

Using Grouper: Newcastle University case studies

Richard James
Caleb Racey



Context: Newcastle University



- UK University
- Over 5000 staff members
- Over 20,000 students
- Research focused
- Centralised IT service
- Malaysian Campus

Context: Who we are

Caleb Racey – Team Leader of Middleware Team

9 years experience of web application provision

Particular focus on issues of single sign on and access control

Richard James – 2 years as Computing officer within the Middleware Team

Main focus on Group Management and data integration

Lead project officer in GRAND project

Grouper Deployment at Newcastle University

First deployed 3 years ago

Early focus on access control via Shibboleth i.e. Wiki access

Advancements in Grouper led to new Use Cases being identified

- New components – Grouper loader
- New Grouper integration methods – LDAPPC, LDAPPC-NG
- New in house integration tools – Talend (www.talend.com)

Background – Grouper components implemented

Grouper Loader

- Uses HR data to load Newcastle University's organisational structure
- Provide source groups and roll up groups

Web services

- Administration of access to wiki service

LDAPPC

Maintenance tools

- Unresolvable subjects/ Bad membership finder

Grouper Deployment at Newcastle University

Focus on 3 main use cases

- Controlling access to web resources via Shibboleth
- Grouper and Active Directory
- Grouper integrating with Third Party Systems

Controlling access to web resources via Shibboleth

First deployment to provision access to wiki service

- Grouper's web services
- Custom built UI to add/delete members
- Moving towards using the new Lite UI

Grouper Group's released to Shibboleth as attributes

`HTTP_SHIB_GROUPER_GROUPS`

`etc:wheel;Applications:CBC:CBCUser;Applications:Collaboration
ASSD_Middleware,Information_Apps_All;CorporateData:Org_St
Customer_Services_All;CorporateData:Org_Structure:Newcastle_`

Make use of Shib's Grouper Groups attribute in htaccess file

- require nclgroup NCL:UserGroups:Richie:RichiesGroup

Scenario - Reading List System

System to allow module leaders and lecturers to manage reading lists

Access dependant on users contribution to module

- Leader, Lecturer, Demonstrator

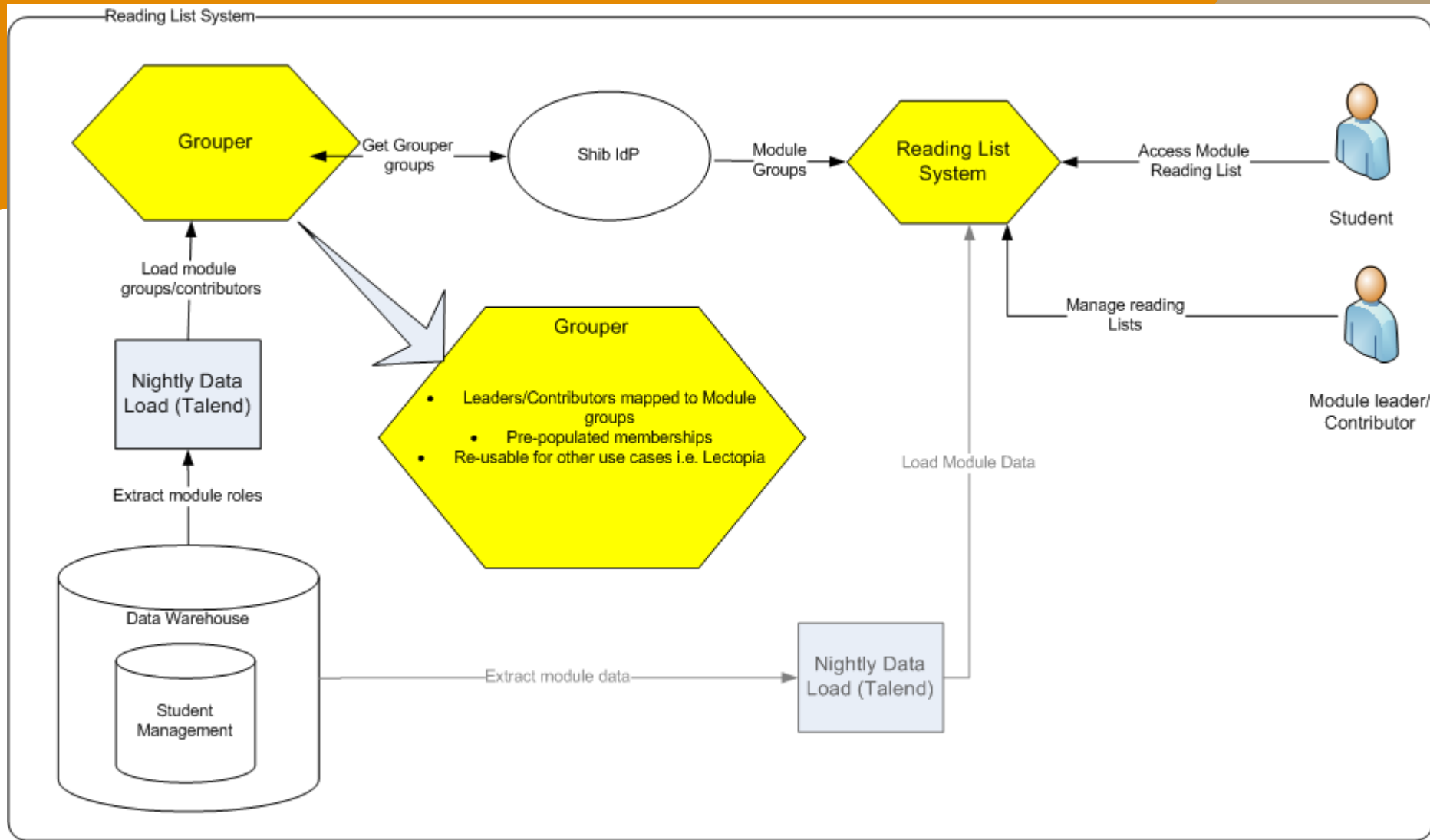
Data from Student Management system to pre-populate access groups

Data integration tool Talend to extract, manipulate and load data

- Groups loaded via GSH command line

Library_Admin group granted administrator privileges on all modules

Groups released as Shibboleth attribute



Use case document available at
<http://research.ncl.ac.uk/grand/resources.php>

Grouper and the Active Directory

LDAPPC/LDAPPC-NG enable Grouper to provision groups to the AD

Why this appeals to us?

- One access group for all
- Access group defined in grouper
- Use HR/Student Management Data
- Control wiki, mailing list, blog access using Shib Attribute
- Control access to file space via AD

Scenario – Delegating access to Wireless Network

Needed a method to delegate access to Wireless network dependant on user type

- Staff and Research Postgraduates to get full access
- Undergraduates and Taught Postgraduates to get part access

Microsoft Radius server had no way of accurately determining user type

- No attributes attached to user in Active Directory to define “type”
- Access delegated on format of Login ID

Restricted to delegating access solely on a users Login ID

Encourages departments to come up with own wireless network solutions

Solution – Delegating access to Wireless Network

Utilise HR/Student Management system data to determine a user type

Create roll up groups for student types

- Undergraduates
- Taught postgraduate
- Research postgraduate

Create access control groups for types of access

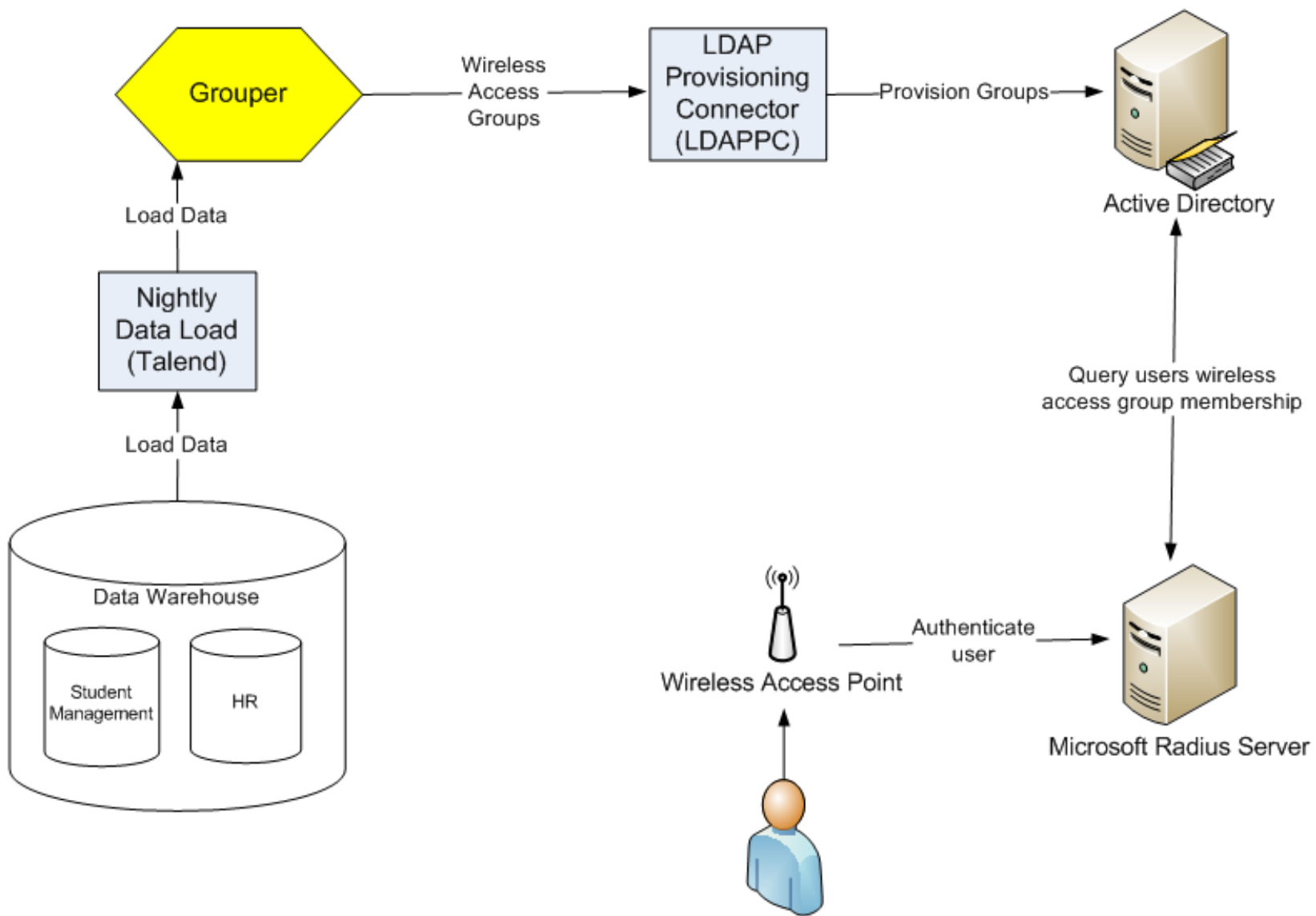
- Assign access using student roll up groups
- Use Org_Structure to assign membership to all of Newcastle University

Provision access control groups into AD

- RADIUS server can query a users membership of access groups

<http://research.ncl.ac.uk/grand/resources.php>

Wireless Network Access



Grouper with third party systems

Systems cant always directly integrate with grouper

- Non web-based, non LDAP based...

Need alternative method of extracting Grouper groups and provision to systems

- Use pre-existing open source tools
- Data integration tool – Talend

Extract data from Grouper

- Direct from Grouper databases, web services
- Combine with organisational data, i.e. HR and Student Management data
- Range of connectors/adaptors allows for easy integration with other systems

Rapid development which is easily maintainable...

Scenario – Syllabus Plus room booking system

Syllabus Plus room booking service

- Backend not web based
- Required role based group management from a central source
- Role membership dependant on department/faculty

Grouper perfect solution to manage roles

- Centralised management
- Admin has full control over roles
- Org_structure allows departments to be assigned to groups
- Individual memberships for more restricted roles



Scenario – Provisioning from Grouper into Syllabus Plus

Talend provided the components necessary to achieve this

Extract role memberships from Grouper

Combine with HR data

- Job position, known as name

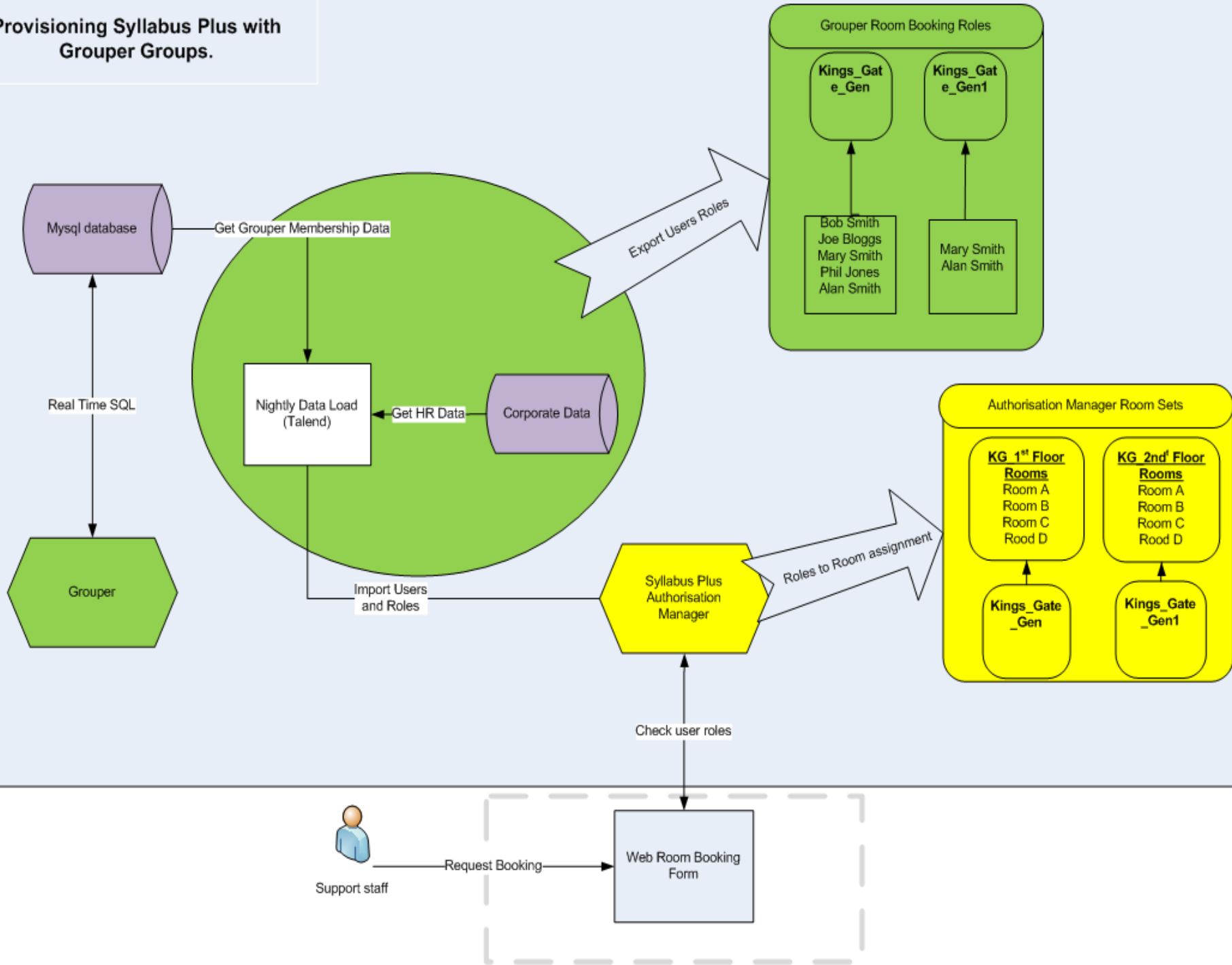
Transform data into desired output format

Transport data from Grouper into Syllabus Plus

Access to syllabus plus room booking service controlled
by roles managed in Grouper

<http://research.ncl.ac.uk/grand/resources.php>

Provisioning Syllabus Plus with Grouper Groups.



High Availability

- Currently it is not a key priority
- Many implementations don't require real time querying of Grouper
- In the future may need to reconsider
 - More use of real time querying from Shibboleth

Any Questions?

Details of all Use cases can be found at
<http://research.ncl.ac.uk/grand>

Contact the project at <http://research.ncl.ac.uk/grand/feedback.php>
or via grand@ncl.ac.uk