# Active Directory Consolidation and Future Governance

## Project Leaders – Bruce Campbell, Erick Engelke

## Report – April 8, 2010~~April 6, 2010~~

### Background

The report of the Information Technology Task Force (Appendix A) recommends consolidation, to the maximum extent possible, of Active Directory forests and domains. The memorandum from the Associate Provost for Information Technology (APIST), Alan George, on Active Directory Consolidation and Future Governance (Appendix B) defines the project to implement the task force recommendation; to define an endpoint active directory design, "how we get there", and a governance model.

This report delivers recommendations on:

- Active directory architecture
- Operations
- Governance

We believe agreement in principle is needed on key recommendations before moving further; specifically agreement is needed on the architecture, before defining how we get there.

### Approach

The project leaders sought written input from CTSC members (Appendix C), and met with representatives from eight campus IT groups.

### Scope

All active directories to support teaching and administration, within faculties, schools, academic support departments, and ancillary departments.

# Recommendations

## Architecture

While there are two major domains currently (ADS and NEXUS), each is managed as a single domain design; i.e., both domains individually have all students, staff, and faculty. A single domain model is the simplest conceptually and technically, and is the basis to which other candidate models were compared.

After review of requirements for service delivery, and consultation with campus IT groups, and based on 9 years of experience with single domain models (Appendix D), we recommend the two existing domains be merged, and retain a single domain model. Departmental and other active directories within the scope of this project should be phased out, with the new campus active directory providing the services required. Appendix D provides additional background and motivation for the recommendation. It also provides sufficient technical detail about the proposed structure to allow campus IT staff to review for operational, support, and security implications.

> **Recommendation 1 – Nexus and ADS should be merged, and the architecture of the new campus active directory should be a single domain model. Departmental and other active directories within the scope of the project should be phased out, with the new campus active directory providing the services required.**

## Governance

The memorandum from the APIST, Alan George, on active directory consolidation and future governance defines a governance model as follows:

> ### *AD Management Committee*
>
> *This committee would be charged with the day to day administration of the AD. Given the genesis of NEXUS and ADS, it is proposed that the membership be:*
>
> - *One representative from Engineering and one from IST*
> - *One representative from each of two faculties other than Engineering, rotating, for two year terms*
> - *Additional resource people as required*
>
> *The management committee would be co-chaired by the representatives from Engineering and IST.*

Some additional documentation is required (e.g., terms of reference), initial committee members chosen, and committee resources setup (e.g., e-mail list, collaboration space).

> **Recommendation 2 – The AD Management Committee should be created, and terms of reference developed. The new committee co-chairs can be tasked with requesting additional resources, scheduling meetings, etc.**

## Operations

ADS is managed by IST, and NEXUS is managed by Engineering Computing. The consolidated active directory will require technical infrastructure, operational management thereof, and ongoing budget for upgrades, maintenance, etc.

> **Recommendation 3 – IST should be responsible for operational management of the core infrastructure for the consolidated active directory. That is, acquisition, hosting, configuration, administration, monitoring, debugging, 7x24 support, disaster recovery, etc., on the set of active directory core servers (e.g., DCs). Engineering Computing will assist with the monitoring and debugging of the directory controllers.**

## Other

Implementation of Recommendation 1 can be accomplished in several ways, including merging to an existing AD, or creation of a completely new AD and migrating all computers/users to that. There are significant technical and non technical factors to consider. An early decision on whether to create a brand new directory, or merge to an existing directory, is needed.

> **Recommendation 4 – The APIST should, after whatever consultation and information gathering he deems reasonable, make a decision on whether to create a new directory, or merge to an existing directory.**

# Summary

The proposed system is based on nine years of experience in both ADS and Nexus, and on education regarding changes in Windows Directory Services 2008 R2.

A good AD design is a simple one and it should reflect the structure of the organization as best possible in the tree-based confines of the technology.

New services, such as databases, desktop video conferencing, software deployment, SharePoint, MS Office Communications Server, Certificate Services and others will increasing use the AD and will benefit from our current efforts to make a well designed, shared, secure AD structure.

# Appendix A – Report of the Information Technology Task Force

The full Report of the Information Technology Task Force is available at http://provost.uwaterloo.ca/Memos/IT TASK FORCE REPORT June 2009.pdf

The section covering Active Directory is as follows:

- *Active Directory*

*There are two major active directory forests used at UW - ADS and NEXUS. ADS is the IST authentication domain used to access QUEST, and to log on to academic support computers. ADS is also used by many corporate resources and provides a single source for account maintenance in the University. NEXUS is managed by the Engineering computing group, and provides the major network for student labs. Separate passwords are needed for those using both systems.*

*Given that there are twice as many NEXUS workstations - 4,000 - as ADS units, and that NEXUS is used in most student labs across campus, rationalization of the services could be achieved by folding ADS into NEXUS, with Engineering and IST computing staff collaborating in managing the system for the University as a whole.*

*Recommendation 2: The University should consolidate, to the maximum extent possible, Active Directory forests and domains, with a preference to move to NEXUS, if feasible.*

# Appendix B – Memorandum Alan George, November 13, 2009

## Active Directory Consolidation and Future Governance

Currently there are two major instances of Active Directory (AD) at UW, along with numerous instances involving smaller constituencies. By far the largest is NEXUS, managed largely by the Faculty of Engineering. The next largest AD is ADS, managed by IST. Having two major ADs and a (growing) number of smaller ones leads to inefficiencies and single points of failure, and prompted the UW IT Task Force to recommend their consolidation. This note is to suggest a way forward in implementing this recommendation.

There are two essential elements to this undertaking. One is to strike a project to sort out what the "endpoint" should be, and how we get there from where we are now. The second is to establish a "governance structure" for the long term. The AD will need day-to-day administration and adjustment and, from time to time, policy issues on its administration will need to be addressed.

### Governance

#### AD Management Committee

This committee would be charged with the day to day administration of the AD. Given the genesis of NEXUS and ADS, it is proposed that the membership be:

- One representative from Engineering and one from IST
- One representative from each of two faculties other than Engineering, rotating, for two year terms
- Additional resource people as required

The management committee would be co-chaired by the representatives from Engineering and IST.

#### UCIST

The AD management committee would make regular reports to CTSC on the operation of the AD and seek its advice and direction on technical matters. Through the CTSC the committee would refer policy issues to UCIST, which provides advice to the Associate Provost, IST. The AD management committee may also seek UCIST's advice directly as appropriate.

### Consolidation Project

It is likely that the architectures of the NEXUS, ADS and other directories differ, and are administered/managed in different ways. Thus, the creation of a single AD to replace them may involve a certain amount of "re-architecting". The main burden of this project will be to identify an ideal architecture for the new AD, and identify best practices for its management and evolution in the future.

It is proposed that Bruce Campbell (IST) and Erick Engelke (Engineering) serve as co-leaders of this project and, for continuity, also serve as inaugural co-chairs of the AD Management Committee.

## Appendix C – e-mail to CTSC seeking written submissions

Sent: Monday, November 30, 2009 11:43 AM

To: ctsc@lists.uwaterloo.ca

A subcommittee of the CTSC has been struck to determine the best route for campus Active Directory consolidation and governance.

The committee will look at what is our desired "endpoint" and how we plan to get there.

Many people across campus have experience maintaining their computers inside one of the campus directories, or outside, or both.

Furthermore, the active directory will impact campus systems which depend on it for authentication, authorization, attributes and relationships. These include WatIAM, the financial systems, HR systems, Email systems, Quest, ACE, etc.

Our first challenge is to collect descriptions of campus needs which will help the committee describe a desired endpoint.

We are inviting written submissions from anyone on campus who wishes to help influence the design. Topics might include:

- software distribution
- two factor authentication
- issues related to campus databases
- security issues
- management issues
- account generation
- etc.

Submissions will be accepted up to January 15th, 2010. The committee would also be happy to meet those who have made written submissions.

After the submissions and interviews identify key issues, the committee will use the acquired data as a starting point for discussions about the desired Active Directory.

The committee will report to CTSC, UCIST, and the Associate Provost for Information Technology.

Bruce Campbell
Director, Network Services
Information Systems and Technology

Erick Engelke
Director
Engineering Computing

# Appendix D - Proposed Active Directory Architecture

## Forest, Domains and Trusts

The proposed active directory will consist of a single domain inside an empty forest comprised of it and the root domain.

The domain will not have any external two-way trusts as they present security risks.

One way explicit trusts may be established by an external domain, as has been the case with ADS and the IST-managed Exchange Email domain.

UW has reliable high speed links to its Canadian campuses, so the AD structure will be single site.

The decision to use a single domain was struck because the user communities of faculty, staff, grad students and students all have shared access to shared resources (data files, databases, printers, some computers, etc.) and any attempt to segregate them creates unnatural boundaries. Active Directory and Windows are quite secure; both ADS and Nexus already have student accounts and yet offer strong security as we use a range of tools and procedures to enhance the security.

Furthermore, the simplest design will offer compatibility with the widest range of 3rd party products we may wish to acquire, such as a handheld computing infrastructure, video conferencing, etc.

## Domain Structure Overview

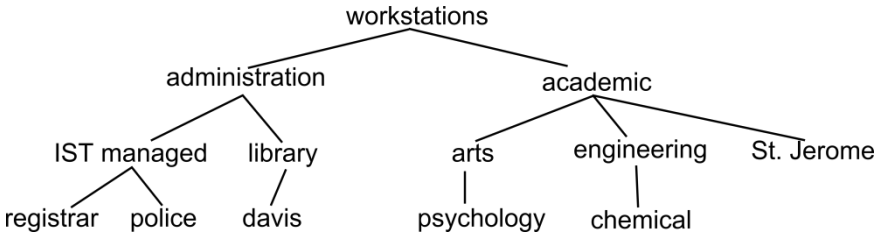
There will be several important 'OrganizationalUnits' added to the root level of the directory:

- ou=Workstations will contain an OU tree of workstations
- ou=People will contain an OU tree of user accounts
- ou=Servers will contain an OU tree of domain member servers
- ou=Domain Controllers will contain the domain controllers
- ou=Groups will contain user groups

In each case, except for the domain controllers, the OU tree will follow a hierarchy representing the organizational structure of the university.

## Workstations Sub-tree

In the administration branch of the workstations tree, most groups have workstations managed by IST, they will be under the IST managed branch. However, some groups, such as the library and housing, have their own IT staff and will largely manage their own portion of the directory tree with some autonomy.




The faculties and the affiliated universities (formerly known as church colleges) will also manage their own portions of the tree. In the case of Engineering, there will be a substructure recognizing the departments; other faculties will make their own decisions regarding their substructures.

All OU's containing publicly accessible workstations (student labs, podiums, kiosks, etc.) will be located under an "ou=public access" part of the tree in the respective jurisdiction. This designation will be used to help monitor and manage these special workstations.

The workstations OU tree determines software delivery by group policy objects (GPOs), which are usually inherited from parent to child OU. The design of this tree allows many important software decisions to be administered at the third level in the tree, such as at the faculty, library or IST managed level.

Of course, software will also be assigned deeper in the tree, but most faculties have made some decisions on software they wish to be available on all their workstations, as with the library.

Software will not normally be assigned at the ou=workstations, ou=academic or ou=administration levels except in the case of special "common apps" GPOs decided by the governing committee. An example would be the UW Emerge utility which pops up warnings in the event of an emergency.

The workstations OU subtree will include all types of clients: Macintosh, Linux, laptops, etc.

## Servers Subtree

The Servers OU subtree will be similar to the workstations tree, and server management will follow logically from the tree. Systems administrators will be delegated authority for their portion of the servers subtree.

## People Subtree

The People OU subtree will also be similar, except it will not have the IST Management umbrella.

The People OU subtree will be entirely administered by WatIAM, which will manage the entire life cycle of user accounts. No user account changes will be made by system administrators directly; their requests will pass through WatIAM.

APIs will be defined and examples given to allow some automation of WatIAM requests from constituency servers, allowing for assignment of home directories, profile locations, etc. Special considerations for Unix are listed later.

WatIAM will also move users to new locations in the AD tree as appropriate, such as when a grad student becomes a faculty member, and new group memberships will be applied automatically.

The sole exception to the WatIAM rule is that the domain top level administrator accounts will not be managed that way.

All people will have their UWuserids in the people tree. Some people will also have an elevated account denoted with an exclamation point and called a bang account (eg., !bjhicks pronounced bang bjhicks). The elevated account will be used in situations where the elevated account has some special privileges and the normal account should not be used.

For example, the bang account would, in some cases, be granted some power user status on workstations. Or in the case of a database, the bang account may have the ability to enact some powerful data operations, such as database administrator, or the ability to change pay. This is how we will offer a two password solution with one domain.

The elevation of privileges depends on the application and the user. For example, all employees will use human resource's web pages, but only certain HR staff would have the ability to change pay, and thus require an elevated account on that system. People will have elevated accounts if they deal with information which is restricted or highly restricted in the university's Policy 8.

To offer real security for elevated accounts, we must look to two factor authentication where the user provides two pieces of evidence to verify his or her identity. Often these solutions involve a password and a smart device. Additionally, we would hope IP subnets can be used to limit access to sensitive accounts for given databases as it is unlikely a hacker would pass two factor authentication and be in the designated subnet.

Windows Directory Services 2008 R2 has Authentication Mechanism Assurance which enables special group memberships for the duration of the session if the user logs in with a smart card or token device.

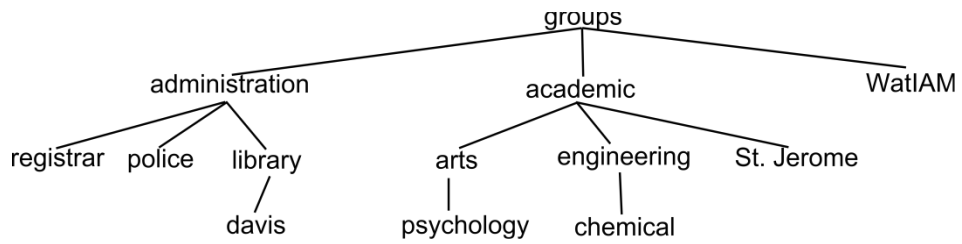
It should be noted that domain account passwords must never be shared. Much like passports, they will uniquely identify the person, not the access to data. If people wish to share data, there are a variety of technical solutions (eg., forwarding to share mail, sharepoint or fileshares to share data, etc.).

A correct userid/password pair will be sufficient to indicate approval, or the equivalent of a signature. This is already true on the GAP system, sharepoint, OFIS, and a variety of existing systems. Future systems will further entrench this point including Microsoft Certificate Services.

Since UWuserid and domain passwords will grant access for medium to high security data, the proposed NetID for wireless access will make sense for the lower security password to be used for wireless logins, and possibly other situations.

## Groups Subtree

The groups subtree will resemble the people subtree but also have a WatIAM branch for WatIAM managed groups




WatIAM will maintain lists of faculty, staff, grad students, students, etc. Also, many situations arise where course enrollment dictates access to computer or data resources. WatIAM will maintain course groups with membership extended to all students of the course.

The rest of the tree will have delegated access to system administrators for each appropriate OU; they will be able to create and manage groups without assistance..

Groups are extremely useful and we encourage their adaptation for any situation where a list of people is to be maintained.

## Naming Convention

A naming convention will be needed for groups, printers and GPOs to reduce confusion in a big AD. This will be an early task of the governing committee.

## Unix Considerations

The campus has a significant investment in Unix technologies. All modern Unix versions support using domain controller technologies (LDAP, Kerberos) for externalized authentication and storing user attributes and can be integrated into our domain.

We should be relying on the Active Directory for externalized authentication, rather than old style Unix password files which can be hacked on the workstations and servers. The AD will be configured to perform account lockout after a number of failed attempts, almost eliminating the ability to expose password hashes that hackers could try to crack.

Some faculties require Unix information (home directory, UIDs , GIDs , etc.) to be stored in the Active Directory using schema extensions defined in the Internet Standard RFC 2307. This presents a challenge, because users can have different UIDs, GIDs, and home directory paths for every IT jurisdiction, but each of these attributes can only have one value in the AD.

There are a few possible solutions:

- RFC 2307 uses LDAP servers to replace typical Unix mechanisms such as NIS and password files. It is possible to leverage AD to support authentication through mechanisms like PAM while relying on the password file for local particulars like UID, GID, home directory information.
- Many Unix systems permit local configuration allowing us to create customized LDAP attributes in the AD person schema, so there could be one GUI attribute for Computer Science, one for the other Math faculty systems, etc.

- It is possible to use a virtual LDAP server which acts between the client machines and the AD. It would offer *pass through* for authentication and most attributes, but return locally relevant data for UIDs, GIDs, etc. It could be combined with the above-mentioned customized schema to set a local value such as UID based on the AD returned value for the given IT jurisdiction. This would support local values, but avoid having a local database; all the data would reside in the campus AD.

The virtual LDAP server is the preferred solution.

A virtualized solution also exists for Macintoshes. They can be supported with Apple's OpenDirectory, where the userid and passwords are checked with Kerberos to the Active Directory, but some other information is returned from the OpenDirectory storage. We would need OpenDirectory servers for each computing jurisdiction with Macintoshes.

Further investigation regarding virtualized directories should find a capable solution for other Unix systems.

## Notes on Infrastructure

The campus supports multiple operating system platforms; however, we recognized the overwhelming majority of clients are Windows based computers, and Microsoft Office is popular on both PCs and Macs.

Many of our present servers are based on Unix. In some cases it is preferable to use Microsoft solutions due to their integration with the client and with Active Directory. SharePoint, Microsoft Domain Name Service, Systems Center and Microsoft Certificate Services are some examples.

While we expect Unix to play a continuing role in our server environment, Active Directory itself has shown Microsoft servers can be used to deliver powerful and reliable services with great benefits for the Windows client.

## Software Delivery

Automated software delivery is one of the benefits of a well managed Active Directory. Distribution will be accomplished using GPOs and tools such as Microsoft System Center.

For software intended for certain offices, labs, etc., the software will typically be assigned to workstations (not to users).

Niche packages, like PhotoShop, will be available for automated installs after user-initiated requests. In most cases, it will no longer be necessary to visit the CHIP to acquire software, or for the user to make installation-related decisions. This will reduce support headaches and user frustration installing software.

Whenever possible, we recommend the use of GPO transforms rather than re-bundling software.

System Center offers many advantages for software delivery, including timed rollouts so software is delivered at a desired time rather than at boot time. Several departments are presently investigating Systems Center.

## Common Applications

There are several challenges for the common applications, ones which are best decided by a campus committee. These include:

- coming up with list of common apps for campus
- time-table for updating flash, firefox, etc.
- determine whether to separate the various apps from a single GPO to several
- test groups for pushing updated apps before general distribution

Our efforts to time software rollouts will not be perfect; we often wait for vendors to release long-promised updates or fixes.

## Workstations

Workstations are grouped into OUs depending on their department, then further organization such as offices, research labs, etc., and still further to software deployment groupings.

Users would log in with their usual unprivileged UWuserid and domain password.

When desirable, single bang accounts tied to particular workstations can be used to grant power user status to those office users who need the privileges for their jobs.

The principle of least privilege reduces the likelihood of malware on the workstation. With Windows 7 this practice is simpler than ever.

While all users will have userids in the domain, Windows access control lists can be used to grant login permissions only to typical users of office systems and their supporting IT staff. This would prevent unauthorized access from other types of users, such as students if they were to gain physical access to an office computer.

## Documentation

The active directory system described here will be larger than any previous AD, and there will be more people involved in its management than before.

Clear, current documentation will be necessary for users and especially for administrators. The AD governance committee is charged with addressing this need.

## Security

The domain controller servers are the guardians of secret passwords and they grant access to privileged data and services. Thus the domain controllers attract interest from hackers wishing to gain access or to impede our operations.

There are steps we normally take to keep the DC's safe from hackers. Many of them are to reduce the attack surface of the DCs.

- firewall network access to only on-campus computers
- temporarily lock out accounts after several bad password attempts
- limit the number of exposed protocols to a minimum
- limit the amount of code running on the DC – server core
- log everything, and react to all unusual events automatically

However, there is only so much we can do. The DCs run software that speaks protocols, but software has bugs and protocols have weaknesses. Also, every computer in the domain must have network access to the DCs. We are necessarily vulnerable to attacks.

Some attacks came from outside the campus borders. A password attack on IMAP (Email) or password authenticated web pages becomes an attack on our domain controllers if the IMAP and web server use the domain for authentication. Many of these protocols should be limited to on-campus access, and a VPN to extend the protocols to campus members off-site. Public facing web pages can use reverse Turing tests such as CAPTCHAs to discern live users from botnet attacks. A campus portal could ask the CAPTCHA once for all the services available through it.

A CAPTCHA

A two domain model was also considered. In one scenario, the controllers' network access is limited only to subsets of the two major campus server rooms and be for secure apps (Sharepoint, HRMS, etc.). Limiting access to the server rooms prevents many attacks from campus workstations. Alternatively, the second domain could extend to staff workstations – increasing risk slightly to the DCs but reducing risk to those workstations from the student areas.

A second domain costs money to buy and administer. Having two domains will be frustrating for users as they will have accounts with different possible passwords, and will sometimes have to specify a domain by name.

This bifurcation of the campus into *trusted* and *untrustworthy* communities becomes increasingly difficult in practice. Faculty and most graduate students are employees of UW but are also academic and need access to servers and clients outside the areas normally administered by IST. They also constitute a significant proportion of the UW user space.

The possible benefits of a second domain do not appear to outweigh its costs and complexity. It is better to secure the campus systems from attack by design than to rely on isolated pockets of trustworthy computers outside our server rooms.

## Enterprise Applications

We must be wary of adopting software which increases the attack surface of the UW-facing DCs. For example, some powerful products wish to be installed directly on domain controllers or require 'enterprise', or 'domain' privileges to work. The risk exposed by adding programs to the domain controller must be carefully scrutinized.