ISPadmin

by Robert Haskins

Robert D. Haskins is currently employed by Renesys Corporation in Hanover, NH.

rhaskins@usenix.org

In this edition of ISPadmin, I look at how ISPs monitor the systems and networks that provide services to their customers. Let me start off by stating that I am employed by Renesys Corporation, which has a product described in this article.

Why Monitor?

There are many reasons for an ISP to monitor systems and networks:

- Troubleshooting: Monitoring systems is very helpful in troubleshooting problems quickly.
- Capacity planning: Historical graphs make capacity planning easier.
- Product differentiation: More information helps customers, making them more likely to use your services.
- Security: Monitoring helps spot potential security problems sooner rather than later.
- Documentation: In order to monitor, you must know what systems and networks are in place.

Background

Even for the smallest service providers, monitoring tends to be a highly customized activity. By that I mean each service provider's situation is unique, and each monitoring system must meet a diverse set of circumstances. Some of these parameters include:

- Number and type of services offered
- Number and type of customers
- Service level agreements in effect
- Complexity of back-end systems and networks
- Internal processes and procedures
- Reporting requirements

Each one of these parameters is covered in the following sections.

Services Offered

The more types of services that are offered, the more complex the monitoring system needs to be. Each service will require some level of monitoring, though the level can vary widely depending upon the complexity.

Customers

If a service provider sells mostly to commercial entities, it is possible their customers *might* directly monitor (a subset of) the provider's services. If the customer base is largely residential/individuals, then monitoring will be more focused on providing tools to an NOC or customer/technical support call center.

Service Level Agreements

If a service level agreement (SLA) is in effect, it might specify exactly how the provider is to monitor their network. Often SLAs specify what level of quality of service (QoS) a provider must achieve. The only way to measure the QoS is to have some sort of monitoring. SLAs also might stipulate that a customer may directly monitor a provider's services. Examples of such monitoring would be SNMP-based monitoring of equipment/systems.

Complexity

This is probably the biggest variable that dictates how a monitoring system is deployed. The more intricate the system/network is, the more complex the monitoring system will be.

Internal Processes

Internal processes will to some degree dictate the monitoring required. For example, if management wants to be made aware when a certain event or problem occurs, then monitoring systems must be in place to handle these occurrences.

Reporting Requirements

Reporting requirements will also necessitate that certain monitoring occurs. For example, if a dial-up provider wants to determine the need to add lines at each point of presence (POP), then the number of calls at each POP must be tracked over time. Similarly, the utilization of all high-speed lines on a provider's network should be tracked, so that additional capacity can be added when needed. In some cases, the information used for monitoring can also drive the service provider's billing systems. For example, Cisco's Netflow application built into their IOS device software can be used for both monitoring and billing.

Wes Cottrell of the Stanford Linear Accelerator Center (SLAC) has an outstanding page listing a wide array of network-monitoring tools. The URL is in the Resources section at the end of this article.

Protocols

With monitoring, the services being monitored must send their results across the network. There are a number of ways to accomplish this transfer. Some of the more common mechanisms/protocols used in monitoring are Simple Network Management Protocol (SNMP), finger, ICMP (ping and traceroute), Remote Monitoring (RMON, a subset of SNMP), and Cisco Netflow.

Of course, many tools have their own customary way of reporting results. For example, Nagios uses the Nagios Remote Plugin Executor to perform certain system checks and to allow administrators to write their own custom plugins.

Software

Both commercial software and good open source software are available for monitoring networks. For the purposes of this article, the available monitoring software is broken down into two categories: network-monitoring platforms and stand-alone products.

Network-monitoring platforms are frameworks that enable management of many different types of devices. Often, they are described as the "manager of managers." Perhaps the most well known of these types of applications is HP Openview. These systems, all by themselves, have little functionality. Applications like Openview are very useful in managing agents specifically designed to run with them or with agents based on open protocols such as SNMP.

Unless it is a service provider with very deep pockets, most will not be able to afford a commercial network-monitoring platform. These systems cost thousands to millions of dollars to acquire and deploy. If a provider does need functionality like Openview but doesn't have a ton of money, they might use the open source product OpenNMS,

which is a freely available network-monitoring platform. It is written in Java, and can be quite daunting to set up and run successfully.

Some of the better-known commercial products in the network-monitoring platform category include SNMPc by Castle Rock, IBM's Tivoli Netview, HP Openview, and Micromuse NetCool.

A common lower-end commercial tool used by ISPs is Ipswitch's WhatsUp Gold. This does an acceptable job of monitoring smaller- and medium-sized networks, up to about 1000 devices, though there is no set maximum. One downside is that WhatsUp Gold runs only under Microsoft Windows.

In the stand-alone area, many tools are available. These range from the likes of ICMP ping and traceroute, all the way up to products like Gradus from Renesys, which is useful in managing exterior border gateway protocol (BGP)-based networks.

Open Source Software

The vast majority of providers utilize free monitoring tools, which might include monitoring, graphing, and traffic-analysis packages.

Monitoring

Of the large number of open source monitoring packages, the most widely deployed is Nagios, but some other packages that could be used include SNIPS (formerly NOCOL), MON, Big Brother, and MIDAS NMS.

These systems all do basic ICMP ping monitoring and save some sort of history. Some also do graphing and SNMP monitoring, which might save an ISP from having to deploy a separate graphing system such as Cricket.

Nagios

Since Nagios is one of the most commonly used monitoring packages out there, it is useful to look at it in detail. I use Nagios 1.1 for the purposes of this article, but 1.2 is now available. Besides being Web-based, Nagios's features include:

- Ability to monitor both network attributes and system services
- User-definable system and service checks
- Escalation
- Acknowledgment of problems via Web interface
- Redundant configuration
- History of events
- Reporting

It would be useful to define the following terms in Nagios's nomenclature before covering the details of what Nagios can do.

- Hosts – any device Nagios monitors (router, switch, server, etc.)
- Hostgroups – collections of hosts that are related in some way
- Contacts – people who get notified when an event happens
- Contactgroups – sets of people who are collectively responsible for services
- Services – individual applications monitored on hosts (Web, DNS, FTP, etc.)

Nagios will monitor the services you define, and keep a history to enable reporting service level agreements and other benchmarking. It has the ability to call programs on remote machines via the Nagios Remote Plugin Executor. This functionality is very

RESOURCES

SLAC's Network Monitoring Tools by Les Cottrell
http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html

SNMP starting point
http://www.snmplink.org/

Another good SNMP reference
http://www.simpleweb.org/

Cisco Netflow
http://www.cisco.com/warp/public/732/Tech/nmp/netflow/netflow_nms_apps_part.shtml

HP Openview
http://www.openview.hp.com/

Sun Solstice Domain Manager (formerly Sun Net Manager)
http://wwws.sun.com/software/solstice/dm/

IBM Tivoli Netview
http://www-306.ibm.com/software/tivoli/products/netview/

WhatsUp Gold
http://www.ipswitch.com/products/whatsup/index.html

SNMPc from Castle Rock
http://www.castlerock.com/

NetCool from Micromuse
http://www.micromuse.com/products_sols/index.html

OpenNMS
http://www.opennms.org/

Nagios
http://www.nagios.org/

CAIDA's cflowd
http://www.caida.org/tools/measurement/cflowd/

SNIPS
http://www.navya.com/snips/

MON
http://www.kernel.org/software/mon/

MIDAS NMS
http://midas-nms.sourceforge.net/

useful, as Nagios can easily be customized to monitor things that are not built into it by default.

Nagios Options

The left-hand side of all Nagios screens always displays the options available. This section goes over some of the more useful Nagios options available.

The "Tactical Overview" screen shows the overall status of Nagios itself, as well as the hosts and services it is monitoring. It is a nice summary of everything within Nagios. I personally find myself viewing the "Service Detail" screen the most. This screen is one big table with the hosts in alphabetic order, with each host listing services, one per line. If you want to see the status of every service you are monitoring, use this.

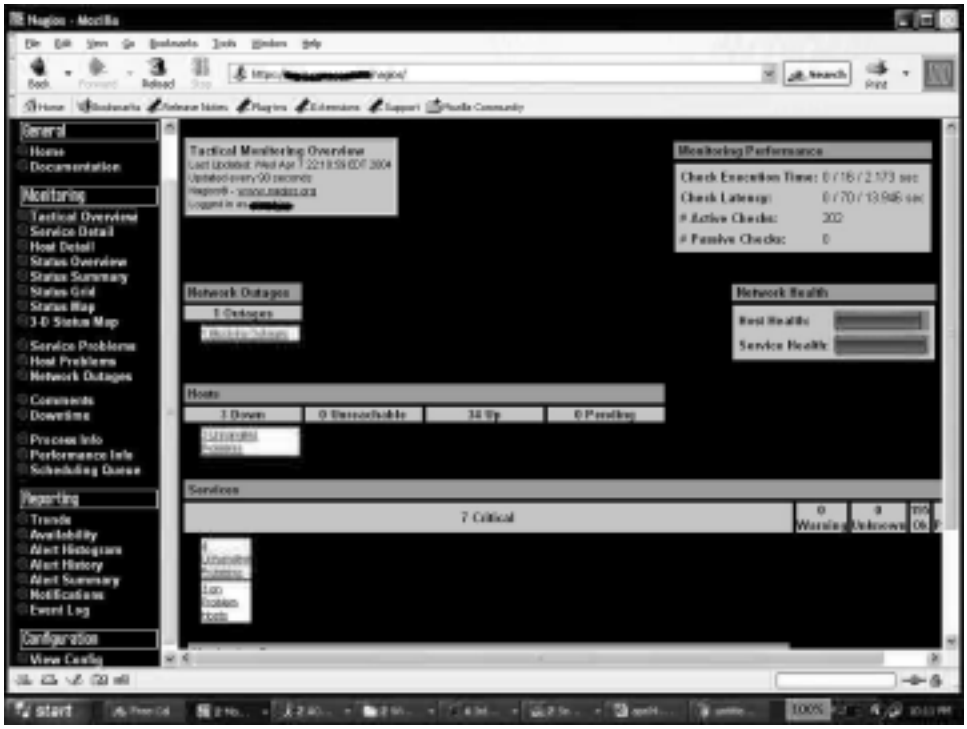
"Host Detail" lists every host's ping status. The "Status Overview" shows the various host groups defined. Each host's set of service-status details can be displayed by clicking on the individual hostname. "Status Map" can be used to graphically show the dependencies between various hosts and is probably most useful for displaying large networks of routers and similar devices. "Service Problems," "Host Problems," and "Network Outages" show the various classifications of items that are currently in alarm.

Nagios allows users to enter comments regarding services. These are used to communicate information about services. "Comments" displays the comments that have been entered for a given service. Nagios also allows users to put services into downtime. "Downtime" lists the services that have been put into downtime and which are not being currently monitored.

Reports

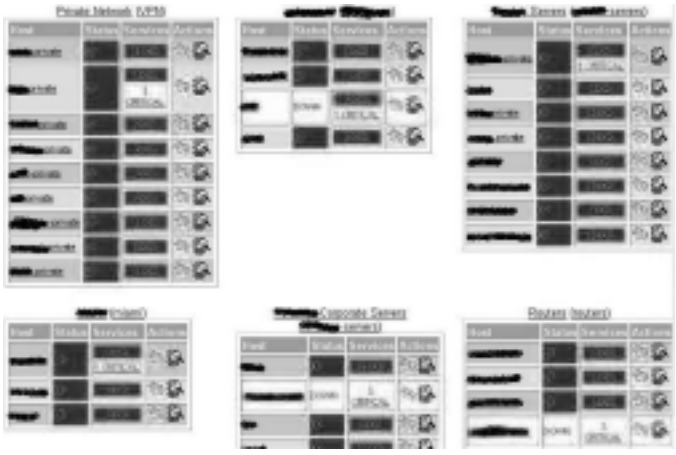
Nagios keeps a history of all services it has monitored. This history can be used to generate reports and statistics for things like mean time between failures and service level agreements. Nagios can graph data over time as well: for example, ping times and alerts via the "Trends," "Availability," and "Alert Histogram" functions. The configuration can also be viewed by clicking on the "View Config" option. Note that the configuration options must be adjusted by editing files (located by default in /etc/nagios) and cannot be managed through the Web GUI.

Next time, I will look at an rrdtool-based graphing package, as well as a couple of network-specific monitoring tools.



Tactical Overview screen

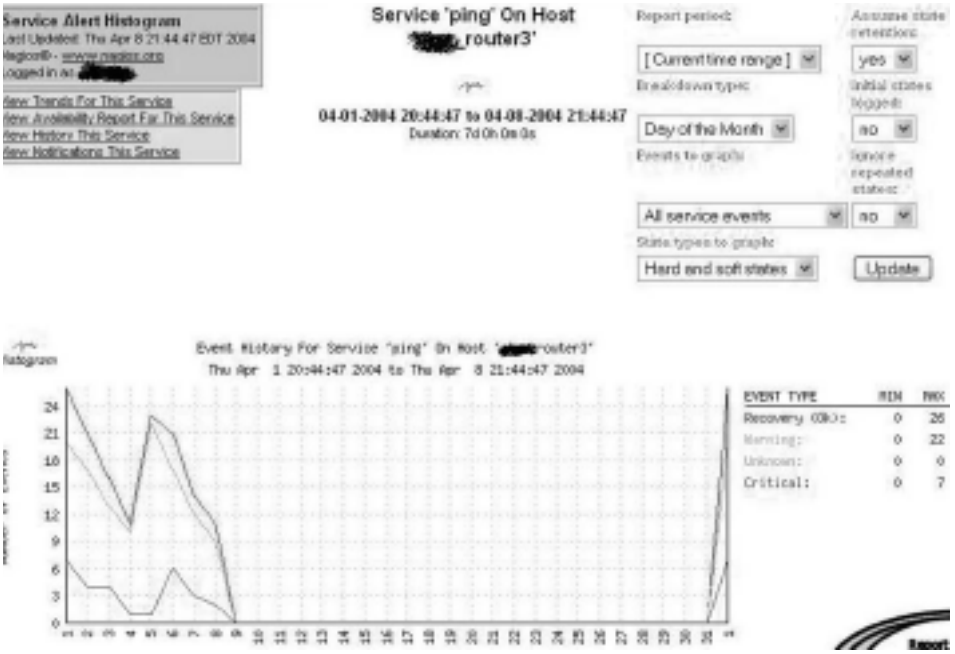
Service Details screen (partial)



Host Details screen (partial)

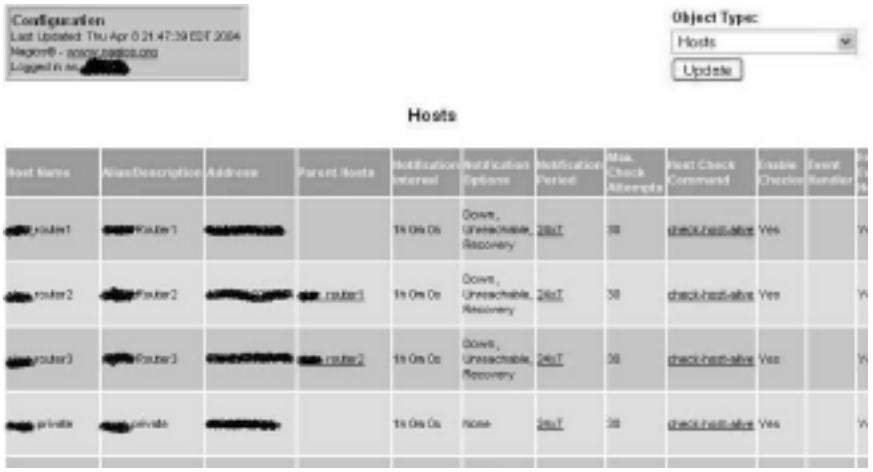
Status Map screen (partial)

Service Overview screen (partial)



Service Problems screen (partial)

Hosts Problems screen (partial)



Network Outages screen (partial)