Wolftech AD Technical Committee
March 18th, 2011, 9:30 AM, Page Hall - Room 21

Minutes:

- Review: 2008 Default Domain Policy Swapout
  - Issues: Firewall consistencies resolved
- Update: Certificate Services
  - Created a new Stand-alone and "Enterprise" CA using MS Certificate Services
  - Cert request process:
    - Some Cert types (default computer and user certs) will use Auto-Enrollment, others will be request/approval (code signing, web servers, etc)
    - Certs can be requested via "certmgr.msc" (certificates snap-in).
  - Key recovery agent:
    - Certain cert types will have their private key escrowed in AD, encrypted with user's password.
    - KRA is a secondary cert that can decrypt the private key in AD in cases of password reset.
  - Certificate Revocation:
    - Permanent Certificate Revocation Location: www.ncsu.edu/crl - we're still waiting on AFS access to put the CRLs and CRTs in place. All certs will have the CRL information populated in them.
    - The timeframe on the root CRL will be long due to being offline, the enterprise will be short and copied via a cron
    - Online Responder – Server running the OCSP protocol. AD machines will do OCSP first, CRL second.
  - Computer Certificates:
    - V2 certs (SCCM docs are inconsistent with respect to x509 v3 cert support)
    - OIDs: Client Authentication (SCCM), Server Authentication (RDP)
    - 1 year length
  - User Certificates:
    - Initially creating a Client Authentication cert for 802.1x for wireless
    - General purpose user certs will be done later after IDM discussion
    - 5 year length
- Update: SCCM
  - Done: Schema
  - Done: SQL Cluster and DB
  - Done: Certificate Services and Site Server Signing Cert
  - Done: Firewall rules (host-based and network based)
  - Done: Local Pre-Reqs
  - Install on Monday
  - Schedule open meeting after agent pushed for reporting
- Update: Website
  - Open up to whole university? Yep.
- Update: Domain Controller upgrades
  - HW - adric.wolftech.ad.ncsu.edu replaces wt-dc-00
  - 2nd new DC
  - SW - Sp1 upgrade – will pull out each DC, upgrade, and add back
- Review: Network Firewall Global Objects

    - Default Outbound rules for Comtech firewalls for access to Directory Services and Client Management servers
    - Default Port Groups for requesting inbound access for server management of windows servers - "I am a server admin on computer BALH and I want to manage my Windows Boxes with IPs BLAH".
- Update: QoS GPO Throttling
    - Group Policy-based QoS settings work.
    - Note that it is in MB, not Mb and must be a power of 2.
- Request: Add Bitlocker configuration to Laptops DDP?
    - ECE, PAMS, COEDEAN are using Bitlocker
        - Develop default policy and email to governance committees
    - Create hierarchical group that we also add NCSU-Laptops group to as default
- Update: Windows Firewall w/Computer Groups
    - Doesn't work without IPSEC settings
    - IPSEC is scary easy to mess up and break things
    - IPSEC w/ null encapsulation uses IPSEC auth + doesn't encrypt payload - IDS can inspect
- Update: AD Health Check: May 2-4
- Update: Home Directory - testing in progress

Action Items:

- Open up website to known-user
- Talk to Comtech about QoS – Default Outbound Throttling set to 850Mb
- Schedule Bitlocker meeting and make recommendation
- Submit Firewall baselines to networking working group

Pushed to Next Meeting:

- Research: ADWS
- Adding Citrix ADMX to central store
- Adding TS Licensing Permissions for user accounts pre 2008
- WSUS - msupdates alias
- DRAC Cards - Schema extension, Certs,
- Mac Schema Extensions
- GPO Modelling Permissions