Use Case – Newcastle University Wireless Access

Scenario

Information Systems and Services at Newcastle University have a campus wide wireless scheme that provides a secure method of accessing the campus network. Due to guidance by the internal audit department, upon trying to access the wireless network, the network forces users to authenticate themselves against the active directory, before being allowed access to the service.

The level of wireless access provided is based on the user's status within the University, be it either student or staff member. Currently the Active Directory has no attributes attached to the user object to determine what a user's "type" is. The current process determines a user's type upon the user ID; staff will use a nID to login i.e. njb99, whilst a student's user name is in the format of a123456. The process is currently achieved by using a Microsoft Radius server. Although the process works, the end result is not fully accurate, as there are a number of staff members who have a user ID in the student format, due to originally studying at the University before being employed by the University. It is the case that staff members can also study at the University, and therefore they are provided with both a student and staff login account.

The current process limits the control that the Network team have over determining what levels of access users can have; they are restricted to basing it solely on the user being a staff member or student. The review of this process has recently been prompted after discussions between ISS and the Computing Science department. The Computing Science department currently have their own wireless setup as the ISS setup was originally not deemed suitable for their requirements. Due to the recent improvements in the wireless service, they have expressed an interest of once again making use of the ISS service. Yet, there are some pre-requisites to the services that they try to deliver to their users, which requires the process of access control to be re-structured.

Currently the ability to be able to distinguish between a student and staff member fits the needs of ISS. However the Computing Science department have put forward the need to be able to group students into sub groups to determine what level of access they will get. These sub groups would be undergraduates, taught postgraduates and research postgraduates. Students enrolled on an undergraduate or taught postgraduate course would be treat as a student. Yet students who are a research postgraduate would be granted full access like a staff member. With the current setup it would not be possible to distinguish between these sets of students and therefore an alternative approach needs to be investigated.

The current closed source system allows access control based on group information, the network team are currently moving towards an open source RADIUS authentication package. The new package will provide more flexibility on what the network team can achieve; either way the proposed approach will work with both packages. They require a method of creating the sub groups on an automated basis before porting these across to the Active Directory. Grouper is an ideal solution; it will provide the basis to create the necessary sub groups using the corporate data that is loaded in on a nightly basis, before provisioning these groups across into the Active Directory.

Actors

- All University staff members
- Students
    - Undergraduates

    - Taught postgraduates
    - Research postgraduates
- Grouper

Approaches and Considerations

The approaches to this scenario are limited due to the nature of the sub groups required. The groups are high level and will take the format of roll up groups that are currently used in the organisational structure loaded into Grouper. The level of granularity required will not need to be fine grained, scenarios such as only allowing 10 students from a particular course to be provided with a certain level of wireless access is something that the service will not have to deal with.

As set out in the "Organising Groups within Grouper" document, the access groups used in this scenario should sit within the Applications stem, as they will make use of groups created from the corporate data stem and possibly custom made groups from the user group stem.

The delegation of access control is split between two main sets of users, students and staff. The grouping of all staff members is a simple process as this is already represented within Grouper as part of the organisational structure. The organisational structure is made up of a series of source and roll up groups, which allows access to be delegated on a team or departmental basis. The role up group for Newcastle University can be utilised as part of delegating the access to the wireless network for staff members.

The provisioning of access control based on a Students type does require some further structuring of the data currently represented within Grouper. Student data is currently represented within Grouper, with regards to students enrolments to modules. Yet, this data does not distinguish between the types of student and therefore there is not a way of determining if a student is a postgraduate or undergraduate.

It will therefore be necessary to create a new set of roll up groups for students similar to those used as part of the organisational structure. The placement of these new roll up groups is important, it needs to be considered whether these groups could be utilised in provisioning access control in further use cases in the future. The ability to be able to distinguish between different types of students has been discussed previously as being a useful dataset to represent within Grouper for use cases such as controlling who can view certain lecture captures. Therefore due to the possible reuse of the student roll up groups, the groups should be created within the corporate data stem. This is the natural home for the groups as they will be pre-populated with corporate data and subsequently non-editable.

Within the corporate data stem, three new loaded groups will be created to distinguish between student user types as shown in figure 1. The groups will be "Undergraduates", "Taught Postgraduates", and "Research Postgraduates", the memberships for each of these groups will be achieved through the use of the Grouper loader or via a job using the data integration tool Talend.

Alongside these three corporate data groups, access role groups will also be created, these groups will determine a user's level of access to the wireless network. Currently it is proposed to provide two levels of access, full access for staff members and part access for students, the correct terminology for these levels have not yet been finalised. For the purpose of this use case, the two access control groups will be referred to as "Full Access" and "Part Access". These groups are then able to make use of the groups that have been created within the corporate data stem.

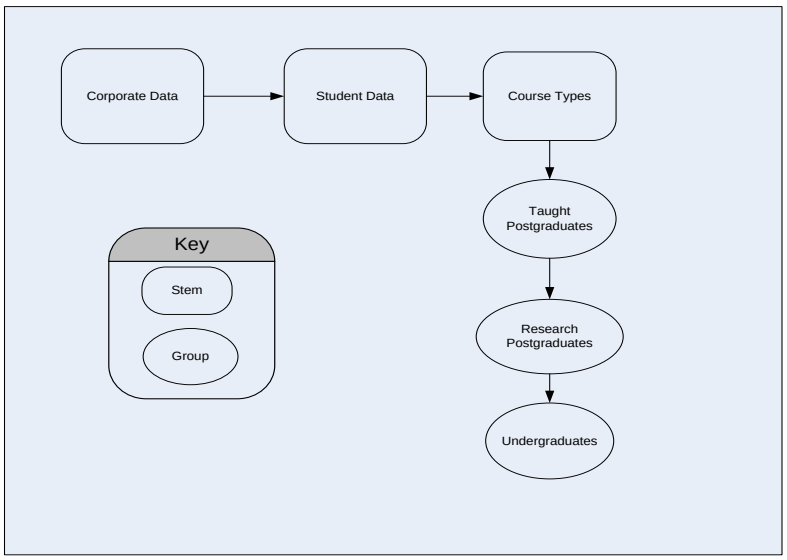

Figure 1: Loaded student groups

As discussed "Full Access" to the wireless network is to be provided to all members of staff and also "Research Postgraduates". With the already available roll up group for Newcastle University within the organisational structure, and with the newly created "Research Postgraduates" group, it will be possible to assign "Full Access" to these user types. As for students who are enrolled on undergraduate and taught postgraduate courses, they can be assigned "Part Access" by making use of the respective groups which have been created using the corporate data. The diagram below provides an overview of the structure that the access groups would take.

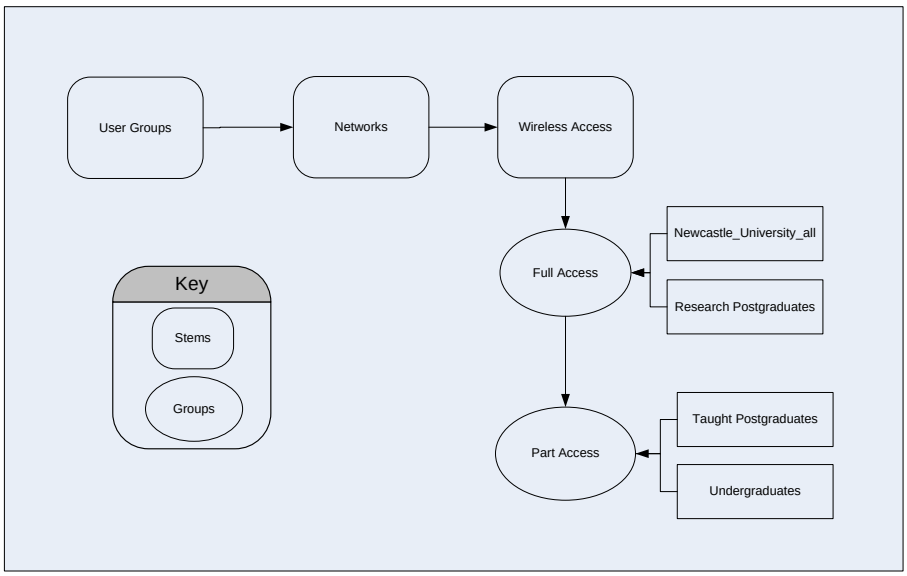

Figure 2: Wireless Access groups

The administration that would be involved with regards to managing the memberships to these groups would be minimal due to the use of source groups from the corporate data stem.

Subsequently the network administrators are assured that the respective access lists are as accurate as possible by making use of corporate data records. The issue of black listing was discussed with the network team with regards to being able to disable a user's access to the wireless access. Grouper allows for group maths to be applied to the access groups, which can be utilised when assigning membership on a group to group basis as above. It would be possible to define that all members of ISS can access a particular resource, except for Joe Bloggs. As part of this use case the use of group maths will not be necessary, as the process makes use of the active directory, any users who were to be blacklisted, would be so at the active directory level, their account would be de-activated subsequently disabling any access to ISS systems or services.

Initial Conclusions

The discussed approach to delegating access to the wireless network should provide an effective method of ensuring that users are provided with the correct level of access to the wireless network. The high level grouping of users means that the level of granularity required is at a manageable level for the use cases purposes. The creation of the custom access groups does allow flexibility to introduce new levels of access if required.

The provisioning of Grouper groups into the Active Directory has always been on the roadmap for the project team in broadening Groupers uses. This use case will provide an opportunity to test the links between Grouper and the Active Directory, and provide a proof of concept for other possible scenarios which could make use of Grouper to manage access groups.