



Advanced Techniques for managing Windows with HP Systems Insight Manager



Scott Shaffer
Manager, Insight Manager development
Hewlett-Packard

© 2004 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice



Agenda

- SSH, OpenSSH, Windows CLI
- XML for copying script and executing it
- Importing (& exporting) tools with mxtool
- Examples
 - Web JetAdmin
 - Terminal Services web launch
 - Systeminfo
 - WMIC

“Administration can prove quite challenging. It takes skill and experience...”

Bruce Momjian

Core developer on PostgreSQL



OpenSSH

- OpenSSH is a **FREE** version of the SSH protocol suite
- OpenSSH encrypts all traffic (including passwords)
- The password for telnet, rlogin, ftp, and other such programs is transmitted across the Internet unencrypted
- OpenSSH provides a myriad of secure tunneling capabilities, as well as a variety of authentication methods.
- The OpenSSH suite includes
 - [ssh](#) program which replaces rlogin and telnet
 - [scp](#) which replaces rcp
 - [sftp](#) which replaces ftp
 - [sshd](#) which is the server side of the package
 - and other basic utilities like [ssh-add](#), [ssh-agent](#), [ssh-keysign](#), [ssh-keyscan](#), [ssh-keygen](#) and [sftp-server](#).
 - OpenSSH supports SSH protocol versions 1.3, 1.5, and 2.0.
- O'Reilly's [SSH book](#) by Daniel Barrett and Richard Silverman is an excellent reference.



The SSH Protocol

- Authentication

- Reliably determines someone's identity. If you try to log into an account on a remote computer, SSH asks for digital proof of your identity (key-based or password-based.) If you pass the test, you may log in; otherwise SSH rejects the connection

- Encryption

- Scrambles data so it is unintelligible except to the intended recipients. This protects your data as it passes over the network.

- Integrity

- Guarantees the data traveling over the network arrives unaltered. If a third party captures and modifies your data in transit, SSH detects this fact.

Authentication and Authorization

- Every SSH connection involves two authentications in the following order:
 - Server authentication – the SSH client verifies the identity of the SSH server
 - This ensures the SSH server is genuine, not an imposter, guards against an attacker redirecting the network connection to a different machine
 - User authentication – the SSH server verifies the identity of the user requesting access
- Authorization – occurs after authentication
 - Privileges granted after authentication (after knowing who they are)
 - Controlled at the user account level after SSH login

Use of SSH features

- OpenSSH runs natively on HP-UX and Linux
- HP has provided OpenSSH for Windows
- SSH's most immediately useful features
 - Logging into a remote computer over a secure connection
 - Transferring files between computers over a secure connection
- HP SIM uses the features of SSH to remotely manage target systems, including the CMS as a managed platform
- The HP SIM role-based security either allows or disallows a CMS logged-in user to use CMS tools to managed authorized systems
- HP SIM uses SSH for initiating the CMS SSH client login to managed systems (public key) and execute a command securely

Setup of SSH

- Deploy HP's OpenSSH to the managed devices through HP SIM
- Or, deploy manually and run mxagentconfig from the CMS to connect to the remote Windows system and setup the keys
- Caveat: Windows 2003 has many security changes, see the white paper and release notes to get it setup on Windows 2003 painlessly

Windows & CLI

- Scripting languages
 - Windows Scripting Host (WSH), CScript (jscript too)
 - Perl (<http://www.activestate.com/>)
 - Extended batch commands
- Commands
 - Resource kit (Windows 2000)
 - Built-in commands (Windows 2003)
 - Extended batch commands

Tools in HP SIM

- My Custom Commands
 - Managed through GUI
 - Runs on the CMS
- TDEFs
 - Managed through CLI
 - Can run on the CMS or the managed device
 - Can be restricted per user per device
 - Part of an authorization
 - 3 types of tools: web-launch, CLI, and X Windows tool

CLI for Tools

- mxtool
 - Main command to import, export, and modify tools
 - mxtool -a : add a tool
 - mxtool -l : export a tool
 - mxtool -m : modify a tool
 - mxtool -r : remove a tool
 - -f <filename> - works with any of the command to read/write to a file (easiest way to work with mxtool)

MXTOOL – XML file

- XML file – web-launch tool

```
<?xml version="1.0" encoding="UTF-8" ?>
<tool-list>
  <web-launch-tool name="WebJetAdmin" max-targets="1">
    <category>Local Tools</category>
    <description>View printer via WebJetAdmin.</description>
    <execute-as-user>root</execute-as-user>
    <toolbox-enabled value="true" />
    <include-filter type="hardware">
      <node-filter name="DeviceType" operator="eq"
value="Printer"/>
    </include-filter>
    <web-block accepts-targets="true">
      <main-url>http://rook:8000/device/%n/</main-url>
    </web-block>
    <attribute name="menu-path">Tools|System
Information</attribute>
    <attribute name="target-frame">WJAFrame</attribute>
  </web-launch-tool>
</tool-list>
```

Terminal Services launch

```
<web-launch-tool name="Terminal Services" max-targets="1">
  <category>Local Tools</category>
  <description>Connect to Terminal Services</description>
  <execute-as-user>root</execute-as-user>
  <toolbox-enabled value="true" />
  <include-filter type="os">
    <node-filter name="OSName" operator="eq" value="WINNT"/>
  </include-filter>
  <web-block accepts-targets="true">
    <main-url> http://hpsim/tswweb/?AutoConnect=1&Server=%n
    </main-url>
  </web-block>
  <attribute name="menu-path">Tools|System Information</attribute>
  <attribute name="target-frame">TSWFrame</attribute>
</web-launch-tool>
```

Systeminfo

```
<ssa-command-tool name="systeminfo">
  <category>General Tools</category>
  <description>Return Windows system information.</description>
  <execute-as-user>Administrator</execute-as-user>
  <toolbox-enabled value="true" />
  <include-filter type="os">
    <node-filter name="OSName" operator="eq" value="WINNT" />
  </include-filter>
  <include-filter type="protocol">
    <node-filter name="SSH" operator="ge" value="1.0" />
  </include-filter>
  <ssa-block>
    <command command-type="stdout" log="false">systeminfo</command>
  </ssa-block>
  <attribute name="menu-path">
    Tools|Command Line Tools|Windows
  </attribute>
  <attribute name="i18n-attrs">TOOL,mxtools</attribute>
</ssa-command-tool>
```

Others

- WMIC
 - Enabled Terminal Services (Remote Desktop)
 - List all running processes
 - Configure services startup state (auto, manual, disabled)
- SC
 - Control services (start, stop, pause, etc.)
- List all print jobs
 - Prnjobs.vbs

Example: MBSA

- Microsoft Security Baseline Analyzer
 - MBSACLI
 - Fully functional scan and report on server security status
 - Gets updates on vulnerabilities & patches from Microsoft
 - Sample scripts
 - Used to generate summary report

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:



RECOMMENDED TRAINING VENUE FOR THE
HP Certified Professional

