Open source tools

Dr.G.Usha Devi
Associate Professor
School of Information Technology and Engineering
VIT University
Vellore

Open source tools

- SNMP - The Simple Network Management Protocol is the standard for remote administration of network devices.
- MRTG - The Multi Router Traffic Grapher is a very widely used tool for graphing bandwidth and other network statistics.
- Neo - This tool was written at MIT for high-level administration of switches, routers, and other devices that speak SNMP.
- NetFlow - NetFlow is a Cisco mechanism for collecting information about the internals of network traffic.
- Oak - Oak is a tool written at MIT for collecting syslog messages from servers and network equipment, condensing the information as appropriate, and notifying operators of problem conditions when they arise.

Open source tools

- Service Monitoring.
  - The Sysmon program, tests network hardware and server software to ensure they are functioning, and if they are not, it notifies the appropriate administrators.
  - The Nagios program, a more complex tool that serves the same purpose, is briefly discussed as well.
- Tcpdump - This is a standard program for directly analyzing network traffic at the packet level.
- Basic Tools - covers the basic tools of network administration, including the ping, telnet, netcat, traceroute, MTR, and netstat programs.
- Custom Tools - working knowledge of the Bourne shell and Perl scripting languages is presented.

Environment

- Solaris
- Linux
- Windows
- MacOS

Background

- understanding of the basics of networking
- OSI layered network model

Terminology and Conventions

- workstation, host, device, and node are all used interchangeably in networking

Sysmon

What's Sysmon ?

- tool to monitorise the state of one or more computers. It's based on a daemon and a php script.
- The first has to be runned in all boxes you need to check, the second calls the daemon and prints the state into a nice web frontend.
- The sysmond functions can be easily expanded by writing modules.

Installation Of Sysmon

- http://www.sysmon.org/

  gunzip -c sysmon-0.91.17.tar.gz | tar xvf –
  cd sysmon-0.91.17
  ./configure
  cd src
  make

- sysmon and sysmond are present

  file sysmon

- Sysmon:ELF 32-bit MSB executable SPARC Version 1, dyn…

  file sysmond

- sysmond: ELF 32-bit MSB executable SPARC Version 1, dyn…
- By default, it will place the sysmon and sysmond programs in /usr/local/bin/:

  make install

Using Sysmon

- **Starting the Sysmon Daemon**
  - root privileges needed
  - Before starting the Sysmon daemon, you will need to create a configuration file
  - Place the following in /usr/local/etc/sysmon.conf

```
root="server";
 config showupalso;
 config statusfile text  "/var/tmp/status.txt";
 object server
 {
 ip  "server.example.com";
type ping;
 contact "admin@example.com"; };
```

- start the daemon with:

  /usr/local/bin/sysmond

  sysmond:15:25:36 Starting System Monitor version v0.91.17

  System Monitor version v0.91.17

  /usr/local/bin/sysmond started on server.example.com

  forked process as pid 7467

- Once Sysmon is up and running, you can check the status of monitored devices by looking at /var/tmp/status.txt, whose path was specified in the configuration file:

  cat /var/tmp/status.txt

Network Summary System Monitor version v0.91.14

Hostname	Type	Port	DownN	UpN	NotifiedStat	Time	Failed
server	ping	0	0	220	No	up	Never

- **Stopping the Sysmon Daemon**

  /usr/local/bin/sysmond stop

  sysmond: 15:35:33 sending signal 15 to sysmond process 7467

Pausing &resuming Sysmon

- to temporarily stop functioning and then resume later with the pause and resume commands:

/usr/local/bin/sysmond pause

sysmond: 15:37:15 sending signal 17 to sysmond process 7486

/usr/local/bin/sysmond resume

sysmond: 15:37:19 sending signal 17 to sysmond process 7486

Reloading the Configuration

/usr/local/bin/sysmond reload

sysmond: 19:07:23 sending signal 1 to sysmond process 7486

sysmond: 19:07:23 Done reloading new config file

- If the configuration is not valid, the process will continue to run with the old configuration. Otherwise, the new configuration will take effect.

Connecting with a Remote Client

- Sysmon runs a TCP service on port 1345 where it provides data about monitored services.

/usr/local/bin/sysmon server.example.com

```
Server: server Current Time: Apr 7 18:22:57 2003

Hostname  Type  Port  Count  Notif  Stat  Time  Failed
-------------------------------------------------------------
www.example.com www  80  66  Yes  Conn  Ref
          Never
-------------------------------------------------------------
q = quit   space = refresh   h = help
```

Other Runtime Options

/usr/local/bin/sysmond –help

Usage: /usr/local/bin/sysmond [-f config-file] [-n] [-d] [-v] [-t] [-p port] [reload] -b : IP Address to listen on -f config-file : Alternate config file location DEFAULT: /usr/local/etc/sysmon.conf

-n : Don't do notifies

-d : Don't fork

-i : Disable ICMP

-v : Print version then exit

-w : Toggle warning messages

-D : Toggle debug messages

-M : Toggle memory debugging

-t : Test/check config file then exit

-p # : Change port number listening on (0 to disable)

-q : Quiet

-l : do not syslog

reload : Test/check config file, and if it passes …

pause : Suspend/resume monitoring (SIGUSR2)

resume : Suspend/resume monitoring (SIGUSR2)

stop : End monitoring and quit (SIGTERM)

Configuring Sysmon

- **Objects and Dependencies**
  - add to the configuration other objects to be monitored
  - Start by adding a simple ping test for the router that server.example.com is connected to:

```
object router1
 {
 ip "192.0.2.5";
 type ping;
desc "Router1";
dep "server";
contact "admin@example.com";
};
```

Setting the Test Type

- **Sysmon Test Types**

Test	Function	Options
ping	standard ping test	
pop3	working POP3 server	username, password
tcp	generic listening TCP port	port
udp	generic listening UDP port	port
radius	working radius server	username, password, secret
nntp	listening news server	
smtp	listening mail server	
imap	listening IMAP server	
x500	listening x500 directory server	
www	listening web server	url, urltext
sysmon	running remote sysmon server	

Example

```
object web-server {
     ip "www.example.com";
     type www;
     desc "Main Web Server";
     dep "router1";
     url "http://www.example.com/";
     urltext "<TITLE>";
     contact "admin@example.com";
          };
```

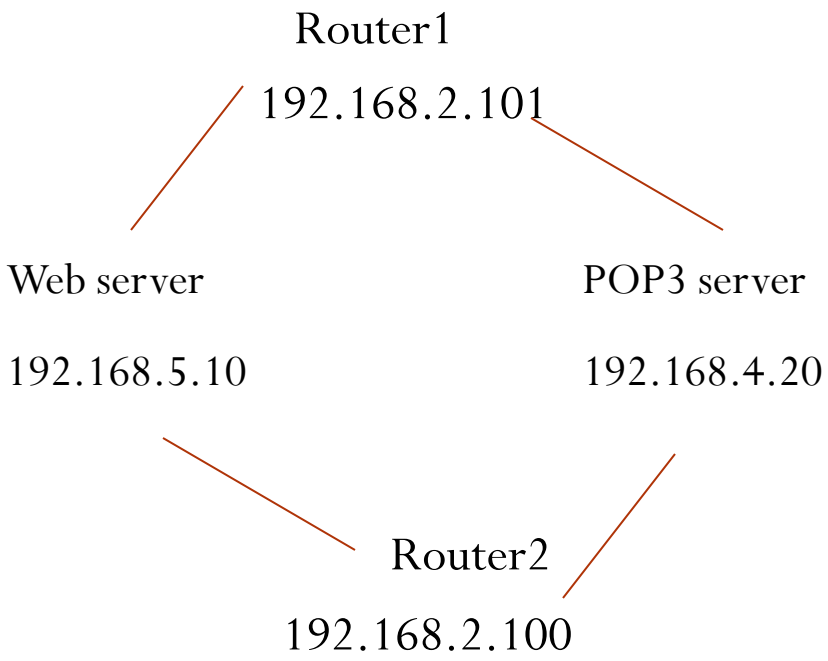
- This tests the URL http://www.example.com/
- If the page is not loadable or does not contain the text <TITLE>, the test will fail.

Example

```
object server1
  {
  ip "server1.example.com";
  type ping; desc "Server 1";
  dep "router1-servernet";
  dep "router2-servernet";
  contact "admin@example.com";
   };
```

Exercise

Create the sysmon configuration file for the following network.



Using the Spawn Option

- Email is not always the best way to notify an administrator of a critical problem.
- It is preferable to send critical notifications via some other mechanism, such as a direct message to a pager or cell phone.
- spawn command will execute a program of your choosing when notification needs to be sent for an object.
- Sysmon has a number of "replacement" variables that will translate to different pieces of Sysmon information.
- For example, %H is replaced with the DNS name of the host being monitored, %s is the name of the service, and %U is the state of the service, either "up" or "down."

spawn "/var/tmp/notify.sh %H %s %U";

Sysmon Replacement Variables

Var	Replacement
%m	local host name
%H	DNS name of host being monitored
%s	Service
%p	port number (numeric)
%T	Current Time hh:mm:ss
%t	Current Time mm dd hh:mm:ss
%d	Downtime dd:hh:mm
%D	Downtime with seconds dd:hh:mm:ss
%i	Unique ID for outage
%I	IP of host down
%w	warning/what
%u	error-type converted into string describing it
%h	hostname with failure
%r	reliability percentage
%V	Verbose History (not implemented)
%c	Failure iteration count (since last success)
%C	Success iteration count (since last failure)
%U	Service state (as 'up' or 'down')

Global Options

- **The Status File**
  - When the Sysmon daemon is running, it will periodically write a file with the status of services that it is monitoring
- Use the config statusfile option to direct Sysmon to write the file:

config statusfile html /usr/local/apache/htdocs/sysmon.html";

config statusfile text "/var/tmp/status.txt";

config html refresh 30;

- **Viewing Both Up and Down Services**
  - The status file will print a list of services that are not responding, but if you would like it to also include those services that are responding, use the showupalso option:

config showupalso;

Mail Header Options

- Sysmon sends mail messages with a from address of "root" at the server the software is running on
- You can change this and other mail headers in the global configuration:

```
config from "admin@example.com";
config replyto "admin@example.com";
config errorsto "errors@example.com";
config subject "Sysmon: %H %s %U";
config nosubject;
```

Test Queuing Options

- control how Sysmon processes service tests and notifications

config numfailures 3;

config queuetime 90;

config maxqueued 50;

config pageinterval 20; send a reminder notification every 20 minutes when a service is down.

DNS Options

config dnsexpire 300; expire entries from the cache every 5 minutes.

- Every 10 minutes, Sysmon also sends information about the cache to syslog. This interval can be changed with the dnslog option, in seconds:

  config dnslog 900;

Message Formatting Options

config pmesg "%H %s %U"; to change the default message formatting

Using Variables

```
set network-group = "netops@example.com, joe-pager@example.com";
set network-group-nopage = "netops@example.com";
set web-group = "frank@example.com, jill@example.com;
object router5 {          ip "router5-backbone.example.com";
                          type ping;  desc "Router 5 Backbone";
                          dep "server";
                          contact "$network-group"; };
object web-ping {         ip "www.example.com";
                          type ping;  desc "Web Server Ping";
                          dep "server";
                          contact "$network-group-nopage"; };
object web-server { ip "www.example.com";
                          type www;  desc "Main Web Server";
                          dep "web-ping";
                          url "http://www.example.com";
                          urltext "<TITLE>";
                          contact "$web-group"; };
```

Using Includes

- It will be easier to maintain if you break it down into smaller files

include "/usr/local/etc/sysmon.webservers.conf";

Maintaining Sysmon

- The toughest part of maintaining Sysmon is **keeping your configuration** in check with reality, especially if you have a large installation or if the people who are deploying equipment are not the same ones who will be updating the config.

Reference

- Open Source Network Administration by James Kretchmar, Prentice Hall