Windows Enterprise Design
Enforced Conventions for User and Group Names

August 17, 2016

The Windows Enterprise Domain design" centers on the ability to use existing ISU NetIDs (from Project Acropolis) to login to Windows desktop systems. ISU faculty, staff, and students will have one common NetID and password combination to access a wide variety of computing resources available from Iowa State University (including Windows systems and resources). The ISU NetID will be the unique namespace for those accounts.

A process has been created to automatically populate Acropolis ISU NetIDs (and their associated passwords) into the Windows Enterprise Domain "Active Directory" environment. This process combined with the ability of Windows departmental IT OU managers to have full control of their departmental OU creates some problems. The main problem arises when a departmental OU manager creates Windows user accounts that later conflict with a NetIDs coming from an ISU NetID registration. This issue is resolved by:

- Establishing a Windows naming convention to eliminate future conflicts
- Ensuring that the ISU NetIDs ALWAYS win any conflicts

This solution is termed "Enforced Conventions" and is defined as follows:

1) OU managers are allowed full control of users/groups/computers in the OU they are delegated control to. This means a Windows departmental OU manager can add/delete/move such objects at will, using all the standard Windows tools available.

2) ISU NetIDs are populated down to the "iastate.edu" Windows domain via an automatic process from the Acropolis system. All newly created user accounts have the official college/dept code for the person used to place into the ISU college/ departmental OU structure ("iastate.edu/<collge>/<dept>") if that OU exists. If a college/departmental OU does not exist for the user the username is placed in the general "iastate.edu/Users" container. OU managers will NOT create accounts for departmental faculty, staff, and students but tell them (as most do now) to create the ISU NetID in Acropolis first.

3) Departmental OU admins requiring additional usernames should create a sponsored NetID via http://asw.iastate.edu (IT Administration/Manage Sponsored Net-IDs). These sponsored accounts have MyFiles storage, an Exchange mailbox, etc. and provisioned by all standard account provisioning processes.

4) In the past departmental OU admins could create special "Windows only" accounts via standard Windows methods within their departmental OU. These were commonly called "bang-accounts" (because the account username started with a "!"). THIS METHOD IS CURRENTLY BEING PHASED OUT AND ALL BANG-ACCOUNTS WILL BE DELETED AUGUST 3, 2015. A sponsored NetID is always recommended (see the previous section). See the following announcement:
http://www.tech.its.iastate.edu/windows/admin/Announce.2015.04.28.pdf

5) If a departmental IT OU admin violates the naming convention the departmental admin (and the user) will suffer. If an Acropolis NetID comes down from above it will look for an existing Windows username and find it wherever it lives in the Windows namespace. It will then synchronize the newly registered user's password with the account found in Active Directory, giving the new user access to all resources the existing user had. The existing user sees their password as "changed" (but does know the current password) and has lost access to their computing resources.

6) A regularly run process passes the OU tree and checks the Windows accounts contained within each OU. Until January 1, 2015 any which start with "!" were "don't cares" (they couldn't have come from Acropolis). However, after June 1, 2015 all bang-accounts should be converted to sponsored Net-IDs or removed. See the announcement at:
http://www.tech.its.iastate.edu/windows/admin/Announce.2015.04.28.pdf
Accounts that don't start with "!" are checked to make sure they exist as ISU NetIDs Email is sent to the departmental OU admins indicating the problem exists. In this way, the danger of having a username used for a long period of time (in violation of the convention) and then abruptly renamed one night (when the first Acropolis conflict comes down) will be minimized. This is just a "safety check" for the departmental OU admin who "forgets".

7) If a departmental OU admin abuses their Windows authority they will punish themselves (or the user will punish them). An example would be a long-term user created by Acropolis registration (not created manually by a departmental OU admin within their OU). One day the departmental OU admin decides to "delete" them (they have that authority). They are gone. The user cannot log in to Windows – but they can still login to Acropolis secure web-services (since that is where the ISU NetID originally came from and it is the "master" for all such accounts). They can change their password (via Acropolis secure web) and the account gets re-populated into the departmental OU via the standard automated process. The user thinks their problem is solved - but now the departmental OU admin has a NEW account (the security-ID – the "SID" - has changed). Now the departmental admins needs to recreate all the Access Control Lists (ACLs) before the user can get at their resources again.

8) The same naming standard used for usernames will apply to departmental groups that departmental OU admins create. The enforced naming convention is in the same way. For example, a departmental security group of lab managers might be called "!My Dept Lab Managers", with the "!" preceding the name to avoid conflicts with Acropolis groups being populated down into the Windows environment. Possible Acropolis groups that may be populated in the future would be departmental and class lists (which would be created in Windows as security groups for use in resource control by departmental OU admins).

Advantages

This design means departmental admins have less "account creation" work. ISU NetIDs for faculty and staff are created and populated into your departmental OU for you. Student accounts are also created for you (via Acropolis systems) and available for use by all departments.

1) Departmental admins retain total control of their OU and can manage it using all standard Windows techniques
2) ITS needed to do little or no work to get this process up an running. The automatic population of Faculty and Staff users into the proper OUs has been implemented.
3) The concern of "how do I know the difference between a main Acropolis NetID and a 'special purpose' Windows account" is answered. The ISU NetIDs are the ones without the "!" preceding them.
4) The Acropolis NetID namespace is not polluted with usernames that mean nothing in the enterprise central directory arena. The Windows usernames needed to schedule building rooms, slide projectors, and backhoes with Exchange, for example, need not live in Acropolis.
5) Some nice functions get better. Accounts suspended/unsuspended in Acropolis will be suspended in Windows. Departmental IT admins should NOT unsuspend/suspend user objects linked to ISU NetIDs (for example, when they leave the department). These users can expect their login to remain active. IT admins should move users they no longer want into the "Relocation" OU and send email to its-ad-admins@iastate.edu indicating their department and the username moved.

Disadvantages

1) Departmental admins must remember to use the "enforced convention" in their OU work
2) Some people may not like the convention - but then they should get their accounts from Acropolis.

Related Documents

http://tech.its.iastate.edu/windows/admin/UserMgmtInOUs.pdf