WolfTech Active Directory: Diagnostic Tools

April 6th, 2012

2-4pm Daniels 201

http://activedirectory.ncsu.edu

What we are going to cover...

- Problem Reporting
  - Problem Steps Recorder
- Application Diagnostics
  - Lua Buglight
  - Sysinternals Suite
- OS Diagnostics
  - Windows Performance Toolkit
  - Sysinternals Suite
- Environment Planning and Diagnostics
  - Security Compliance Manager
  - WDRAP Scoping Tool
  - WDRAP (Windows Desktop Risk and Health Assessment Program) Tool

Problem Steps Recorder

How do I use Problem Steps Recorder?

- Start -> Run -> psr
- Start Record, click around, add comments, stop record

Uses MHTML

- All images are mime encoded in the hypertext
- Viewable in Chrome/IE/Opera
- Firefox requires a plugin

Already in Win7+

NC STATE UNIVERSITY

Application Diagnostics

LUA Buglight

- Uses Administrator Credentials only for UAC Admin Approval mode
- Run Application you wish to diagnose
- As the Application gets "Access Denied" it elevates and logs the change
- You get a report of all actions that need Administrative access

Sysinternals Suite

- AccessEnum
  - View all of the permissions within a directory structure
- Process Explorer
  - View all aspects of current processes
- TCPView
  - View all of the open TCP/UDP connections
- Process Monitor
  - View all registry, file, process, and network activity
  - Provides filtering, highlighting, and summaries

http://technet.microsoft.com/en-us/sysinternals
http://live.sysinternals.com/

OS Diagnostics

Windows Performance Toolkit

- Capture - Copy Xperf{x86, x64, i64} folder to local machine
- Run traceboot.bat as admin, Reboot, Login, End Capture
- Evaluate - Install wpt_{x86, x64, ia64}.msi - Performance Analyzer to view
  - Process Lifetimes/Service Startup - Determine what is slowing boot/login times
  - Disk/Processor Usage per Process - Determine what is limiting certain processes

Install From:
\\wolftech.ad.ncsu.edu\engr\coedean\ou_admins\WDRAP\Windows Performance Toolkit Install

Sysinternals Suite

- AutoRuns
  - View all items that run automatically at startup or login
- PSTools
  - Command-line set of tools for pulling info or running commands remotely

http://technet.microsoft.com/en-us/sysinternals
http://live.sysinternals.com/

NC STATE UNIVERSITY

Security Compliance Manager

Backup GPOs
Import GPOs
Diff GPOs
Security Compliance Manager Page

Diff'ing Does Do:

- All administrative template settings in recent versions of Windows, Internet Explorer, and Office
- Password policies, account lockout policies
- Security options and user rights assignment
- Legacy audit policies and advanced audit policies
- Windows Firewall with Advanced Security

Diff'ing Doesn't Do:

- Restricted groups
- Software restriction and application control policies
- Public key and Kerberos policies
- Scripts
- IP security policies and policy-based QoS
- Group policy preferences

NC STATE UNIVERSITY

WDRAP Scoping Tool

Verifies connectivity to client machines
If all the tests are passed, it means that:

- SCCM Right-Click tools will work
- Remote MMC Consoles will work
- Powershell remote execution will work (not WinRM)
- PSTools will work

Install From:
\\wolftech.ad.ncsu.edu\engr\coedean\ou_admins\WDRAP

Requires:

- An "Allow * from IP" firewall rule from OU Admin computer to clients
- Remote Registry, WMI, Performance Monitoring

NC STATE UNIVERSITY

WDRAP Tool
(Windows Desktop Risk and Health Assessment Program)

WDRAP Datasheet

Pulls lots of information from clients, locates issues, and rates them

Includes:

- Remote Event Logs
- Resultant Set of Policy
- Microsoft Baseline Security Analyser
- Windows Performance Toolkit
- Hardware, Software, Networking

Install From:
\\wolftech.ad.ncsu.edu\engr\coedean\ou_admins\WDRAP

Run from Win7 Machine

NC STATE UNIVERSITY

Where Can I Go for Help?

AD Site

- http://activedirectory.ncsu.edu

Mailing Lists

- activedirectory@lists.ncsu.edu

Jabber

- "activedirectory" on conference.jabber.eos.ncsu.edu

Remedy

- wolftech_ad_technical@remedy.ncsu.edu

Governance Committees

- http://activedirectory.ncsu.edu/governance/

NC STATE UNIVERSITY

Q & A

NC STATE UNIVERSITY