Care and Feeding of Windows Servers
(Best Practices/101/ “...for Dummies”)

IT Partners
June 1, 2006

Paul Dzus, Network/IT Manager, The MIT Press
Background

• Myself
  – 10 years at MIT Press
  – 7 of them in IT Dept; Manager for last 3

• Mostly self-taught / “hands-on” experience
  – Some A+/Microsoft classes
  – assembled workstations/server from components
  – Lots of “best practices” reading material
  – Help desk / support calls

• Our environment
  – Workgroup, not Domain
  – Windows 2000/2003 and some Linux (RH & FC); 12 servers total
    • 75% WinXP clients; 25% OSX clients
  – 3 FT techs (myself incl.) cover 100+ employees
  – Since XP/OSX; employees are User-level, not Admin-level

• weekend server monitoring
  – poor “server room” conditions
  – overheating / crashes
  – multiple compromises
Setup checklist

*(not for win.mit.edu!)*

- Clean installs
- Service packs
- WAUS
  - [http://web.mit.edu/ist/topics/windows/updates/](http://web.mit.edu/ist/topics/windows/updates/)
- VirusScan
- Windows Firewall (Server 2003)
  - Especially if no hardware firewall, turn it on!
  - Only necessary exceptions
- Users/Permissions
  - Limit access/rights
  - Strong passwords
- Turn off unnecessary services
  - Security & performance benefits
- Clean out: `HKEY_Local Machine\Software\Microsoft\Windows\CurrentVersion\Run`
- Group Policy
  - Restrict anonymous access, enforce password rules, etc…
Daily checklist

• netstat –ano
  – whois

• Event viewer
  – System errors
    • Disk full
  – Failed login attempts
    • Esp. 529, 681

• MRTG (http://web.mit.edu/mrtg/www/)
  – normal vs. abnormal traffic

• 3-DOWN (http://is3down.mit.edu/)
  – current events & warning of planned outages

• Backups
  – current, multiple, off-site
EOQ/EOM/EOY checklist

- Free space
- Defragment
- Password audits
  - LC5
- Network scanning
  - Nessus (ports)
  - MBSA (patches)
- Policies & Procedures
  - Disaster recovery
  - written
    - Setup checklists
    - Employee hire/exit
Other Useful Tools

  - TCPview
  - ProcessExplorer

  - Search for .exe’s & .dll’s
    - What is it? What does it do?

- Remote Desktop (w/MIT VPN!)

- have a personal “toolkit”
  - on a CD (or USB thumb/keychain drive)
    - Keep it updated
    - Also use to copy off logs, etc.

- Google!
Educate yourself

Books 24x7
- [http://libraries.mit.edu/get/books24x7](http://libraries.mit.edu/get/books24x7)

- Safari Tech Books Online (includes O’Reilly pubs)
  - [http://libraries.mit.edu/get/safari](http://libraries.mit.edu/get/safari)

- Element K
  - wbt-request@mit.edu
  - for yourself and your “customers”
Stay informed!

• Websites of interest:
  – Internet Storm Center (news/alerts)
    • http://isc.sans.org
  – Shields Up! (free port scan)
    • https://www.grc.com/x/ne.dll?bh0bkyd2
  – Microsoft TechNet (info/links for IT folk)

• Mailing lists of interest:
  – Security-fyi mailing list (Security-fyi@mit.edu)
    • http://mailman.mit.edu/mailman/listinfo/security-fyi
  – UNISOG mailing list (unisog@lists.sans.org)
    • http://www.dshield.org/mailman/listinfo/unisog
Stay informed!

- **User groups:**
  - MIT= WinPartners, IT Partners, MacPartners, etc..
  - Boston Area Windows Server User Group
  - New England Information Security Group
    - [http://neisg.org/](http://neisg.org/)
  - Boston Network Users Group
    - [http://www.bnug.org/](http://www.bnug.org/)

- **Other:**
  - IS&T Security page
    - [http://web.mit.edu/ist/topics/security/](http://web.mit.edu/ist/topics/security/)
  - Security Camp @ MIT (annual, August)
  - Security Camp @ Boston University (annual, February)
    - [http://www.bu.edu/security/camp/](http://www.bu.edu/security/camp/)
  - Other local/regional user groups (Exchange, SQL, Unix/Linux, Mac)
    - [http://www.bostonusergroups.net/](http://www.bostonusergroups.net/)
Q & A / Discussion
THANK YOU!