated view of all users within the University. This data is available through LDAP, SQL and Webservices Interfaces. Following testing, the SQL database was selected as the subject source for Grouper as it offered the fastest performance. Having a single subject source addressable by JDBC enables the Grouper infrastructure to operate efficiently.



Grouper provides the core of a very successful, high performance group management and synchronisation infrastructure at Cardiff University.

- 95% of required core functionality was already available
- Remaining 5% could be easily added
- Grouper development team very welcoming and easy to work with
- Mature and stable - no errors encountered during testing, implementation or production
- Uses reliable underlying technologies such as SQL database, JDBC and Hibernate