Minutes 02-25-11

AD Policy Committee

Attendees: Dan Green, Joshua Gira, Daniel Henninger, Tom Farwig, Joey Jenkins
Guests: Derek Ballard, Alan Gerber, Debbie Carraway

SCCM Update (Billy):

Hardware is purchased, arrived, racked, and being installed. We'll should be building the SQL cluster and rolling machine certs in the next 2 weeks. Which means we'll probably be pushing the agent to all machines in March and working on reporting.

2008/2008r2 Default Domain Policies: Missing firewall setting for Win2008 Domain (Dan):

" It looks like we missed a fairly important setting in the 2008/2008r2 Default Domain Policies. For 2008 + Domain profile, the state is set to "Not Configured". So for 2008r2/Public/Private/Domain and 2008/Public/Private the firewall is on, but 2008/Domain its probably Off. There are 90 2008 servers in the domain. At least 15 or so I'm certain there is a closer setting turning it on. So I'd like the go-ahead to schedule a date to flip the switch to "on". Spring break seems like a good time."

AD Pol Committee approved action -- recommend that the email goes out tonight and that the units affected get a side-email to make sure they pay attention. Dan will send out.

2008 Server Default Policies and "RemoveUsers" Script (Dan):.

Want to remove the RemoveDefaultUsers.vbs script from the domain wide 2008 Servers policy (and all future server policies. Reasoning: this script is intended for client computers -- servers are expected to use restricted groups and this policy can conflict with that practice, interrupting services.

Was removed by the Domain Admins on 02/15/2011 to prevent problems:
http://sysnews.ncsu.edu/news/4d5b30c4

AD Pol Committee approved action. Keep as is now. (though we should probably remove the "Domain-Remove Default Users" policy as it would appear to be unnecessary)

Firewall rules for Applications (Billy): (TABLED for email discussion or next Meeting)

When packaging applications for deployment to campus systems on Windows, the default rules are for closed, open to local subnet, and open to the world. In making a number of applications work correctly, firewall rules are being set to "open to the world" or "*". If determining the exact hosts that need access to a port for an application, app packagers are recommended to use the follow list that corresponds to "on-campus": 152.1.0.0/16, 152.7.0.0/16, 152.14.0.0/16, 10.0.0.0/8, 172.16.0.0/12

Sample applications: Trend AntiVirus, Xwin32, VMWare Player, Remedy (not a comprehensive list)

Discussion of impact?
Who'll implement?
How to monitor for in the future?

New NCSU Certificate (Derek)

At a recent discussion with S&C, Comtech, ISO, and most WT Domain Admins, a request was made to switch from using the current NCSU CA to a new CA created using MS Certificate services and chain all other certs from there. ***Previously, we had gotten approval for creating computer certs off of a subordinate of the current NCSU CA***, and not a new one that we'll be generating for OIT-S&C, who will be the admin for it. Additionally, Comtech is requesting auto-enrollment of User Certificates to be used to roll 802.1x for the Wireless network this summer. So, while it might be premature, I'd like approval (pending testing of course) to be able to do user auto-enrollment later this semester.

- Moving to using a new "North Carolina State University CA" will require pushing it out to all clients on all OS's. Which will take a while. So we'll likely be pushing both for a long time while the old NCSU CA-generated certs age out. Just like the ITD CA ones are now.
- Using an MS CA at the root lets us get support from MS and prevents us from running into issues on the AD side in the long run.
- User cert auto-enrollment, if limited to the "client authentication" OID will cause next to zero problems and only be able to be used for (gasp!) client authentication, and at this time, only planned for wireless. Note that comtech was going to roll their own certs for this already. IF the discussion turns towards having the user certs be usable for encryption, then there is a whole lot of possible implications.

Other uses for user certs -- code signing, new wireless auth, new voicemail service?
Which users? UnityID, dept accounts?

(need to think about getting the new certs to linux and mac? Web servers that do the ldap scripts?)

AD Pol Comm -- approves new MS CA method, rolling of new cert in the main policies, and roll out of computer certs. Want more testing (and a clearer explanation of usage and scope) of user certs before approval to push across the board.

NCSU-Banned Software Policy (Dan)

Recommendation to remove this policy. Was created back in 2005, and has hardly ever been updated (we've certainly not added or removed applications from the list since 2006-2007… based on a very old way of doing software restriction -- pain to edit. New policy would need to use AppLocker instead.

- Question: can we simply delete this policy, then later add a new one, or do we need the new one first?
- App locker doesn't work on Win7 Professional?

Email to the list explaining WHY we're dropping this.

a. Un-enforce first. Allows local testing.
b. Create a "SW" group that is added to the deny for the policy to let folks add their computers to it.
c. In about a month, Unlink it. Keep for historical for now.
d. They want the Sec Comm to maintain the new one.
e. Publish information to the OU Admins on how to block software, for one, AppLocker.

Steps above approved by Committee

Debbie: AD Health Check

May 2nd-4th. MS sending folks on campus to examine our setup and find out any issues / make recommendations.