ClamAV on Linux

- Using ClamAV on a Linux server

By Josh Knight <jgknight@mtu.edu>
Linux/UNIX Users Group
Fall 2011 Installathon

What is ClamAV?

- Open source anti-virus program
- Cross-platform, BSD, Linux, and Windows
- Detect infected files, does not remove them by default
- Free of cost

Linux...and Viruses?

- Though Linux is secure, a file server could be holding infected files
  - Don't want to spread to Windows clients
- File server, mail server, even web servers could accidentially spread a virus to clients
- ClamAV on Linux can remove those files
  - Other vendors have clients but are proprietary and have licensing fees

Installing ClamAV on Linux

- Debian/Ubuntu
  Sudo apt-get install clamav
  - This installs both the scanner and the updater
  - You can install clamav-daemon to automate use
- In the repos for most distros
- GUIs also exist for desktops

Running and Updating

- You'll want to update the anti-virus database before you scan
  - Sudo freshclam
- Next run the actual scanner
  - Sudo clamscan -r -i /
  - This scans '/' recursively and only lists infected files
  - Manually inspect or remove the listed file
    - May be wrong, not 100% accurate. Be careful. Use -V with caution

Automate Scanning

- You can automate scanning, useful on servers
  - Sudo crontab -e

  -
    ```
    0 0 * * 1-7 freshclam
    5 0 * * 1-7 clamscan -r -i / | mail tux@mtu.edu
    ```
  - This updates at 12:00am and scans 12:05am, and then emails you any infected files
- Some daemons and services can use clamav-daemon to scan on-demand
  - Mail server scans incoming emails
  - Drupal module scans new attached files

ClamAV File Systems

- ClamFS
  - User-space file system scans a file before opening them
- Avfs – Anti Virus File System
  - True file system with on-access scanning
- Dazuko
  - Kernel module for file access, on-access scanning
- Samba-vscan
  - Scans Samba shares, on-access scanning

Resources

- ClamAV website, http://clamav.net
- man clamav
- ClamSMTP for mail servers, http://thewalter.net/stef/software/clamsmtp/
- ClamAV module for Drupal, http://drupal.org/project/clamav