MRTG used for Basic Server Monitoring

SANS Institute Masters
Presentation by T. Brian Granier

Objectives

- What is MRTG?
- How do I set it up?
- What tools do I use to pull SNMP data?
- What minimum information should I monitor about servers?
- How do I monitor this information on a Windows platform?

What is MRTG?

- The Multi Router Traffic Grapher
  - Originally designed as a tool to monitor and graph router statistics
- SNMP was the first, but is not the only method to feed it information
- Designed to monitor 2 targets per graph
- http://www.mrtg.org
- http://www.rrdtool.org

How do I setup MRTG?

- Can run on Windows or *nix based operating systems
- Performance issues running on Windows
- Well documented on the MRTG website
  - Windows: IIS/ActivePerl/MRTG
  - *nix: Apache/gcc/perl/gd/libpng/zlib/mrtg
- http://www.giac.org/certified_professionals/practicals/GCUX/0227.php
- Configuring the targets is typically done by copying and modifying “templates”
  - Relaunch mrtg after config changes are made

What tools do I use to pull SNMP data?

- snmpget

Usage: snmpget [-Cf] [options...] <hostname> {<community>} [<objectID> ...]

- snmpwalk

Usage: snmpwalk [options...] <hostname> {<community>} [<objectID>]

- *nix and Windows versions available
  - http://net-snmp.sourceforge.net/
- Various GUI based tools exist for SNMP browsing

What minimum information should I monitor about servers?

- Disk Space Used
- Memory Utilization
- CPU Utilization
- Network Utilization

SNMP-Informant

- Configure the Windows SNMP Service
- Windows built-in SNMP functionality has been historically problematic for MRTG
  - SNMP-Informant resolves this issue by extending the operating systems SNMP functionality
- “Stationary” OIDs
- FREE for the basic agent
  - Advanced agents, for a price, gives access to even more information
- http://www.snmp-informant.com/

Monitoring Setup – Disk Information

- diskperf –y
  - Requires a reboot
- The Command:

snmpwalk <ip address> <community name> .1.3.6.1.4.1.9600.1.1.1.1.1

- Example Output:

enterprises.9600.1.1.1.1.1.2.**67.58** = "C:"

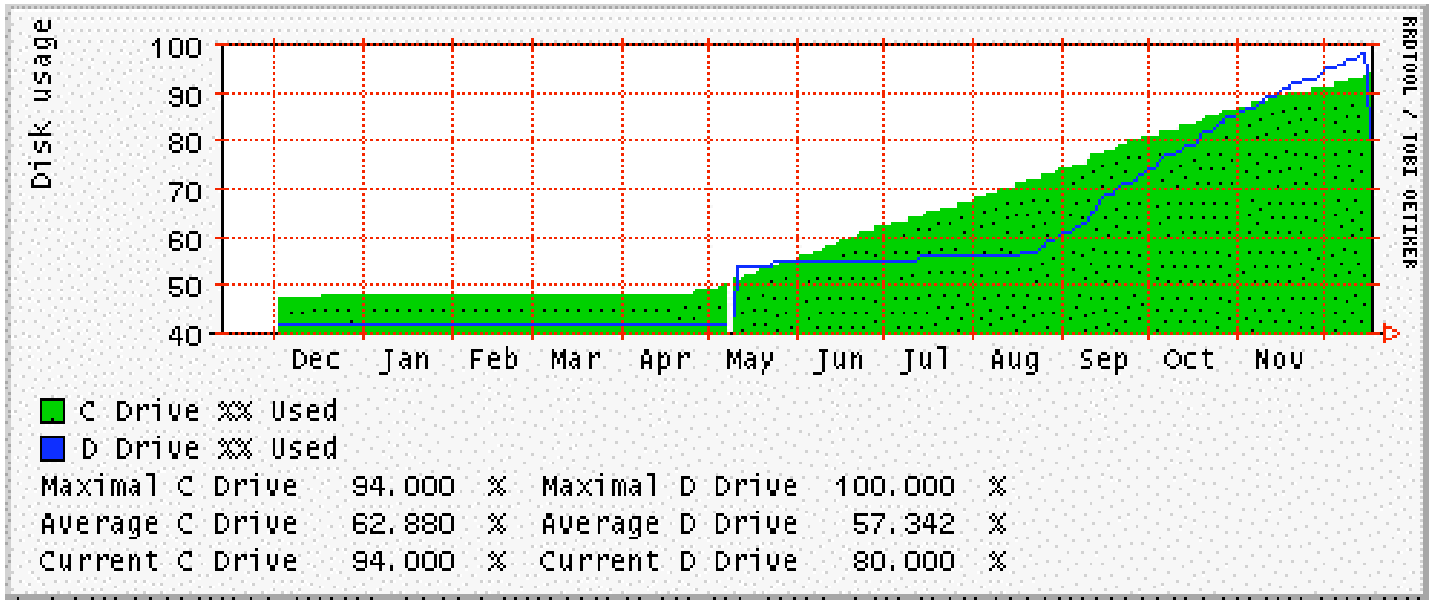
enterprises.9600.1.1.1.1.1.2.**68.58** = "D:"

enterprises.9600.1.1.1.1.1.2.**69.58** = "E:"

enterprises.9600.1.1.1.1.1.6.95.84.111.116.97.108 = "_Total«

Disk Utilization – What to look for

- The primary purpose of monitoring disk space is to predict when a system will run out of space



Monitoring Setup – Memory Utilization

- Commands:

snmpget <ip address> <community> .1.3.6.1.4.1.9600.1.1.2.4.0

snmpget <ip address> <community> .1.3.6.1.4.1.9600.1.1.2.1.0

- Command 1 Example Output:

enterprises.9600.1.1.2.4.0 = Gauge32: **787484672**

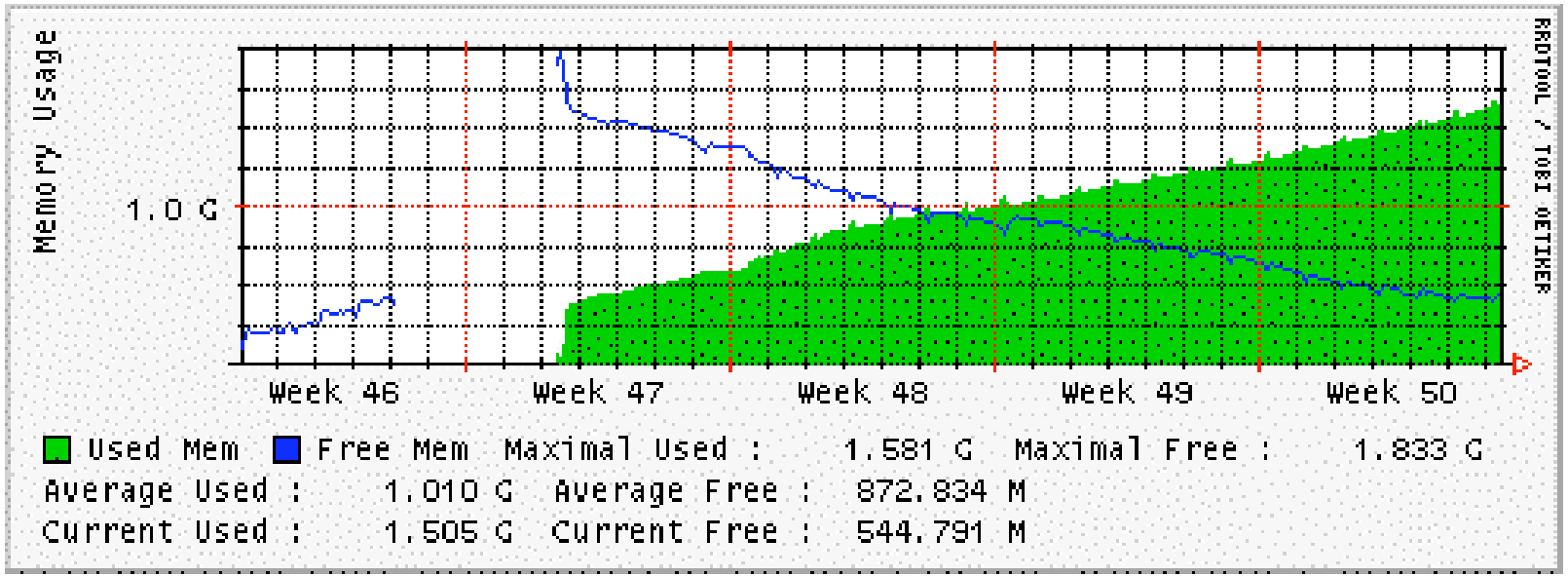
- Command 2 Example Output:

enterprises.9600.1.1.2.1.0 = Gauge32: **220704768**

- Added results represents physical memory plus used virtual memory

Memory Utilization – What to look for

- Identifies systems that need more memory
- Even more useful in identifying systems with memory leaks



Monitoring Setup – CPU Utilization

- The Command:

snmpwalk <ip address> <community> .1.3.6.1.4.1.9600.1.1.5.1.1

- Example Output:

enterprises.9600.1.1.5.1.1.1.**48** = "0"

enterprises.9600.1.1.5.1.1.1.**49** = "1"

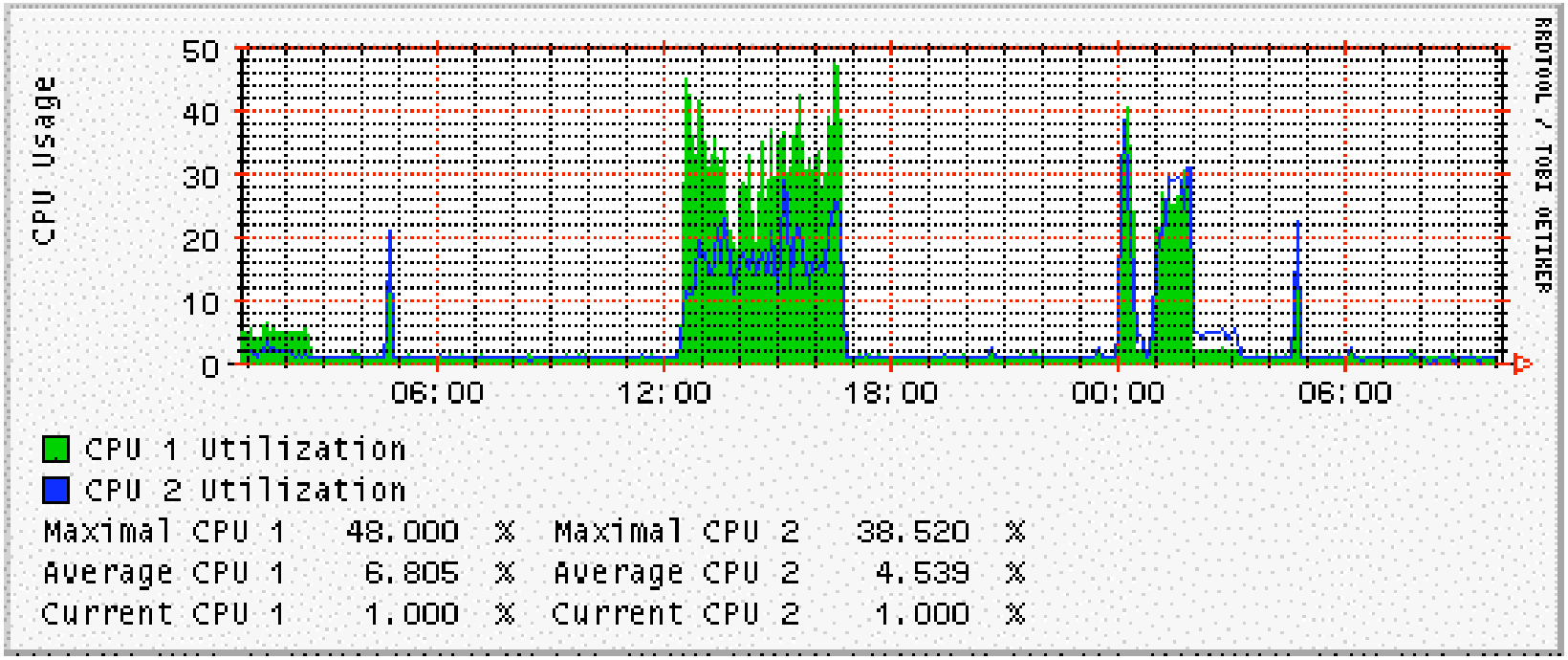
enterprises.9600.1.1.5.1.1.1.**50** = "2"

enterprises.9600.1.1.5.1.1.1.**51** = "3"

enterprises.9600.1.1.5.1.1.6.95.84.111.116.97.108 = "_Total"

CPU Utilization - What to look for

- Determine if more processor power is needed
- Establish processing baseline



Monitoring Setup – Network Utilization

- The Command:

snmpwalk <ip address> <community> .1.3.6.1.4.1.9600.1.1.3.1.1

- Example Output:

enterprises.9600.1.1.3.1.1.**20.73.110.116.101.108.91.82.93.32.80.82.79.32.65.100.97.112.116.101.114** = "Intel[R] PRO Adapter"

enterprises.9600.1.1.3.1.1.**22.73.110.116.101.108.91.82.93.32.80.82.79.32.65.100.97.112.116.101.114.35.49** = "Intel[R] PRO Adapter#1"

enterprises.9600.1.1.3.1.1.**25.77.83.32.84.67.80.32.76.111.111.112.98.97.99.107.32.105.110.116.101.114.102.97.99.101** = "MS TCP Loopback interface"

MRTG used for Basic Server Monitoring Summary

- Setup an MRTG Server
- Prepare a System for monitoring
  - diskperf –y
  - Configure SNMP
  - Install SNMP-Informant
- Modify templates and launch MRTG