Jisc

E-infrastructures: access and security

In many fields – from astronomy and medicine to linguistics – new knowledge is increasingly being discovered by researchers (and sometimes commercial partners) collaborating to gather, process and analyse large collections of data[1].

The combinations of computers, networks, software and support required to enable this type of work are referred to as "e-infrastructures".

E-infrastructures are collaborative, not centralised. They support users from many different organisations; many involve computers and datasets under different management as well. Making even a simple e-infrastructure work smoothly requires coordination among many parties. This has been achieved within a number of different research disciplines. There is now an ambition to connect and extend national and international "ecosystems" to let researchers in any subject access the appropriate e-infrastructure resources for the type and stage of research they are doing. This would facilitate cross-discipline research, make general-purpose infrastructures available to new domains and new researchers, and make more efficient use of infrastructure facilities.

Although researchers in different disciplines have many common requirements there are some significant differences in the functions and security features they need. Systems designed to handle medical data are unlikely to be suitable for astronomy, and vice versa. Even where requirements are the same, different infrastructures may deliver them in different ways. Working out how to share infrastructure components, and when not to, is a key challenge.

Collaborative infrastructures also bring significant benefits. Duties can be allocated to the organisations best able to deliver them accurately: data owners can classify their information; infrastructure operators can ensure appropriate physical and digital security; users' home organisations can hold them to account for any misbehaviour. Indeed many will already be doing this for their own purposes. Identifying common approaches lets this federated approach deliver efficient and accurate implementation of policies.

At the request of the UK Research Councils, Jisc has established a working group of e-infrastructure providers and specialists to review access management and security. These are areas that all e-infrastructures need to consider, where coordinated approaches could have particular benefits.

[1]

1 rcuk.ac.uk/research/xrcprogrammes/otherprogs/einfrastructure/

For example:

- Documenting current approaches should help new infrastructures and services identify opportunities to reuse existing good practice
- Recognising common requirements can help existing infrastructures make their services available to new researchers and subject areas
- Identifying common components could make more efficient use of scarce development and support resources
- Providing greater harmonisation of policies and other requirements will make it easier for both users and infrastructure components to comply with necessary restrictions

The working group has focussed on four specific aspects of e-infrastructures.

Authentication

Authentication is the process whereby a person demonstrates their association with a particular online account. Often this is done by issuing usernames and passwords: a pain both for infrastructure services that may be hundreds of miles from their users and for users who don't want to have to log in separately to each service. An increasing number of research and education services now rely instead on authentication provided by users' home organisations. This "federated authentication" greatly improves the experience for both users and services; services also benefit from an account managed by an organisation with a close connection to the user. New technologies are making federated authentication available to e-infrastructures, which could share these benefits.

[Read more at http://bit.ly/jisc-eiwg-authentication]

Authorisation

Authorisation defines the actions that an authenticated user can perform. Unlike online services that define their own authorisation, e-infrastructures typically devolve this task to individuals who manage their co-workers' access to resources. The system through which these individuals create and manage groups and their access rights is therefore a key component. Current group management systems are often tied to particular e-infrastructures and authentication systems. Broadening the range of services available, so group definitions are portable across infrastructures and can include users authenticated in different ways, will be essential to achieve an e-infrastructure ecosystem.

[Read more at http://bit.ly/jisc-eiwg-authorisation]

Security

Security aims to ensure that users can access resources within their authorisation and that other people cannot. E-Infrastructures are challenging from a security perspective. Systems, users and potential attackers may be anywhere on the Internet: very different to traditional security models with an "inside" and an "outside". But e-infrastructures have many more layers than a simple network, and many more kinds of security controls that can be applied. Testing typical e-infrastructures against the Cyber-Security Council's Top 20 Controls indicates that appropriate security can be provided: the challenge is to choose which combination of the many available security components to use.

[Read more at http://bit.ly/jisc-eiwg-security]

Policy

Different components of an e-infrastructure often have their own policies. These include rules on how data or systems may be used, but also undertakings to other infrastructure components, for example on how problem reports will be handled. These will often be complementary: for example if a dataset may only be accessed by current staff and students then an undertaking by universities to provide accurate status information provides the best possible implementation of that policy. Where these policy matches are likely, common policy statements make it easier for infrastructures to have their policies enforced.

[Read more at http://bit.ly/jisc-eiwg-policy]