MFM - Medium Facilities Management

By Marc DeBonis
Systems Architect, Sr.
SETI-MIG
marcd@vt.edu

V1.1 - 051012
w2k.vt.edu (Hokies)

- Managed by CIT
  - Forest infrastructure
  - Domain infra
    - Just DCs in here…
  - User accounts
    - 6739 user objects

- Managed by DIT
  - User accounts
    - Via HSS
    - Via OUadmin
    - Via MMC

- Cost = personnel
cntrlsvcs.w2k.vt.edu (Central Services)

- Managed by CIT
  - Forest infra
  - Domain infra
    - Over 50 dept OUs

- Managed by DIT
  - Computer accounts
  - User accounts
    - Via MMC

- Cost = $\Delta t$, personnel
childdomain.w2k.vt.edu (Child Domain)

- Managed by CIT
  - Forest infra
    - 14 child domains

- Managed by DIT
  - Domain infra
  - Computer accounts
    - Including DCs
  - User accounts

- Cost = Δt, $, personnel
univsvcs.w2k.vt.edu (University Services)

- Managed by CIT
  - Forest infra
  - Domain infra
  - Computer accounts
    - Including DCs

- Managed by DIT
  - Computer accounts
    - Via HSS

- Cost = personnel?
HSS - My Services

<table>
<thead>
<tr>
<th>Manage a Computer in the University Services Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation Name: W2KSRV</td>
</tr>
<tr>
<td>Operating System: Windows 2000 Server</td>
</tr>
<tr>
<td>Service Pack: Service Pack 4</td>
</tr>
<tr>
<td>OS Version: 5.0 (2195)</td>
</tr>
<tr>
<td>Status: Enabled</td>
</tr>
<tr>
<td>Level of Service: No Facilities Management</td>
</tr>
<tr>
<td>Change Level of Service to: [Medium Facilities Management (public beta)] Change</td>
</tr>
<tr>
<td>Click <a href="#">Here</a> for detailed information about Medium Facilities Management (public beta).</td>
</tr>
<tr>
<td>MFM is currently in a public beta test. Click <a href="#">Here</a> for more information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Add a Computer to the University Services Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>You currently manage 1 computer in the University Services Domain. You are allowed to manage up to 3 computers.</td>
</tr>
<tr>
<td>Workstation Name:</td>
</tr>
<tr>
<td>Level of Service: No Facilities Management</td>
</tr>
<tr>
<td>Click <a href="#">Here</a> for detailed information about No Facilities Management</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remove a Computer from University Services Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation Name: W2KSRV</td>
</tr>
<tr>
<td>Remove Computer on <a href="#">Here</a> for more information.</td>
</tr>
</tbody>
</table>
## FM feature set comparisons

<table>
<thead>
<tr>
<th></th>
<th>Computer domain membership</th>
<th>Proactive security scans</th>
<th>System security hardening (ICF/WSUS)</th>
<th>Managed SW install (AV, Firefox, BGinfo, etc)</th>
<th>Defense-in-depth (LUA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NFM</strong></td>
<td>![√] 171</td>
<td>![X]</td>
<td>![X]</td>
<td>![X]</td>
<td>![X]</td>
</tr>
<tr>
<td><strong>SFM</strong></td>
<td>![√] 29</td>
<td>![√]</td>
<td>![X]</td>
<td>![X]</td>
<td>![X]</td>
</tr>
<tr>
<td><strong>MFM</strong></td>
<td>![√] 10</td>
<td>![X]</td>
<td>![√]</td>
<td>![√]</td>
<td>![√]</td>
</tr>
<tr>
<td><strong>FFM</strong></td>
<td>![?] 0</td>
<td>![?]</td>
<td>![?]</td>
<td>![?]</td>
<td>![?]</td>
</tr>
</tbody>
</table>
MFM requirements

- A desktop class system running Windows XP Pro or higher
  - Updated to service pack 2
- The system is attached to the network with a wired Ethernet connection
- A valid Hokies ID to access Hokies Self-Service
  - Use your PID to upgrade your Hokies contact to a full Hokies user account!
- A willingness to provide feedback!
  - please please please please…
- A reminder that MFM is in a late beta phase
DIY?

- See http://mfmwiki.w2k.vt.edu
  - Site includes the 70+ page document which details EVERYTHING we’ve done to build MFM!
  - Use the wiki for Q&A, feature requests, comments and suggestions
- Feel free to email mfm_beta_help@vt.edu
One more thing...

- Those using SFM have been getting proactive security scans on a weekly basis from a tool called Sunflower...

- Today we’d like to announce Sunflower v2!
  - Based off of MBSA v2.0 technology
    - Security updates
    - File system security
    - Automatic updates
    - Password expiration
    - IE zones / Macros
    - Auditing
    - Services
    - Shares

- Reports stored as secure web reports

- A report identifies what was scanned, strengths, weaknesses, and steps for remediation

- Systems will maintain a history of the last 5 scans
Sunflower v2 (mockup)

Welcome to Sunflower v2

MBSA scanning results

You are logged in as: hokebird

Sunflower History

Your Machines:
- GOHOKIES
  - 10/10/05
  - 10/3/05
  - 9/26/05
  - 9/19/05
  - 9/12/05
- HOKIESRULE
  - 10/10/05
  - 10/3/05
  - 9/26/05
  - 9/19/05
  - 9/12/05
- FLYVTFLY
  - 10/10/05
  - 10/3/05
  - 9/26/05
  - 9/19/05
  - 9/12/05

Return to Sunflower home

Sunflower v2

MBSA scanning results

Not all hard drives are using the NTFS file system.

Result Details

<table>
<thead>
<tr>
<th>Drive Letter</th>
<th>File System</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:</td>
<td>FAT</td>
</tr>
<tr>
<td>D:</td>
<td>NTFS</td>
</tr>
<tr>
<td>E:</td>
<td>NTFS</td>
</tr>
</tbody>
</table>

Administrative Vulnerabilities

<table>
<thead>
<tr>
<th>Issue</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System</td>
<td>Not all hard drives are using the NTFS file system.</td>
</tr>
<tr>
<td>Automatic Updates</td>
<td>The Automatic Updates feature has not been configured on this computer. Please use the Control Panel to configure Automatic Updates.</td>
</tr>
<tr>
<td>Password</td>
<td>Some user accounts (2 of 3) have non-expiring passwords.</td>
</tr>
<tr>
<td>Incomplete Updates</td>
<td>No incomplete software update installations were found.</td>
</tr>
<tr>
<td>Windows Firewall</td>
<td>This check was skipped because it cannot be done remotely.</td>
</tr>
</tbody>
</table>
Present & Future MIG errata

- Did you know? IT Wiki now available
  - [http://itknowhow.w2k.vt.edu](http://itknowhow.w2k.vt.edu)

- Migration of Hokies root domain from Windows 2000 to Windows 2003
  - ETA: ~before Thanksgiving (Nov 14 -18)

- WSUS for Faculty/Staff/Students
  - In discussion with potential sponsors now!
  - ETA: ?

- ADadmin
  - Replacing OUadmin, MMC, and many IRM manual processes
  - ETA: ?