Windows Domain Strategy

March 20, 2003

Agenda

- Why bother?
- Objectives
- Process to gain consensus
- Key Issues
- Key points of Domain Proposal
- What next?

Why?

- Windows is very popular
- Support has evolved out of necessity
- Departments and Colleges building own structures
- An ITS strategy is needed
  - For support of ITS needs
  - For support of Penn State needs
  - For ubiquitous Penn State Access Account use

Objective

- Define a Windows Domain structure enabling the use of Penn State Access Account userids and passwords
- Deliver in two phases
  - Phase 1 – support for ITS departments
  - Phase 2 – support for other Penn State departments

Objective

- Solution must:
  - Provide authentication to domain users
  - Provide authorization for our domain users and systems (need to work on details for this - phase II)
  - Support the built in tools and services provided by Active Directory to manage systems, applications, and services
  - Be secure
  - Scale relative to our institutional size
  - Create an infrastructure that preserves the University's independence from any one vendor in supplying core services

Process

- Initial Strategy Proposal – July 2002
- Formed a Windows Domain Working Group to resolve issues
- Have been meeting since October 2002
- Have formed a consensus set of recommendations
- These were presented to our CIO 2/12/2003
- Have been accepted
- Now we really need to get busy!

DNS Issue

- Windows Child Domain by default inherits DNS from its parent
- Will cause DNS to match Windows Domain structure
- Would prefer that DNS matched organizational structure

DNS Policy Change

- DNS Policy had a loophole
- Have new proposed policy change
  - **DNS subdomain hierarchies must mirror Penn State organizational reporting hierarchies. It may happen that subdomain hierarchies show part of an organizational structure and to whatever level they do, the subdomains must reflect the organizational reporting structure. Hence, organizations may only assign lower level entries for their assigned subdomains that reflect administrative reporting hierarchies. For example, the College of X is assigned the subdomain X.PSU.EDU, then it may only make lower level assignments under the subdomain X.PSU.EDU to organizations within the College of X. And subdomains under X.PSU.EDU must mirror the reporting hierarchy within the College of X.**

Recommendations

- DNS is a separate issue from Active Directory or Windows Domain Strategy as long as we can comply with the newly proposed DNS Policy.
- Use a tree to forest child domain relationship to avoid DNS inheritance.
- Thus if we have a centrally managed windows domain called PSAD, its DNS name would be psad.psu.edu.
- Then if AIS wanted to create a Windows Child Domain called Betty, it could create betty.ais.psu.edu and have it be a Child Domain of psad.psu.edu.

Recommendation

- Authentication: The clear objective is an external trust relationship between the Windows Root Domain and a PSU MIT Kerberos 5 Key Distribution Center (KDC). This requires Windows Server 2003.
- Establishing an MIT K5 KDC as our master PSU KDC is the replacement strategy for DCE. We hope to have this by June 2003.
- Will use Windows Server 2003 for the ITS Windows Root Domain and establish an External Trust to the new K5 KDC.

Recommendations

- Use of existing “win.psu.edu” domain has not been adopted as a preferred option by the working group.
- Create a new centrally managed root domain managed by some other group, perhaps within ASET.

Recommendations

- The group recognizes that this initiative is time sensitive, and that an implementation target of fall of 2003 for phase I.

Recommendations

- As we move to a Windows Domain with an external trust to K5, support for services for older operating systems will not work.
- The Penn State community needs to receive information regarding the required OS level for participation in a centrally managed Windows Domain, and the sooner the better.

Recommendations

- Policies regarding the creation of child domains will need to be created and enforced.
- The Windows Operations Workgroup has a good start on these.

Test of Concepts

- Built separate Windows Server 2003 test bed
- Tried tree to forest child relationship
  - Was successful
- Built separate K5 KDC on Linux
- Formed external trust from root domain
  - Was successful
  - Requires Windows Server 2003

Domain Architecture

- Single centrally managed root domain
  - Authentication managed here
  - Access Account userids are joined here
    - **Enables services such as file service, roaming profiles, web authentication, automated application deployment, and terminal server**
    - **Authentication is the number one requested service**
  - Need to pick a name
    - **ad.psu.edu ?**

Domain Architecture

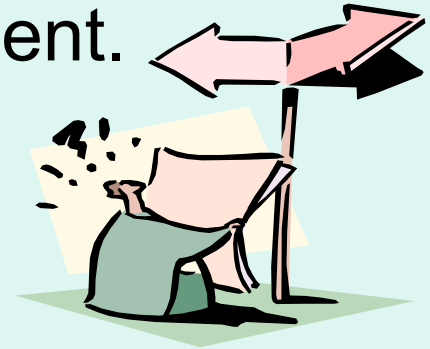
- Propose following offerings from root
  - Child domain
    - Tree to Forest Root
    - Must have admin resource to support this
    - Can delegate OU from here

What Happens to Existing?

- The TLT win.psu.edu remains separate.
  - Serving the needs of labs and classrooms
  - Stable and working well
  - Continue with password synch with DCE
- When we have the central K5 KDC form external trust from win.psu.edu
  - ad.psu.edu will move there faster

Next Steps

- Write a “white paper” defining the strategy
- Form a technical advisory group
- Define phase II services
- Set expectations and timeline for phase II
- Define what will happen to existing Beta Testers (Ag Sci and Wilkes Barre).
- Form a support group and implement.



Comments? Questions?