Namespaces Identity Management

IST346

Namespaces

So, what is a namespace?

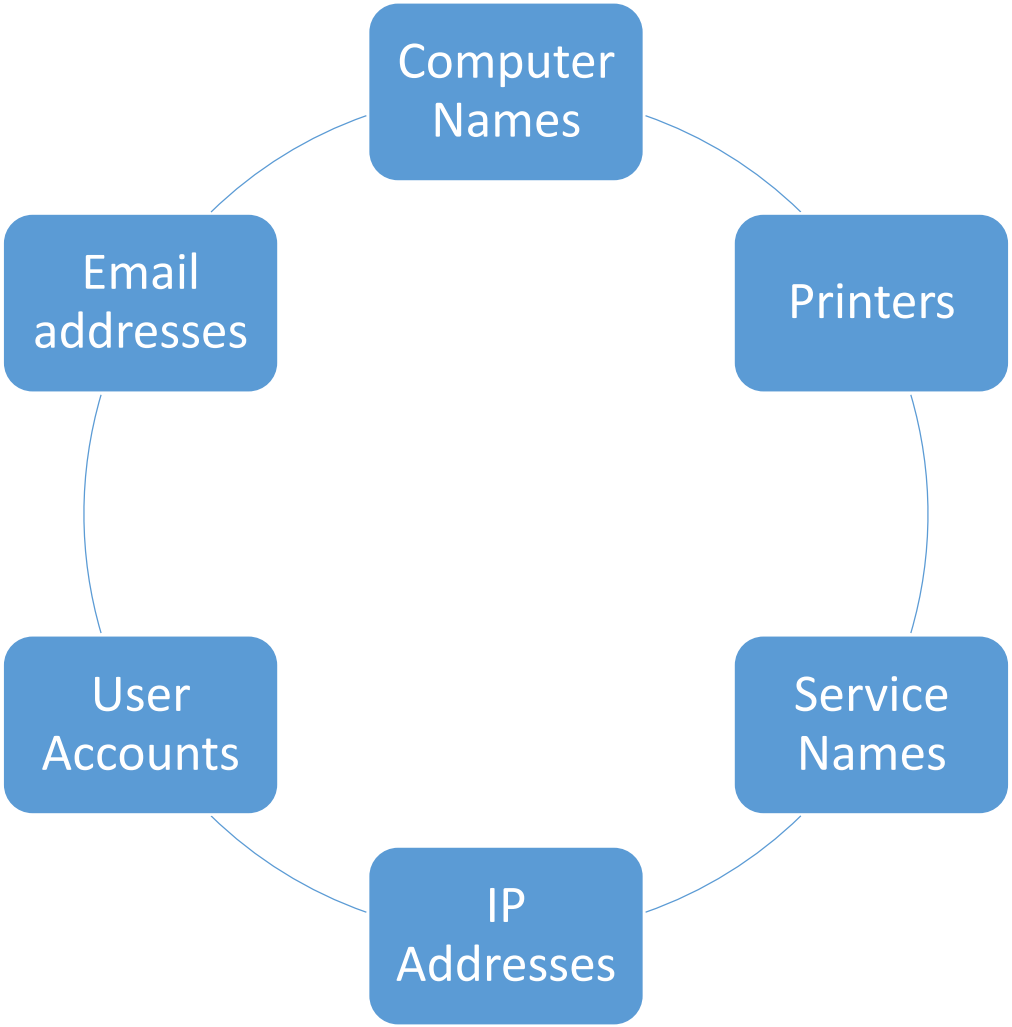
- **A namespace consists of :**

1. A set of defined and named keys
2. The attributes associated with each of the keys

- **For example, the linux and windows user accounts we've created in our labs are namespaces**

1. The have defined names (the user accounts themselves) tom, dick, harry, etc…
2. Each account has attributes associated with it: password, home directory, default shell, etc…

All sorts of namespaces:



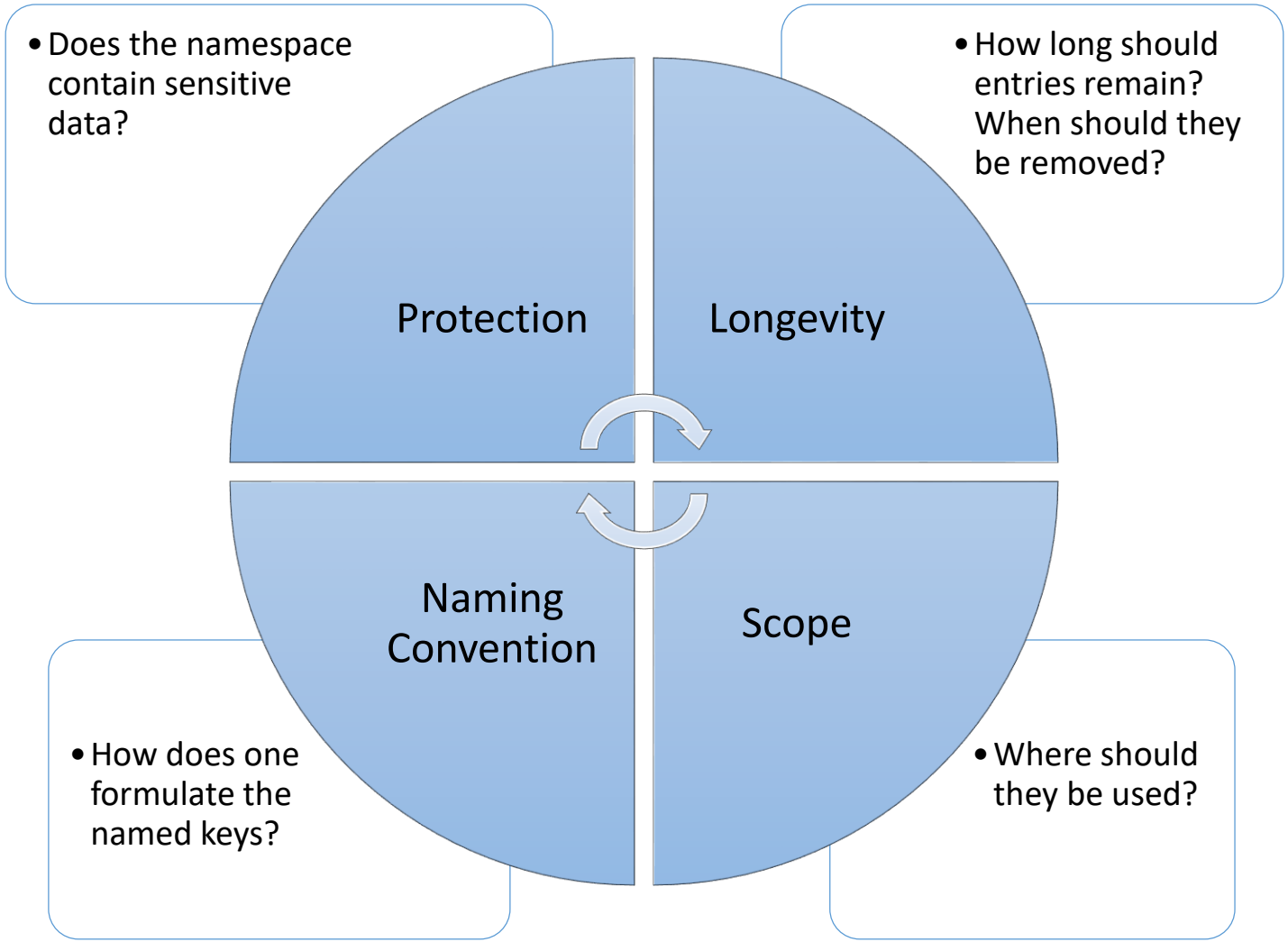
Two type of namespaces

- Flat
  - No duplicates can exist in a flat namespace.
  - SU NetID is a flat namespace: no two people have the same named key: tajorgen, sjrieks, relstad
  - User accounts are a flat namespace.
- Hierarchical
  - Namespace is organized in a tree
  - Duplicates can exist at nodes in the tree, but the overall name is globally unique.
  - DNS is an example of such a namespace: **www**.syr.edu **www**.microsoft.com **help**@oracle.com **help**@microsoft.com

Namespace Policy

- Consistent namespaces make everyone's job easier.
- Helps your users and admins find resources
- A well-governed policy is the key to a consistent and reliable namespace.
- The policy should have collision prevention for flat namespaces.
- Once you decide on a naming convention, it is difficult to change it.
- If there's one thing you should do by committee, its namespace policy creation!
- **ITS-Printer-MH250-01**

Issues Surrounding Namespaces



Naming Conventions

- Formulaic
  - Based on an algorithm, generic look and feel
  - Student001, student1002, server0001
- Themeatic
  - Planets, Constellations, Cartoon characters
  - Gamera.syr.edu, rodan.syr.edu
- Functional
  - Name matches function
  - smtp-host.syr.edu, help.syr.edu, clock.syr.edu
- Descriptive
  - By location, resource, type, device class
  - How SU names its objects in Active Directory.
- No Method
  - Everyone picks their own, first come first serve.
  - This is how DNS registrars allocate names on the Internet.
- Applied uses are usually a combination of multiple approaches.

Some Examples of namespaces.

And their naming conventions

Example namespace: NetID

- What is it?
  - Represents accounts for all users on campus
- Rules and Constraints:
  - Legacy systems require the account to be no more than 8 characters.
  - Flat namespace for all users associated with SU.
  - No two people can have the same NetID
- Convention:
  - Named keys are created via a combination of formulaic and functional approaches
- Examples:
  - **T**imothy **A Jorgen**sen **- tajorgen**
  - **P**eggy **M Brown** – **pmbro01 (pmbrown already existed)**

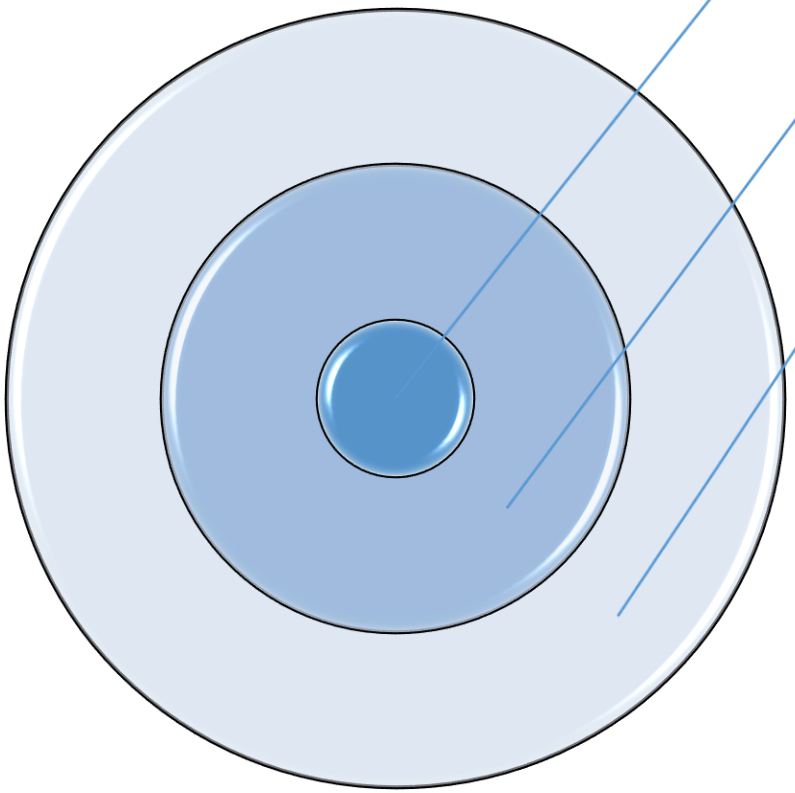
iSchool Workstation Naming (AD)

- What is it?
  - The method the iSchool uses to identify user workstations
- Rules and Constraints
  - For legacy windows computers, 15 characters maximum
  - Must begin with IST- to avoid conflicts with other organizations on campus (flat namespace)
- Convention:
  - Named keys are created from the user's netid and machine type (fac/staff desktop/laptop)
- Examples:
  - IST-SD-MAFUDGE
  - IST-FL-DJMOLTA

DNS Namespace

- What is it?
  - Used for registering names of computers on the internet or intranet.
  - www.syr.edu help@google.com
- Rules and Constrains
  - Except for .edu, .gov and.mil there aren't any
  - DNS is a hierarchy, duplicates allowed within different contexts, but not globally.
  - www.syr.edu www.syracuse.com www.google.com
- Convention
  - Top level, org level, hostname
  - Top level: http://www.iana.org/gtld/gtld.htm

DNS Hierarchy **www.syr.edu**



www

- host

Syr

- domain

Edu

- gtld

Descriptive Namespaces

- Descriptive names are the friendliest namespace.
- They are usually “self-explanatory”
- The should be governed carefully within the organization, for obvious reasons.
- Examples:
  - president@whitehouse.gov forwards email to user **barak.obama**
  - chancellor@syr.edu forwards email to **ksyverud**
  - http://printing.google.com gives you information about all the printers in google
  - The wireless networks AirOrangeHelp, AirOrange, AirOrangeX

Managing Namespaces

- Let's suppose your organization has
  - 10 Linux,10 windows servers, and 100's of workstations.
  - 100's of Users
  - An established a naming convention for user accounts and computers.
- How can you:
  - Avoid collisions of named keys?
    - E.g. **jasmith** = Jo Ann Smith on a Linux host, John Andrew Smith on a Windows host.
  - Manage the user and computer namespaces so that your system admins follow the conventions?
    - Create user **jsmith,** instead of **jasmith** for example.
- These are real-world issues… ideas?

Meta-Directory

- A Meta-Directory is a unified database of your namespaces.
- To create a named key for a namespace, such as a new user:
  - The information is added to the meta-directory
  - The account is *provisioned* from the meta-directory to the resource itself. (Account created on the Windows or Linux Server or both)
- Meta-Directories are namespace management.
  - You can buy **identity management** software to implement a meta-directory or build your own.
  - These solutions require a lot of planning, design and testing.

Name Services

Nameservice?

- **Nameservice** – A service which manages a namespace
- Examples:
  - **DNS** - manages host names
  - **DHCP** – manages IP Addresses
  - **LDAP** – manages user information
  - **Active Directory** – manages users, computers and devices.

Three A's

- **Authentication** – Verification of identity. Answers the question "Who are you?"
- **Authorization** – Verification of access. Answers the question "What can you do?"
- **Accounting** – Logging access to a service. Answers the question "What did you access or do?"

- Example: Your SUID card.
  - Verifies who you are.
  - Provides access to things (library, GYM)
  - Is recorded when used.

Two-Factor Authentication

- What you have
- What you know
- Example:
  - Google Authenticator

Directories

Directories offer a database for your namespaces.

Directories 101

- ***Directory***
  - A collection of information that is primarily searched and read, but rarely modified.
  - Named keys from namespaces are ideal storage candidates for directories.
- ***Directory Service***
  - Provides access to directory information.
- ***Directory Server***
  - Application that provides a directory service.
- ***Note:***
  - Directories are not Meta-directories. Directories store named keys, but do not provision them.

Advantages of Directories

- Make administration easier.
  - Change data only once: people, accounts, hosts.
- Unify access to network resources.
  - Single sign on.
  - Single place for users to search (address book)
- Improve data management
  - Improve consistency (one location vs many)
  - Secure data through only one server.

LDAP

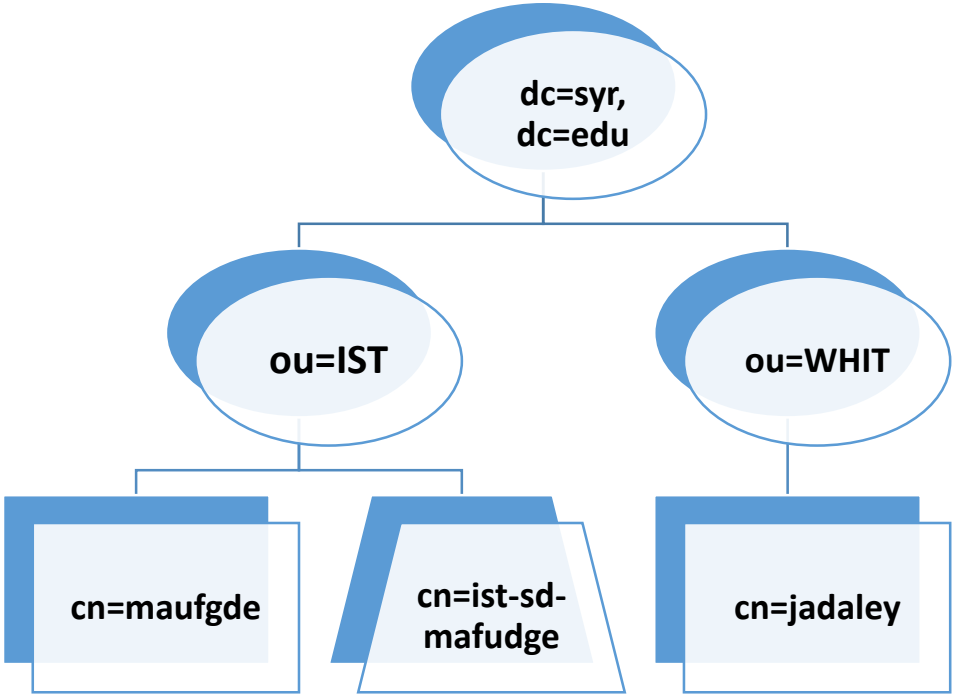
- Lightweight Directory Access Protocol
  - Lightweight version of the DAP based on X.500 directories. http://www.x500standard.com/
  - Just an Access protocol, not a directory itself.
  - The directory must be implemented on the server end.
- Directory services which implement LDAP
  - OpenLDAP
  - Fedora Directory Server (formerly Sun, Netscape)
  - Mac Open Directory
  - Microsoft Active Directory
  - Novell eDirectory (NDS)

LDAP Structure

- Hierarchal structure
  - Containers are called ***organizational units***
- An LDAP directory is made of ***entries***.
  - Entries may be employee records, hosts, accounts etc.
- Each entry consists of ***attributes***.
  - Attributes can be names, phone numbers, etc.
  - ***objectClass*** attribute identifies entry type, or ***schema***
  - ***Schema*** determines the available attributes for the entry
- Each attribute is a ***type / value*** pair.
  - Type is a label for the information stored (name)
  - Value is value for the attribute in this entry.
  - Attributes can be multi-valued.

LDAP DN

- The DN, or ***distinguished name*** represents the path from the root of the directory to the entry.
- (In this example the rectangle is a user objectClass, and the trapezoid is a computer objectClass)



My account:

Dn: `cn=tajorgen,ou=Users,ou=ITS,dc=ad,dc=syr,dc=edu`

My laptop computer:

Dn: `cn=its-l-tajorgen,ou=Computers,ou=ITS,dc=ad,dc=syr,dc=edu`

LDAP Authentication

- Anonymous Authentication
  - Binds with empty DN and password.
- Simple Authentication
  - Binds with DN and password. Cleartext. Bad.
- Simple Authentication over SSL/TLS
  - Use SSL to encrypt simple authentication.
- Simple Authentication and Security Layer
  - SASL is an extensible security scheme.
  - SASL mechanisms: Kerberos, GSSAPI, SKEY

Active Directory

- Microsoft's Directory service
- Used to manage users and computers in the enterprise.
- Hierarchy: Forest, Trees, Domains
- The Namespace is flat at the domain level
- AD Implemented using LDAP + DNS + Kerberos
- LDAP used for user, group, computer, policies and more.
- Kerberos used for computers on the domain and user logons
- DNS is used for naming computers on the domain

Active Directory

Some details about Microsoft's Active Directory

What is Active Directory?

Functional definition:

A Directory service developed by Microsoft that uses a hierarchical structure to store information about *objects* on the network. The differentiating component of this directory implementation vs. others are the types of objects that it tracks.

Also referred in some circles as AD or ADS.

What kinds of objects can AD track?

- Shared Resources:
  - Workstations
  - Servers
  - Shared volumes
  - Printers
  - Applications

- User resources
  - Users
  - Groups
  - Contacts
  - Mailboxes (Exchange)

Key features of AD

- AD as a namespace that is integrated with the Internet's Domain Name System (DNS).
- AD is a directory service central to the Windows Server operating system, which runs only on servers called “Domain Controllers”.
- Some directory services are integrated with an the operating system, and others with applications such as e-mail (Exchange) directories. Operating system directory services provide user, computer, and shared resource management while application services it provides extend the functionality or management of said application.

  Ex: AD stores all smtp (email) address for accounts in the user objects, allowing Exchange servers to receive email destined for those addresses.

AD Utilizes a distributed architecture

- In addition to providing a place to store data and services to make that data available, Active Directory can also protect network objects from unauthorized access and replicate information about objects across the entire network so that information about objects is not lost if one domain controller fails.

- The key here is building in redundancy when designing redundancy of this service (remember our in-class exercise from last week?).

Authentication

- Each domain controller has information for the entire forest to support authentication and access control.
- This provides the ability for local domain controllers (the “tree”) to provide a quick local lookup of authority.
- Not only do users but every object authenticating to Active Directory must reference the global catalog server (a domain controller), including every computer that is joined.

Benefits to using AD - Users

Prior to AD

- User accounts were configured in all of the disparate systems that users had to access, each with different passwords and policies governing access. Myslice, Email, file sharing servers, database servers, Peoplesoft, registrar system, etc…

After AD

- User accounts are created one central directory system and all other systems access AD for account information. Single account to manage, single system for making password changes, and groups can be created in AD for granting multiple users access to the same resource.

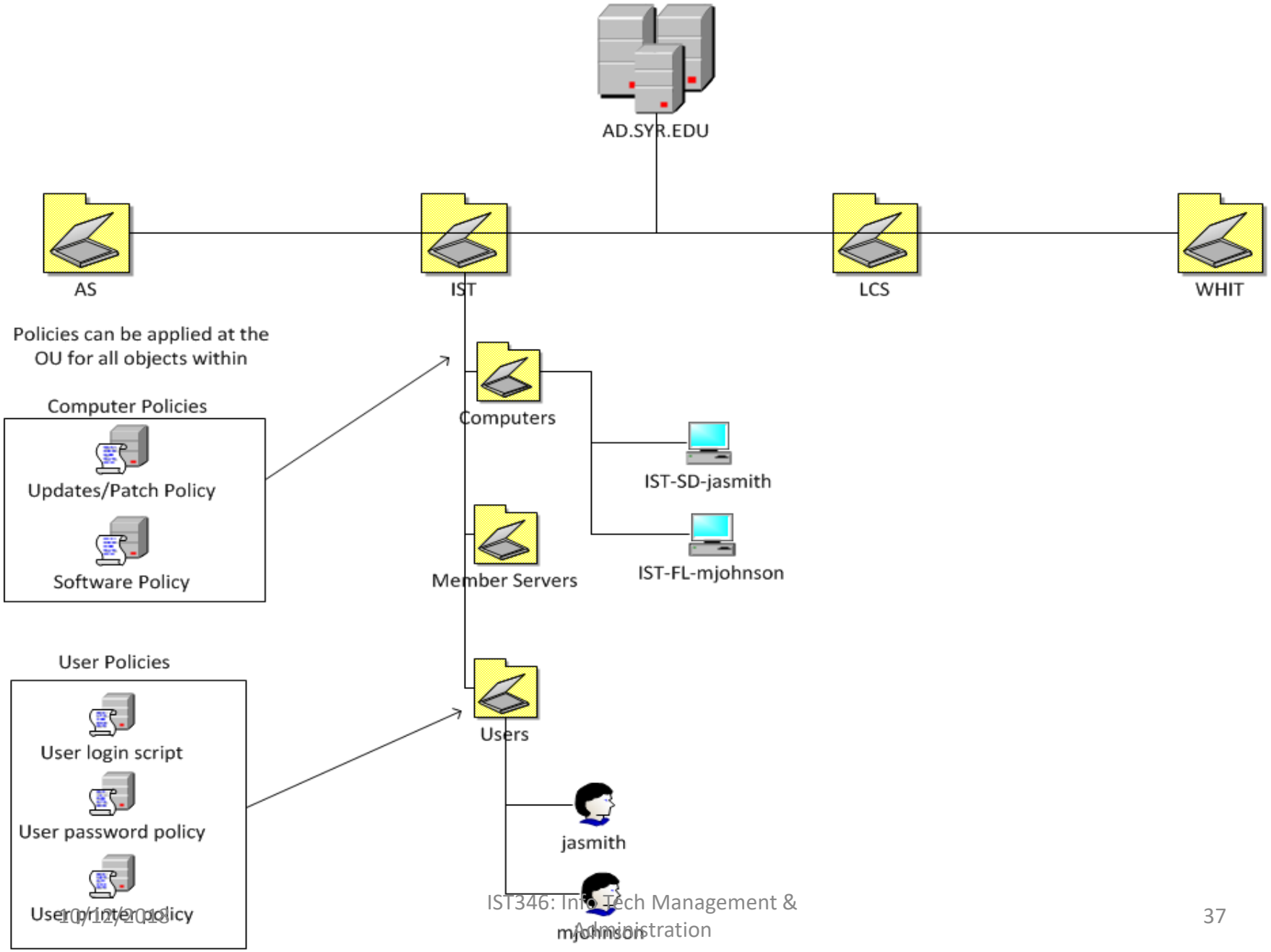
Benefits to using AD - Computers

Prior to AD

- PCs were setup as standalone entities, it would take as much as 10-20 hours of effort to manually visit each machine to configure the OS, setup local user accounts, map network drives, install software, etc… Not to mention the ongoing maintenance costs!

After AD

- PCs are joined to the domain, group policies can be created that will push new security patches, software, shared printers, and manage settings for all machines with a few mouse clicks.


AD.SYR.EDU
AS
IST
LCS
WHIT
Policies can be applied at the OU for all objects within
Computer Policies
Updates/Patch Policy
Software Policy
Computers
IST-SD-jasmith
IST-FL-mjohnson
Member Servers
User Policies
User login script
User password policy
User profile policy
Users
jasmith
mjohnson

Documentation

Every SA's favorite thing to do!

What is Documentation?

- Documentation: Process of keeping records for the purpose of referencing information at a later time or for use by others.
- What should be documented?
  - What you need later in time.
  - Don’t’ try to document everything. You can’t.
  - Don’t over complicate documentation.

Documentation

- What?
  - Complex procedures
  - Screen captures
  - Source code
- How?
  - Templates (title, metadata, what, body)
  - Tools (wiki, document repository, shared drive)
- Why?
  - Train other staff
  - Eliminate single-person dependencies
  - Reduce support calls
  - Justify the need for additional staff

Documentation templates

- Create a document template for similar types of documentation
  - Title: title of document that others understand
  - Metadata: author's name, date created / modified, etc.
  - What: describing the goal or purpose of the document
  - Body: the information your interested in documenting.

Examples of Common SA Documents

- Screen captures or screen shots
- Serial numbers or licensing information
- Complex commands or procedures
- Source code, if writing programs
- Important contact information, vendors information, emergency contact information.
- Checklists needed for common repetitive tasks.
- System/service design documents

Tools for Documentation

Systems for documentation other than file shares

- Helpdeks, SysAdmins, Procedures, FAQ, etc
- Wiki, such as wikipedia.com
  - Confluence: http://answers.syr.edu
- Sharepoint: http://sp.syr.edu
- Any type of Content Management System (CMS)
  - Basically what appears to be a website but can be managed, new pages added, documents attached, groups created, etc. via a series of web forms and a WYSIWYG tools.
- Can be automatically created: HW and SW inventory

Questions?

Do people who spend $2 apiece on bottles of Evian water know that spelling it backwards is Naive?