

**AD Policy Committee**  
**April 29th, 2011**  
**3110 Engineering Building II**  
**3pm-4:30pm**

Attending: Dan Green, Dan Evans, Billy Beaudoin, Michael Underwood, Joshua Gira, Tom Farwig  
Absent: Wes Thibodeaux Daniel Henninger

Policy Changes Approved Via Email:

"Apparently in the list of "things in the portal IE doesn't like" is the fact that <https://acs.ncsu.edu> is in the intranet zone but <https://www.acs.ncsu.edu> isn't. Any problem with adding the www version to the default client OS policies?" Approved over email, updated and posted to Sysnews on March 13th: <https://sysnews.ncsu.edu/news/4c7d355f>

## Agenda Items:

### Home Directory

The results/mitigation of the Home Directory attribute testing:

- Timeouts w/ offsite laptops
  - (laptops w/o connectivity having the 2 min delay even with cached creds)
- Users shouldn't be able to change their own rights
  - Decision is to remove users ability to do this.
- What's/Where B? from users
  - Solve w/ education
- Ported apps had some issues
  - Daniel found a few -- need a better list. What to do when we find an app? How do you mitigate?

### ReadOnly DC

Public Safety and University Police requests a ReadOnly DC.

- to maintain operations in the event of a network outage (their own servers will be hosted on-site in their building, with both login and rights management to files based on WolfTech AD).
- there will be lots of logistical discussion to follow (physical server? vm? firewalls?)
- Billy:
  - a. probably need to move them to their own site...
  - b. By object, point at RODC (rather than site)
  - c. Install 6th full DC if there's a secure facility
- **Policy Comm: Tech Comm should decide about which option above; Policy is fine with their decision. We agree that from a policy standpoint, the issues to consider is the physical security of the DC. We believe Campus Police can provide that level of physical security (though the DC Admins will need to be given a tour of the facility). In addition, the new DC (full or RODC) should only be providing this function, meet the performance requirements/standards of existing DCs, and we'd expect Campus Police to provide the**

**funding for said machine.**

#### **SCCM Update:**

- Update on Progress
  - Discovery Methods: currently it scrapes all of AD at midnight. Can also then scrape deltas throughout the day -- set now to 5mins.
- Decisions Needed:
  - Add oit.ncsu.edu to the list of DNS domains that resolve for all computers. **Agreed; Billy will handle.**
  - Various other default settings explained by Michael Underwood. **In the end, committee didn't have much to say about the defaults, and consensus was to stick with them until we'd seen the results and could always change them later. Basically, we don't have the experience at this point to make an informed decision. Some members suggested that a subgroup review/discuss the settings and report back.**
  - Want to get the committee's input on whether to roll out SCCM client to all machines at once or stage it.

#### **Certs Update:**

- RDP Certs

"One of the goals of rolling computer certs is to have win7/2008r2 machines using them for their RDP certs."

  - We've not set the GPO setting, but would like to discuss it at the next meeting.
- User Certs
  - Still need to provision to allow ComTech to use for new wireless network authentication.

#### **Default QoS setting [Billy]**

Request to implement new Default Domain QoS policy that will define a default outbound bandwidth throttling rule limiting outbound bandwidth to 850Mb/second. This should help prevent individual boxes with a 1Gb uplink from being able to saturate the uplink of an access switch on their own. The majority of current Gb uplinks are limited to servers in the data centers and thus single boxes causing network saturation is rare, we want to be proactive and be as good of netizens as possible, preventing networking issues as much as possible while trying not to impede clients or services. The majority of clients will never hit the threshold. Those that do will have their outbound bandwidth limited and traffic kept at the 850Mb/second rate. This should also help alleviate any negative impact from QoS settings set by Comtech on the networking infrastructure. Note that this is a "default" policy, meaning that any OU administrator can choose to override these settings at their OU. **Committee had no objections.**