ISC11D010

Title:	**Systems team service vision 2011-16**
Author:	Jon Woodley
Date:	14 October 2011
Circulation:	ISSC – 10 November 2011
Agenda:	ISC11A001
Version:	Draft v0.1
Status:	Open

Issue

To receive a draft of the service vision for the ICT Systems team.

Recommendation

The committee is asked to note the report.

Resource Implications

The creation of the vision itself has no resource implications, but implementations of recommendations contained in it may have resource implications.

Risk Implications

Not applicable

Equality and Diversity

Not applicable

Timing of decisions

Not applicable

Further Information

Iain Reeman, ICT Systems Director. Extension 2926. Email: i.reeman@uea.ac.uk

Background

This vision will contribute to the work being done on an IT strategy for the University.

Discussion

Systems Team
Service Vision 2011-16

Overall

The authentication, email, storage and certificate services provided by ISD for the university are intended to keep pace with, compliment and facilitate the University's corporate plan, Faculty Strategic plans and the ISD strategy. Where appropriate references are given in square brackets to the lines in the Systems Team: Service > Product > Component Map.

The systems team provide the following services (listed with a sample of products):

- Data storage – Backup and personal document storage
- Digital certificates – internal and external
- UEA Email Service – Staff and Researchers Email
- UEA authentication service – client authentication

We also provide the following product elements of these services:

- Server hosting:
    - Physical servers
    - Virtual servers
    - System monitoring
    - Infrastructure Database servers
- Desktop and development support
    - Operating System Deployment
    - Operating System Management
- Application deployment
    - Deployment servers

Data storage

Data storage is a key service that ISD provides and the current plan is for this to remain locally hosted, though options for cloud hosting of certain data should be explored. Growth in research storage is predicted to be substantial; the expectation from the UEA research community being that around 10PB of data is likely to require storage in the next 5 years, moving forward we need to undertake further work to ensure that appropriate costs for storage are recovered via research grants and the work on research Data Management Plans will assist with this by allowing us to gain a better understanding of the upfront requirements for research data storage. The issue of what to do with legacy research data, much of which is stored locally and insecurely needs further thought (this issue was raised in the 7Safe Security Audit). Further to this personal file store quotas are likely to increase further in line with user expectations and file sizes. Work needs to be undertaken on records management and this may help to contain growth in file store requirements, nonetheless changes in technology, the way we teach and opportunities for research all indicate that the requirement for storage will continue to increase.

It is therefore important that investment in this area is not only maintained but substantially increased in order that replacement cycles and increases in storage requirements can be met. Current funding will not be substantial enough in the coming years if growth is as predicted and personal file store quotas, when reviewed bi-annually, continue to increase. To address some of the impact of this we are actively investigating a number of storage technologies. Fast Fibre Channel (FC) based disk is currently used, at considerable cost per TB, to provide storage to highly utilised systems such as databases. It is now possible to achieve equivalent performance now with Serial Attached SCSI (SAS) based disk, when hosted as we do behind a SAN Volume Controller (SVC), at around half the cost. We will be looking to migrate from FC to SAS [DAT-19] as part of our usual replacement cycle and

future expansion from 2011/12 onwards. This is in line with the storage industries expectation that SAS disk is likely to supersede FC in the next 5 years. To reduce both disk space and backup requirements we will be investigating the use of both inline compression appliances and de-duplication technologies [DAT-1] with a view to possible implementation if appropriate in 2012/13. In the area of backup we will need to review our current approach to backup [DAT-5]. As our storage requirements increase so too does the length of time for backup and as a result the window for backup schedules is relatively small, in order that performance is not impacted, but as storage levels increase it is difficult to keep backup confined to those defined periods. A number of new approaches are emerging that potentially reduce both backup and more importantly recovery time by using incremental forever backups. There are downsides to such technologies as many use disk as the backup media rather than the traditional and relatively cheap media of tapes which can escalate initial costs. Further investigation in 2011/12 including a proof of concept and return on investment exercise will be required before a firm commitment can be made. The two tape libraries that currently support the backup process have recently been enhanced to vault (mirror copy) data between the libraries in each data centre. 2011/12 will see this process completed [DAT-6] removing our requirement for fire-safes and manual tape movements across campus. The tape library in Data Centre 2 will now act as the offsite DR location with an addition tape drive being added to increase capacity. To reduce costs in this area we will be extending the life cycle of the tape frames, used to store tapes in the libraries, from 5 to 10 years. 2012/13 will see an upgrade to the Data Centre 1 library to increase capacity by replacing legacy tape drives that are no longer in use. Further drive upgrades, to remove legacy tape drive, will be applied to the Data Centre 2 library in 2013/14.

Our current personal file store system is configured primarily to support Windows desktops despite both Linux and Mac OSX being able to access it, during 2011/12 this will be restructured [DAT-7] to support all desktop systems, remove a number of legacy items and to allow for greater growth in quotas. The existing structure has been in place for over a decade and served the university well but as requirements have changed this structure has failed to keep pace. Once completed a common area across desktops will be available for documents and other data users frequently access whilst allowing researcher quotas to grow above the current ceiling of 50GB per user. Archiving has been a long term goal for ISD which has been difficult to achieve with the technologies available. Although a pilot was established we have never been able to establish a product that was sufficiently user-friendly. In 2011/12 we will be working with our current storage partner Tectrade on how we take this forward to service in 2012/13 [DAT-14].

A number of developing trends are emerging in storage that are likely to affect our SAN infrastructure over the coming years. Currently our infrastructure is based around enterprise class storage designed to run 24/7 all year round with reduced failure rates. A number of vendors are developing solutions based around commodity storage (usually used in consumer technology such as USB hard-drives, easily attainable but not necessarily as reliable) in order to reduce the cost of implementation. This may be appropriate in some areas such as Research Computing [DAT-15 -18] but could potentially increase TCO with disks requiring replacement on a more frequent basis. In conjunction with this ATA over Ethernet (AoE) is rapidly gathering pace with lab testing indicating that Fibre Channel like performance is theoretically possible. However routing of the traffic is not possible and security mechanisms are limited. As such any potential implementation is likely to be limited and would need to be planned with these limitations in mind. Solid state storage (SSD) is gathering pace but reliability and cost is still an issue at present but as the technology develops these issues are reducing. It does however provide a number of advantages for fast caching of regularly accessed content to enhance performance when implemented as part of an SVC implementation. The 2013/14 replacement of SVC will see us investigate the feasibility of implementing SSD to this end. As things stand at present implementation more widely is unlikely [DAT-1 and 2].

Digital certificates

A digital certificate's main purpose is to ensure that data, servers or web sites are authentic and that you know who has created or provided it and that it hasn't been altered in any way since it was created. In many cases certificates can also provide a mechanism for secure communication. ISD provide digital certificates for both internal and externally facing services and products. The externally facing service and products, such as the library system Aleph and Email Web Access, have been using the JANet funded Certificate Service for a number of years. The service has developed significantly since inception but still lacks some flexibility in terms of certificate duration and alternative

server names. 2011/12 will see the suitability of the service reviewed [CER-2]. Our internally hosted digital certificate product is primarily geared to ensuring that internal traffic between systems is encrypted where possible particularly with UEA authentication. 2012/13 sees an upgrade to Windows Server 2008 R2, to keep pace with changing requirements, and a review of certificate life-cycles based on that of a system or service [CER-2].

UEA Email Service

2010/11 saw significant changes to the UEA Email Service for students with the migration to a locally hosted Exchange 2007 solution. This greatly enhanced the student experience and provided them with a considerable quota increase to 500MB and access to email via mobile devices for the first time. In 2011/12 we will be enhancing this further with an upgrade to Exchange 2010 [EML-5] allowing student access to the full web client, currently only available when using Windows Internet Explorer, on a number of other supported browsers. Staff will also be migrated to Exchange 2010 but will be given a 5 fold quota increase to 1GB [EML-1]. Whilst increasing staff quotas we are also able to half the cost of the associated storage once migrated is completed as Exchange 2010 enables the use of the less expensive SATA rather than the more expensive Fibre Channel based disk on the SAN. Prior to this Postgraduate Researchers and any remaining staff will be migrated to the existing Staff and Researchers Exchange solution. Costs will be further reduced once completed as we will be reviewing the life cycle of email hardware extending it from 3 to 5 years. To increase the security of the email service both of the insecure protocols POP and IMAP will be removed from service. All access to email will then be provided by either clients supporting MAPI, Outlook Web Access or mobile devices supporting Active Sync. Staff mobile devices using the service will also have security enhanced with security policies being applied that enforce PIN access to the devices [EML-4]. In tandem consideration should be given to applying the same policy to student devices using the service if it is felt to be appropriate [EML-6].

Prior to the next hardware replacement cycle in 2016/17 the possibility and viability of outsourcing email services to the cloud should be evaluated for both staff and students [EML-1 and 5]. Although a number of universities have already undertaken this we are aware of at least one that is currently evaluating bringing the service back in-house due to login issues which in turn have become their number one IT Helpdesk issue. Serious consideration must also be made around service level agreements for DR recovery, the issue of where data is held and if it is subject to Safe Harbour framework and the impact on the network if the funding model for JANet changes.

Email archiving has been running in pilot with ITCS and ISD for the last twelve months. In 2011/12 we will be working with the vendor Quest Software to determine how we can proceed with regard to FOI compliance [EML-2]. Until this can be achieved progress is likely to be slow but it is hoped that we will expand the pilot during this period with a view to campus wide rollout towards the end of the academic year. In 2012/13 we intend, dependent on FOI progress, to further enhance archiving with the importing of PST or personal archive files.

2010/11 saw a marked increase in phishing attacks at UEA which in turn caused us to be black-listed by a number of internet mail and service providers. 2011/12 will see the implementation of rate-limiting for email to further improve our defences against being blacklisted [EML-8]. Once enabled mail accounts will only be able to send a yet to be determined number of messages before being blocked from doing so. Exceptions will be registered for bulk-senders who will be contacted prior to implementation. One other area that phishing and SPAM has targeted has been our email mailing lists. Mailing lists at UEA have been provided by a number of methods over the last 10 years with each having its drawbacks. To reduce phishing, SPAM, support costs and management overhead 2010/11 saw the start of the initial work to migrate to Exchange based lists managed by the UEA Identity Management System. 2011/12 will see this work completed and the decommissioning of the older services [EML-10]. Once completed lists will have defined senders helping to reduce unwanted emails. Email routing will also be simplified once all email is hosted on the Exchange based solution enhancing user provisioning by reducing the time between request and creation [EML-9].

UEA authentication service

The UEA authentication service is the core dependency for providing the secure authentication mechanism for clients and services across the university. Built on Microsoft Active Directory and Network Policy Server for remote access services, such as EduRoam and VPN, it is essential that this service maintained and enhanced where necessary. In 2011/12 we will be looking to simplify and flatten the existing Organisational Unit hierarchy in Active Directory [ATH-1]. The current structures, put in place when the university faculty model was implemented, helped the various IT support teams around campus support their users. The downside to this approach is that users when moving between departments or schools can often have issues logging into services such as the Portal. Flattening the structure that these accounts occupy will greatly reduce this issue, improve the user experience and reduce complexities in user provisioning. 2011/12 will see the need to upgrade Linux and Mac OSX clients to version 4 of Quest Authentication Services to maintain support and compatibility [ATH-2]. An audit of existing installations will be undertaken to assist with this process and we will work with IT support where necessary to ensure that this process is as smooth as possible. A number of systems and services depend on LDAP for authentication; unfortunately many have been configured to connect anonymously which presents a security risk to our infrastructure. Bearing this in mind during 2011/12 we will be working to reduce the use of anonymous LDAP [ATH-4] where supported and encouraging the use of Quest Authentication Services on Linux systems to secure LDAP traffic. We are taking the medium to long-term view that we will disable anonymous authentication to mitigate the risk completely but this must be weighed against functionality of other services. 2011/12 will see the RADIUS proxy services, which provide support to the Remote Access and Wireless Network services, being migrated to the new Exchange client access servers [ATH-5] with which they share resources. In 2012/13 the domain controller server hardware is due for replacement [ATH-1] at which point we will review the host Operating System. It is not clear at this stage if this will be Windows Server 2008 R2 or Windows 8 Server from Microsoft's road-map and as such a decision will need to be made nearer the time taking in consideration future requirements. To assist in reducing costs the existing profile servers, due for replacement in 2015/16, will be replaced with shares hosted on our NSeries filer appliance [ATH-3].

Server hosting

ISD has invested considerably in standardising on HP server hardware in particular blade servers. This has helped to simplify support and maintenance and reduce energy consumption. In order that we maintain reliability and remain within support criteria there is a need to ensure that this hardware is kept up to date. To reduce unplanned downtime we are proposing that preventative maintenance is undertaken 3-4 times a year at off-peak periods [SVR-1]. This frequency should ensure that any required downtime and therefore disruption is kept to a minimum. To reduce costs we will be reviewing the replacement cycle of blade enclosures in 2011/12 [SVR-3]; increasing the existing cycle from 5 to 10 years. HP have made a long term commitment to the current specification and the modular design of the enclosures means that replacement parts can be purchased at a cost substantially less than an entire enclosure. The savings in this area will allow us to further expand our blade infrastructure where required and investigate the possibility of upgrading the enclosure connection modules [SVR-4], used to connect storage and networking, to a converged connection module if appropriate. Storage and data networks continue to move to a convergence in technology but at present are very much separate at UEA. This could add considerable cost initially and as such must only be considered if the benefits are significant over the long term. Currently the more expensive connection modules, without convergence, are only used for virtualisation in order to control costs as this also impacts on the Networking Teams Campus Wired Connections service.

In the area of virtualisation we are adopting a strategy of replacing physical servers with a virtual server at the end of their life cycle where appropriate based on an earlier capacity planning exercise. This will assist in reducing operational costs and enable greater flexibility and agility when provisioning servers [SVR-6].

System monitoring is an essential part of our server hosting service; providing us with early warnings of potential system failures and service issues. In 2010/11 we started to review our existing monitoring product and took the view that it was no longer fit for purpose. We have now started to develop the replacement product based on Microsoft System Centre Operations Manager. During 2011/12 we will

be completing the migration of system monitoring [SVR-7] with the aim of providing customised views to support teams as per their requirements. In addition we will be able to provide information to end-users regarding service availability in real-time.

Desktop development and support

Operating System Deployment and Management are both provided to Desktop Services and IT Support by Microsoft System Centre Configuration Manager. The servers supporting this are due to for replacement in 2013/14 at which point we will consider if these servers are appropriate for virtualisation [DES-1 and 2]. In collaboration with Desktop Services we will also review the version of Configuration Manager and its appropriateness moving forward. 2011/12 will see the Microsoft Key Management Service server coming to the end of its lifecycle [DES-4]. Although currently used to activate Windows 7 clients Microsoft has been very clear that it will continue to use this technology in future versions of not only Windows but also Microsoft Office. As such this products importance will continue to grow. Future versions of both of these products could well adopt a subscription model and this may further extend the requirement to host such services locally. However with any potential move to web hosted applications this requirement may also diminish over the next 5 years.

Application deployment

As with Desktop development and support this service is supported by Microsoft System Centre Configuration Manager. Again in 2013/14 the servers supporting this will be due for replacement [APP-2]. Deployment methods will be severely impacted by how much vendors move applications to the cloud. Further to this Microsoft has shifted the emphasis of application delivery from the machine to the user with the next release of Configuration Manager. This is likely to impact how any replacement servers are specified. In 2015/16 the software share servers, used to provide installation packages to both Configuration Manager and applications deployed via Active Directory, are due for replacement [APP-1]. There is potential for savings to be made here if this requirement diminishes in the next 5 years but this is very much dependent on how distribution methods develop over this period.

Assumptions

In creating this 5 year vision document the following assumptions have been made:

Political

- That current tax (including VAT) levels will continue to apply
- No centrally applied academic standard contracts regarding the procurement of equipment or services are introduced
- No requirement to comply with central government Impact Level (IL) assessments (which are likely to be part of any membership of a PSN)
- Maintain university existing profile – does not have additional spotlight with respect to IT security alerts or contentious research
- No war or aggression regarding essential resource such as energy or raw materials (incorporating known demands such as China's continued draw of cable-grade copper in building and construction)

Economic

- Exchange rates relatively stable
- External suppliers remain in business or are in keeping with existing contracts if firms are taken over by rivals
- Perceived value for money from HE funding is maintained
- Ranking of the university and the relative impact on recruitment of students/attracting research funding is maintained.

Socio/cultral

- Student expectations are rising due to increased fees
- No diversions away from normal business focus
- No new medical or environmental incident will occur (ash cloud, flu pandemic, localised flooding) which will incur a rapid change in delivery model or capacities

Technological

- Credibility of HEI technical implementations is maintained
- Existing hardware and software solutions are not irreversibly compromised by being found to have an security flaw (e.g. Playstation network) or patent infringement (e.g. Forgent Networks over the JPG standard in 2002)

Legal

- No change in EU contract legislation
- EU/US Safe harbour framework continues to be relevant
- FOI legislation is maintained as is at present

Environmental

- Environmental impact is still permitted to be defined as part of, not the major factor, with respect to procurement