

Open Source Management Options

September 30th, 2008

Jane Curry

Skills 1st Ltd

www.skills-1st.co.uk

Jane Curry Skills 1st Ltd 2 Cedar Chase Taplow Maidenhead SL6 0EU 01628 782565

jane.curry@skills-1st.co.uk

Synopsis

Nuts and bolts network and systems management is currently unfashionable. The emphasis is far more on processes that implement *service management*, driven by methodologies and best practices such as the Information Technology Infrastructure Library (ITIL). Nonetheless, all service management disciplines ultimately rely on a way to determine some of the following characteristics of systems and networks:

- Configuration management
- Availability management
- Problem management
- Performance management
- Change management
- Security management

The commercial marketplace for systems and network management offerings tend to be dominated by the big four – IBM, HP, CA and BMC. Each have large, modular offerings which tend to be very expensive. Each has grown their portfolio by buying up other companies and then performing some level of integration between their respective branded products. One can argue that the resulting offerings tend to be "marketechtures" rather than architectures.

This paper looks at Open Source software that addresses the same requirements. Offerings from Netdisco, Cacti and The Dude are examined briefly, followed by an indepth analysis of Nagios, OpenNMS and Zenoss.

This paper is aimed at two audiences. For a discussion on systems management selection processes and an overview of three main open source contenders, read the first few chapters. The last few chapters then provide a product comparison.

For those who want lots more detail on Nagios, OpenNMS and Zenoss, the middle sections provide in-depth discussions with plenty of screenshots.

Table of Contents

1	Defining "Systems Management"	5
	1.1 Jargon and processes	5
	1.2 "Systems Management" for this paper	6
2	Systems management tools	6
	2.1 Choosing systems management tools	7
	2.2 The advantages of Open Source	8
3	Open Source management offerings	8
4	Criteria for Open Source management tool selection	.10
	4.1 General requirements	.10
	4.1.1 Mandatory Requirements	.10
	4.1.2 Desirable Requirements	.10
	4.2 Defining network and systems "management"	.11
	4.2.1 Network management	.11
	4.2.2 Systems management	.12
	4.3 What is out-of-scope?	.13
5	A quick look at Cacti, The Dude and netdisco	.14
	5.1 Cacti	.14
	5.2 netdisco	.17
	5.3 The Dude	.20
6	Nagios	.21
	6.1 Configuration – Discovery and topology	.22
	6.2 Availability monitoring	.27
	6.3 Problem management	.32
	6.3.1 Event console	.33
	6.3.2 Internally generated events	.37
	6.3.3 SNMP TRAP reception and configuration	.39
	6.3.4 Nagios notifications	.39
	6.3.5 Automatic responses to events – event handlers	.41
	6.4 Performance management	.42
	6.5 Nagios summary	.45
7	OpenNMS	.46
	7.1 Configuration – Discovery and topology	.47
	7.1.1 Interface discovery	.47
	7.1.2 Service discovery	.48
	7.1.3 Topology mapping and displays	.51
	7.2 Availability monitoring	.53
	7.3 Problem management	.59
	7.3.1 Event console	.59
	7.3.2 Internally generated events	.62
	7.3.3 SNMP TRAP reception and configuration	.65
	7.3.4 Alarms, notifications and automations	.69

7.4 Performance management	76
7.4.1 Defining data collections	76
7.4.2 Displaying performance data	85
7.4.3 Thresholding	91
7.5 Managing OpenNMS	97
7.6 OpenNMS summary	98
8 Zenoss	98
8.1 Configuration – Discovery and topology	
8.1.1 Zenoss discovery	
8.1.2 Zenoss topology maps	107
8.2 Availability monitoring	108
8.2.1 Basic reachability availability	
8.2.2 Availability monitoring of services - TCP / UDP ports and wi	ndows services
8.2.3 Process availability monitoring	113
8.2.4 Running commands on devices	120
8.3 Problem management	
8.3.1 Event console	122
8.3.2 Internally generated events	
8.3.3 SNMP TRAP reception and configuration	125
8.3.4 email / pager alerting	126
8.3.5 Event automations	
8.4 Performance management	
8.4.1 Defining data collection, thresholding and graphs	
8.4.2 Displaying performance data graphs	
8.5 Zenoss summary	141
9 Comparison of Nagios, OpenNMS and Zenoss	142
9.1 Feature comparisons	
9.1.1 Discovery	143
9.1.2 Availability monitoring	144
9.1.3 Problem management.	
9.1.4 Performance management	145
9.2 Product high points and low points	146
9.2.1 Nagios "goodies" and "baddies"	
9.2.2 OpenNMS "goodies" and "baddies"	
9.2.3 Zenoss "goodies" and "baddies"	147
9.3 Conclusions.	
10 References	149
11 Appendix A Cacti installation details	

1 Defining "Systems Management"

1.1 Jargon and processes

Every organisation and individual has their own perspective on systems management requirements; the first essential step when looking for systems management solutions is to define what those requirements are. This gives a means to measure success of a project.

There are many different methodologies and disciplines for systems management from the International Standards Organization (ISO) "FCAPS" acronym – Fault, Configuration, Accounting, Performance and Security, through to the Information Technology Infrastructure Library (ITIL) which divides the ITIL V2 framework into two categories:

- Service Support which includes the:
 - Service Desk function
 - Incident management process
 - Problem management process
 - Configuration management process
 - Change management process
 - Release management process
- Service Delivery which includes the:
 - Service Level management process
 - Capacity management process
 - IT Service Continuity management process
 - Availability management process
 - Financial management for IT services

Key to the core of configuration management and the entire ITIL framework is the concept of the Configuration Management Database (CMDB) which stores and maintains Configuration Items (CIs) and their inter-relationships.

The art of systems management is defining what is important – what is in-scope, and perhaps more importantly, what is currently out-of-scope. The science of systems management is then to effectively, accurately and reliably provide data to deliver your systems management requirements. The devil really is in the detail here. A "comprehensive" systems management tool that delivers a thousand metrics out-of-the-box but which is unreliable and / or not easily configurable, is simply a recipe for a project that is delivered late and over-budget.

For smaller projects or Small / Medium Business (SMB) organisations, a pragmatic approach is often helpful. Many people will want a say in the definition of management. Others, whose requirements may be equally valuable, may not know "the art of the possible". Hence, combining top-down requirements definition workshops with a bottom-up approach of demonstrating "top 10" metrics that can easily be delivered by a tool, can result in an iterative process that fairly quickly delivers at least a prototype solution.

1.2 "Systems Management" for this paper

For the purposes of this paper, I shall define systems management as spanning:

- Configuration management
- Availability management
- Problem management
- Performance management

I shall further define "systems" to include local and wide-area networks, as well as "PCs" and "Unix-like" systems. In my environment, I do not have mainframe or proprietary midrange systems. "PC"s run a variety of versions of Windows. "Unix-like" tends to mean a flavour of Linux rather than a vendor-specific Unix, though there is some legacy IBM AIX and Sun Solaris.

2 Systems management tools

There are no systems management "solutions" for sale. The successful implementation of systems management requirements is a combination of:

- Appropriate requirements definition
- Appropriate tools
- Skills to translate the requirements into customisation of tools
- Project management
- User training
- Documentation

In theory, the choice of tool should be driven by the requirements. In practise, this is often not the case and a solution for one aspect of systems management in one area of a business may become the de facto standard for a whole organisation.

There are good reasons why this might come about. It is not practical to run a centralised Service Desk with a plethora of different tools. A Framework-based tool with a centralised database, and a common look-and-feel across both Graphical User Interface(GUI) and Command Line Interface (CLI), offering modules that deliver the different systems management disciplines, is a much more cost-effective solution then

different piecemeal tools for different projects, especially when the cost of building and maintaining skills and educating users is taken into account.

Tool integration is a large factor in the successful rollout of systems management. The concept of a single Configuration Management Database (CMDB) that all tools feed and use, is key to this.

A good tool delivers "useful stuff" easily out-of-the-box and provides a standard way to then provide local customisation.

At its most basic, the "tool" is a compiler or interpreter (C, bash, ...) and the "customisation" is writing programs from scratch. At the complex end of the spectrum, the "tool" may be a large suite of modules from one of the big four commercial suppliers, IBM, HP, CA and BMC. At the *really* complex end, is where you have several of the big commercial products involved in addition to home-grown programs.

2.1 Choosing systems management tools

Every organisation has different priorities for the criteria that drive tool selection. For the moment, let's leave aside the technical metrics and look at some of the other decision factors:

- Ease of use not just what demos well but what implements well in your environment
- Skills necessary to implement the requirements versus skills available
- Requirements for and availability of user training
- Cost all of it not just licences and tin evaluation time, maintenance, training, ...
- Support from supplier and/or communities
- Scalability
- Deployability management server(s) ease of installation and agent deployment
- Reliability
- Accountability the ability to sue / charge the vendor if things go wrong

If accountability is high in your priorities and the software cost is a relatively low priority then you are likely to choose one of the commercial offerings; however if you have a well-skilled workforce, or one prepared and able to learn quickly, and overall cost is a limiting factor, then Open Source offerings are well worth considering. Interestingly, you can find offerings that suit all the other bullets above, from both the commercial and the Open Source stables.

2.2 The advantages of Open Source

One attraction of Open Source to me is that you don't actually have to fund "salesfolk". Some costs do need to be invested in your own people to investigate the offerings available, research their features and requirements, and participate in the online fora that share experience around the globe. These costs may not be small but at least the investment stays within the company and hopefully those people who have done the research will then be a key part of the team implementing the solution. This is often not the case if you purchase from a commercial supplier.

Open Source does not necessarily mean "you're on your own, pal!". Most of the Linux distributions have a free version and a supported version, where a support contract is available to suit your organisation and budget. Several of the Open Source management offerings have a similar model - but do ensure that the free version has sufficient features for your requirements and is not just a well-featured "demo".

All software has bugs in it. Ultimately, if you go Open Source, you have the source code so you have some chance of fixing problems with local staff or buying in global expertise – and that doesn't necessarily mean transporting a guru from Australia to Paris. Open Source code is available to everyone so remote support and consultancy is a distinct possibility. With the best will in the world, commercial organisations will prioritise problem reports according to *their* criteria – not yours.

There are some excellent fora and discussion lists for commercial products - I have participated in several of them for many years; some even have input from the support and development teams; however, the source code is not open for discussion or community development. With a very active Open Source offering, there tends to be a much larger pool of developers and testers (ie. "us") and the chance of getting problems fixed may be higher, even if you cannot fix it yourself. I would emphasise *very active* Open Source offerings – unless you really do have some very highly skilled local staff that you are sure you are going to keep, it may be a risky choice to participate in a small Open Source project.

3 Open Source management offerings

There are lots of different Open Source management offerings available. Many of them rely on the Simple Network Management Protocol (SNMP) which defines both a protocol for an SNMP manager to access a remote SNMP agent, and also defines the data that can be transferred. SNMP data values that an SNMP manager can request, are defined in Management Information Bases (MIBs) which can either be standard (MIB-2) or can be "enterprise-specific" - in other words, each different manufacture can provide different data about different types of device. Information events emanating from an agent (typically problems) are SNMP traps. There are three versions of the SNMP standard:

• V1 (1988) – still most prevalent. Significant potential security and performance issues.

- V2 (1993) solved some performance issues. Never reached full standard status.
- V3 (2002) significantly improved performance and security issues. Much more complex.

Of the Open Source management solutions available, some are excellent point solutions for specific niche requirements. MRTG (Multi Router Traffic Grapher) written by Tobi Oetiker, is an excellent example of a compact application that uses SNMP to collect and log performance information and display it graphically. If that satisfies your requirement, don't look any further – but it will not help you with defining and collecting problems from different devices and then managing those problems through to resolution.

An enhancement of MRTG is RRDTool (Round Robin Database Tool), again from Tobi Oetiker. It is still fundamentally a performance tool, gathering periodic, numeric data and displaying it but RRDTool has a database at its heart. The size of the database is predetermined on creation and newer data overwrites old data after a predetermined interval. RRD can be found embedded in a number of other Open Source management offerings (Cacti, Zenoss, OpenNMS).

A further enhancement from RRDTool is Cacti which provides a complete frontend to RRDTool. A backend MySQL relational database can be used behind the Round Robin databases; data sources can be pretty-well any script in addition to SNMP; and there is user management included. This is still a performance data collection and display package, not a multi-discipline, framework, systems management solution.

Moving up the scale of features and complexity, some offerings are slanted more towards network management (netdisco, The Dude); others towards systems management (Nagios).

Some aim to encompass a number of systems management disciplines with an architecture based around a central database (Nagios, Zenoss, OpenNMS).

Some are extremely active projects with hundreds of appends to maillists per month (Nagios, Zenoss, OpenNMS, cacti); others have a regular but smaller community with hundreds of maillist appends per year (netdisco).

Some are purely Open Source projects, typically licensed under the Gnu GPL (MRTG, RRDTool, cacti) or BSD license (netdisco); some have free versions (again typically under GPL) with extensions that have commercial licences (Zenoss). In addition to free licences, several products offer support contracts (Zenoss, Nagios, OpenNMS).

Most are available on several versions of Linux; MRTG, RRDTool and cacti are also available for Windows. The Dude is basically a Windows application but can run under WINE on Linux.

Most have a web-based GUI supported on Open Source browsers. OpenNMS can only display maps by using Internet Explorer.

4 Criteria for Open Source management tool selection

It is essential to define what is in-scope and what is out-of-scope for a systems management project. A prioritised list of mandatory and desirable requirements is helpful.

4.1 General requirements

For the purposes of this paper, here are my selection criteria.

4.1.1 Mandatory Requirements

- Open Source free software
- Very active fora / maillists
- Established history of community support and regular fixes and releases
- Integrated network and systems management including:
 - Configuration management
 - Availability management
 - Problem management
 - Performance management
- Centralised, open database
- Both Graphical User Interface (GUI) and Command Line Interface (CLI)
- Easy deployment of agents
- Scalability to several hundred devices
- Adequate documentation

4.1.2 Desirable Requirements

- Support for SNMP V3
- User management to limit aspects of the tool to certain individuals
- Graphical representation of network
- Controllable remote access to discovered devices
- Easy server installation
- No requirement for proprietary web browsers
- Scalability to several thousand devices
- Good documentation
- Availability of (chargeable) support

4.2 Defining network and systems "management"

The "Integrated network and systems management" requirement needs some further expansion:

4.2.1 Network management

- Configuration
 - Automatic, controllable discovery of network Layer 3 (IP) devices
 - Topology display of discovered devices
 - Support for SNMP V1, V2 and preferably, V3
 - \circ $\,$ Ability to discover devices that do not support ping
 - $\circ~$ Ability to discover devices that do not support SNMP
 - Central, open database to store information for these devices
 - Ability to add to this information
 - o Ideally, ability to discover and display network Layer 2 (switch) topology
- Availability monitoring
 - Customisable "ping test" for all discovered devices and interfaces
 - SNMP availability test for devices that do not respond to ping (eg. comparison of SNMP Interface administrative status with Interface operational status)
 - $\circ~$ Simple display of availability status of devices, preferably both tabular and graphical
 - Events raised when a device fails its availability test
 - Ability to monitor infrastructure of network devices (eg. CPU, memory, fan)
 - \circ $\;$ Differentiation between device / interface down and network unreachable \;
- Problem
 - Events to be configurable for any discovered device
 - \circ Central events console with ability to prioritise events
 - \circ Ability to categorise events for display to specific users
 - $\circ~$ Ability to receive and format SNMP traps for SNMP V1, V2 and preferably, V3
 - $\circ~$ Customisation of actions in response to events, both manual actions and automatic responses
 - Ability to correlate events to find root-cause problems (eg. failure of a router device is root cause of all interface failure events for that device)
- Performance

- Regular, customisable monitoring of SNMP MIB variables, both standard and enterprise specific, with data storage and ability to threshold values to generate events
- Ability to import any MIB
- $\circ~$ Ability to browse any MIB on any device
- Customisable graphing of performance data

4.2.2 Systems management

Many of the criteria for systems management are similar to the network management bullets above but they are repeated here for convenience.

- Configuration
 - Automatic, controllable discovery of Windows and Unix devices
 - Topology display of discovered devices
 - Support for SNMP V1, V2 and preferably, V3
 - $\circ~$ Ability to discover devices that do not support ping
 - \circ $\,$ Ability to discover devices that do not support SNMP $\,$
 - \circ Central, open database to store information for these devices
 - Ability to add to this information
- Availability monitoring
 - Customisable "ping test" for all discovered devices
 - Availability test for devices that do not respond to ping (eg. comparison of SNMP Interface administrative status with Interface operational status, support for ssh tests)
 - \circ Ability to monitor customisable ports on a device (eg. tcp/80 for http servers)
 - Ideally the ability to monitor "applications" (eg. ssh /snmp access to monitor for processes, wget to retrieve web pages)
 - Simple display of availability status of devices, preferably both tabular and graphical
 - \circ $\;$ Events raised when a device fails any availability test $\;$
 - Ability to monitor basic system metrics CPU, memory, disk space, processes, services (eg. the SNMP Host Resources MIB)
- Problem
 - \circ Events to be configurable for any discovered device

- Central events console for network and systems management events with ability to prioritise events
- \circ $\;$ Ability to categorise events for display to specific users
- $\circ~$ Ability to receive and format SNMP traps for SNMP V1, V2 and preferably, V3
- $\circ~$ Ability to monitor Unix syslogs and Windows Event Logs and generate customisable events
- Ideally the ability to monitor any test logfile and generate customisable events
- \circ $\,$ Customisation of actions in response to events, both manual actions and automatic responses
- Ability to correlate events to find root-cause problems (eg. single-point-offailure router is root cause of availability failure for all devices in a network)
- Performance
 - Regular, customisable monitoring of SNMP MIB variables, both standard and enterprise specific, with data storage and ability to threshold values to generate events
 - Ability to import any MIB
 - $\circ~$ Ability to browse any MIB on any device
 - $\circ~$ Ability to gather performance data by methods other than SNMP (eg. ssh)
 - Customisable graphing of performance data

4.3 What is out-of-scope?

In my environment, some things are specifically out-of-scope:

- Software distribution
- Remote configuration
- Remote control of devices
- High availability of management servers
- Application response time

In the next few sections of this document I will explore some of the niche products briefly and then take a slightly more in-depth look at OpenNMS, Nagios and Zenoss. These sections are not intended to be a full analysis of the products, more an "initial impressions" and a comparison of strengths and weaknesses. Subsequent documents will investigate Nagios, OpenNMS and Zenoss in more detail.

5 A quick look at Cacti, The Dude and netdisco

Cacti, The Dude and netdisco do not meet my mandatory requirements; however they are interesting niche solutions that were investigated during the tools evaluation process. Cacti and netdisco were installed; The Dude was only Internet-researched.

5.1 Cacti

Cacti is a niche tool for collecting, storing and displaying performance data. It is a comprehensive frontend to RRDTool, including the concept of user management. Although the default method of data collection is SNMP, other data collectors, typically scripts, are possible.

Data collection is very configurable and is driven by the Cacti Poller process which is called periodically by the Operating System scheduler (cron for Unix). The default polling interval is 5 minutes.

Devices need to be manually added using the Cacti web-based GUI. Basic information such as hostname, SNMP parameters and device type should be supplied. Depending on the device type selected (eg. ucd/net SNMP Host, Cisco Router), one or more default graph templates can be associated with a device along with one or more default SNMP data queries. In addition to the web-based GUI, configuration of Cacti can be done by Command Line, using PHP which is a general-purpose scripting language especially suited for web development.

Cacti now has support for SNMP V3.

For high-performance polling, Spine (used to be cactid) can replace the base cmd.php polling engine. The user manual suggests that Spine could support polling intervals of less than 60 seconds for at least 20,000 data sources.

Cacti is supported on both Unix and Windows platforms.

Get the Cacti User Manual from http://www.cacti.net/downloads/docs/pdf/manual.pdf.

Cacti has a very active user forum with hundreds of appends per month. There is also a documented release roadmap going forward to 2nd quarter 2009.

Here are a few screenshots of Cacti to give a feel for the product.

🧕 cacti - Mozilla Firefox					_	
<u>File Edit View History Bookmarks Tools H</u> elp						$\langle \rangle$
👍 🕶 🔶 😴 🏠 🚺 http://cacti/cacti/host.php			v			Q
📕 🔚 Firefox Support 💆 Plug-in FAQ 🗁 RSS Feeds						
console graphs					V	1
Console -> Devices				Logged in a	is admin (Lo	ogout)
Create Devices						Add
New Graphs					[go
Management Ally						clear
Management		Showing Pows 1 to	7 of 7 [1]		Novi	~ ~
Graph Trees Description**	Status	Hostname	Current (ms)	Average (ms)	Availabilit	v –
Data Sources adsl2.skills-1st.co.uk	Up	adsl2.skills-1st.co.uk	8.2	3.59	100%	
Devices bino.skills-1st.co.uk	Up	bino.skills-1st.co.uk	5.14	16.87	99.48%	
Collection deodar.skills-1st.co.uk	Up	deodar.skills-1st.co.uk	1.96	3.16	100%	Г
group-100-r1.class.example.org	Up	group-100-r1.class.example.org	62.62	69.51	79.47%	Г
Data Queries group-100-r2.class.example.org	Up	group-100-r2.class.e×ample.org	20.86	152.09	79.55%	₩
Methods group-100-r3.class.example.org	Up	group-100-r3.class.example.org	86.22	92.69	79.47%	
Templates Localhost	Up	127.0.0.1	0	0	100%	Г
Graph Templates << Previous		Showing Rows 1 to	7 of 7 [1]		Next	>>
Host Templates		Choose an action:	Delete		-	go
Data Templates						
Import/Export						
Import						
Templates						
Templates						
Configuration						
Settings						
Utilities						
System Utilities						
User						
Management						
Logout User						
						-
Done					A	block

Figure 1: Cacti main Devices panel



Figure 2: Cacti graph of interface traffic



Figure 3: Cacti graph of memory for device bino

5.2 netdisco

netdisco was created at the University of California, Santa Cruz (UCSC), Networking and Technology Services (NTS) department. It is interesting as a *network* management *configuration* offering. It uses SNMP and Cisco Discovery Protocol (CDP) to try and automatically discover devices. Unlike most other management offerings, netdisco is Layer 2 (switch) aware and can both display switch ports and optionally provide access to control switch ports.

It provides an inventory of devices that you can sort either by OS or by device model, displaying all ports for a device. It also has the ability to provide a network map. User management is included so you can restrict who is allowed to actively manage devices. There is good provision of both command line interface and web-based GUI.

netdisco is supported on various platforms – it was originally developed on FreeBSD; I built it on a Centos 4 platform.

If your requirement is strictly for network configuration management and your devices respond suitably to netdisco then this might be worth a try. I found it very quirky as to what it would discover. It appears very dependent on the SNMP system sysServices variable to decide whether a device supports network layer 2 and 3 protocols; if a device did not provide sysServices or didn't indicate layer 2 / 3, then netdisco would not discover it. I also had very few devices supporting Cisco CDP so the automatic discovery didn't work well for me. Although there is a file where you can manually describe the topology, this would be a huge job in a sizeable network if you had to hand-craft a significant amount of the network topology.

This project is not nearly so active as some of the other offerings discussed here (around 500 appends to the users maillist in 2007) but there seems to be a steady flow. Building the system was a fair marathon but the documentation is reasonably good.

Here are some screenshots of the main device inventory panel, plus the details of a router and the details of a switch.

🔋 n e t d i s c o - Device Inventory - Mozilla Firefox							
<u>File Edit View Histor</u>	y <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp				$\langle \rangle$		
- 🔶 - 💽 🙆 👔	http://netdisco/netdisco/device_inv.ht 🗈	tml	🔹 🕨 💽 Google		Q)		
📕 🔚 Firefox Support	9 Plug-in FAQ 🗀 RSS Feeds						
Netdisco	D						
din	Device Inventory						
(FIR)							
	By Age						
[Network Map]	Find Devices Last Updated	▼ 2 ▼ months ▼ Search					
[Device Search]	Find Devices That have been up for at leas	st 2 • months • Search					
[Device Inventory]	By Model			_			
[Node Search]	Vendor	Model		Coun	t i		
	cisco	2924XLv		2			
[Port Report]	cisco	3640		1			
[Duplex Mismatch	cisco	7206		2			
Finderj	CISCO	Total:		9	_		
[Node Inventory]							
[Backend Log]	By OS			1			
[Documentation]	OS	Version	C	ount			
[About]	Unknown	Unknown 8 01 02		3	_		
User jane [Logout]	ios	12.0(12)		2			
[Change Password]	ios	12.0(5.1)XP		2			
	ios	12.0(7)XK1		1			
	By Location Inventory by Location Wireless SSID Inventory Wireless SSID Inventory	Tutai.		3			
Done		Netdisco 0.95		0	Adblock		

Figure 4: Netdisco main device inventory display

🧿 netdisco-Devi	ice View - Mozil	la Firefox							_ 🗆 🗙	
<u>F</u> ile <u>E</u> dit ⊻iew Histor	Eile Edit View History Bookmarks Tools Help									
< • 🔶 • 🥑 🛞 🏠 🗈 http://netdisco/netdisco/device.html?ip=10.191.100.4&submit=Show+All+Ports&portcol= 🔹 🕨 💽 Google										
📕 🔚 Firefox Support	💹 Plug-in FAQ	CRSS Feeds								
Netdisc	C								-	
Device View group-100-r1.class.example.org (10.191.100.4) [Device Control]										
[Network Map]	Name	group-100-r1.class.example.org								
[Device Search]	Location / Contact	Virtual comms rack 100 / Andrew	v.Findlay@)skills-1st.co.uk						
	Model / Serial	cisco 7206 / Unknown								
[Device Inventory]	OS / Version	ios / 12.0(12)		100 (1-1 7000 0 1					FAOF	
[Node Search]	Description	SOFTWARE (fc1) Copyright (c)	1986-2000) by cisco Systems, In	c. Compile	d Tue 11	vi), version 12. I-Jul-00 02:09 b	y htseng	.EASE	
[Port Report]	Uptime/ Last Discovered	71 weeks,0 days,2 hours,27 min	. / Thu Jur	1 26 17:36:00 2008						
Finder]	Aliases	172.30.100.1 (group-100-r1.clas	s.example	org) @ Serial1/0						
[Node Inventory]	<u>First</u> Discovered	Tue Apr 29 15:16:16 2008								
[Backend Log]	Last ArpNip	Thu Jun 26 18:30:02 2008		2 2						
[Documentation]		Port	Duplex (Link/Admin)	Name	Speed	VLAN	Connected Devices	Port Control		
User jane [logout]		FastEthernet0/0	[NA]/[NA]	Main site network	100 Mbps					
[Change Password]	172.30.100.1	Serial1/0 (group-100-r1.class.example.org)	[NA]/[NA]	E1 line to remote site	2.0 Mbps					
	Kev									
	Ports: [Admin	Disabled] [Link Down] [Blocking] [IP Phone	(Discovered Neighbor	not acces	sible)				
	Best Man									
	Show All Po	rts Hide Ports								
	Columns: Nan Connected De Show Connec	ne IF VLAN IF Duplex IF Descrij evice Age Stamp: IC Off IC On ted Device IP: IC Off IC On	otion 🗖 S Show Resolve I	panning Tree	Change 🗖 C On	Speed	🛛 Туре 🗖 Ро	t MAC 🗖	мтиг	
Done	chunge view							Q	Adblock	

Figure 5: Netdisco details of router device

🎯 netdisco-Devi	ice View - Mozilla F	irefox							_ 		
Eile Edit View History Bookmarks Tools Help											
<											
📕 🔚 Firefox Support	💹 Plug-in FAQ 🚞	RSS Feeds	5								
Netdisco											
do	Device View										
switch.skills-1st.co.uk (10.0.0.253) [Device Control]											
	Name sw	itch skills-1	st co uk								
[Network Map] [Device Search]	Location / Contact Sk	ills 1st Offic	ce / andrew.findlay@skills-1st.c	o.uk							
	Model / Serial cis	co 2924XL	v / 0x0E								
[Device Inventory]	OS / Version ios	/ 12.0(5.1)XP								
[Node Search]	Cis Description 12 10-	sco Interne .0(5.1)XP, -Dec-99 10	twork Operating System Softwa MAINTENANCE INTERIM SOF 1:37 by cchang	are IOS (tr TWARE C	1) C2900 opyright	XL Software (C (c) 1986-1999	2900XL-C3 by cisco S	3H2S-M), Version ystems, Inc. Comp	iled Fri		
[Port Report]	Uptime/										
[Duplex Mismatch Finder]	Last 53 Discovered	min. / Thu	Jun 26 18:11:16 2008								
[Node Inventory]	<u>First</u> Discovered	u Jun 26 1	7:42:02 2008								
[Backend Log]	Last MacSuck Th	u Jun 26 20	0:00:27 2008								
[Documentation]	VTP Domain ski	lls									
[About]	Port	Duplex (Link/Admin)	Name	Speed	VLAN	Connected Devices	Port Control				
User jane [Logout] [Change Password]	FastEthernet0/1	full/auto	Linksys wireless access point	100 Mbps	1						
[enaliger desitera]	FastEthernet0/2	half/auto	Blue Atlas	10 Mbps	1						
	FastEthernet0/3	half/half	Brick		1						
FastEthernet0/4 half/half Blossom 1											
FastEthernet0/5 half/auto 1											
FastEthernet0/6 half/auto 1											
FastEthernet0/7 half/auto											
FastEthernet0/8 half/auto 1											
	FastEthernet0/9	half/auto			1						
	FastEthernet0/10	half/auto			1						
Done	FastEthernet0/11	half/auto			1			Q	- Adblock		

Figure 6: Netdisco details of a switch device, including ports

5.3 The Dude

I put some research into The Dude as it apparently provides auto discovery of a network with graphical map layout – something that is hard to find done well. From the Open Source perspective though, it really doesn't qualify. It is basically a Windows application though it can apparently run under WINE on Linux. It comes from a company called MikroTik and their website says it is "free" but it is unclear what the licensing arrangement is for The Dude. It has a very active forum.

It offers more than simply discovery and configuration as it can apparently monitor links and devices for availability and graph link performance. It can also generate notifications

6 Nagios

Nagios evolved in 2002 out of an earlier systems management project called NetSaint, which had been around since the late 1990s. It is far more a *systems* management product, rather than a *network* management product. It is available to build on most flavours of Linux / Unix and the installation has become much easier over the years. The Nagios Quickstart document is reasonably comprehensive (although it misses a few prerequisites that I found necessary like gd, png, jpeg, zlib, net-snmp and their related development packages). I downloaded and built Nagios 3.0.1 on a SuSE 10.3 platform (hostname nagios3), and had it working inside half a day.

To start the Web Interface, point your browser at <u>http://nagios3/nagios/</u>. The Quickstart document has you create some user ids and passwords – the default logon for the Web console is nagiosadmin with the password you specified during installation.

Here is a screenshot of the Nagios Tactical Overview display.



Figure 7: Nagios Tactical Overview screen

6.1 Configuration – Discovery and topology

Nagios uses a number of files to configure discovery – out-of-the-box it will find nothing. Samples are available, by default, in /usr/local/nagios/etc . The main configuration file is nagios.cfg which defines a large number of parameters, most of which you can leave alone at the outset.

Typically the main things to discover are "hosts" and "services". These are defined in an object-oriented way such that you can define host and service top-level *classes* with particular characteristics and then define sub-classes and hosts that inherit from their parent classes. Rather than having a single, huge nagios,cfg, it can reference other files (typically in the *objects* subdirectory), where definitions for hosts, services and other object types, can be kept. So, for example, /usr/local/nagios/etc/nagios.cfg may contain lines such as:

```
cfg_file=/usr/local/nagios/etc/objects/hosts.cfg
cfg_file=/usr/local/nagios/etc/objects/services.cfg
cfg_file=/usr/local/nagios/etc/objects/commands.cfg
```

Definitions of hosts are built up in a hierarchical manner so the top-level definitions may look like the following screenshot. Note the "use" stanza to denote inheritance of characteristics from a previous definition.

```
📮 jane@bino:~ - Shell - Konsole 🎱
```

Session Edit View Bookmarks Settings Help

	re .		
# HUSTS			
#			
#######	*************************************	************	
#######	**************************************	************	
# Dofin	a boot tomplates - these and not	wast boots!!!!	
# DCIII	template "generic_hest" defined	in templates of	
# 00 -	complate generit-nost dellined	in complates.cių	
#define	host{		
#	name	generic-host	; The name of this host template
#	notifications enabled	1	; Host notifications are enabled
#	event handler enabled	1	; Host event handler is enabled
#	flap detection enabled	1	; Flap detection is enabled
#	failure prediction enabled	1	; Failure prediction is enabled
#	process perf data	1	; Process performance data
#	retain status information	1	; Retain status information across program restarts
#	retain nonstatus information	1	; Retain non-status information across program rest
#	notification period	24x7	; Send host notifications at any time
#	max check attempts	4	; Check each Linux host 10 times (max)
#	register	0	; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HO
	3		
PLATE !			
PLATE! #	}		
PLATE! # # Linux	} host definition template - This	is NOT a real H	host, just a template!
PLATE! # # Linux #define	} host definition template - This host{	is NOT a real }	host, just a template!
PLATE! # # Linux #define #	} host definition template - This host{ name	is NOT a real }	host, just a template! ; The name of this host template
PLATE! # # Linux #define # #	} host definition template - This host{ name use	is NOT a real } linux-server generic-host	host, just a template! : The name of this host template : This template inherits other values from the gene
PLATE! # # Linux #define # # ate #	<pre>} host definition template - This host{ name use check period</pre>	is NOT a real b linux-server generic-host 24v2	host, just a template! ; The name of this host template ; This template inherits other values from the gend ; Bu default. Linux hosts are checked round the clu
PLATE! # # Linux #define # # ate # #	<pre>} host definition template - This host{ name use check_period obeck_interval</pre>	is NOT a real b linux-server generic-host 24x7	host, just a template! ; The name of this host template ; This template inherits other values from the gend ; By default, Linux hosts are checked round the clo
PLATE! # # Linux #define # # ate # # #	<pre>} host definition template - This host{ name use check_period check_interval retwu interval</pre>	is NOT a real H linux-server generic-host 24x7 5	host, just a template! : The name of this host template : This template inherits other values from the gend : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check methics at 1 minute interval
PLATE! # # Linux #define # # ate # # # #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval may check attempts</pre>	is NOT a real H linux-server generic-host 24x7 5 1	host, just a template! ; The name of this host template ; This template inherits other values from the gend ; By default, Linux hosts are checked round the clo ; Actively check the host every 5 minutes ; Schedule host check retries at 1 minute intervals ; Check each Linux host 10 times (max)
PLATE! # # Linux #define # # ate # # # # #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command</pre>	is NOT a real b linux-server generic-host 24x7 5 1 10 check-host-al	host, just a template! : The name of this host template : This template inherits other values from the gene : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check retries at 1 minute intervals : Check each Linux host 10 times (max) ime : Default command to check Linux hosts
PLATE? # # Linux # # # ate # # # # # # # # # # #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command motification period</pre>	is NOT a real H linux-server generic-host 24x7 5 1 10 check-host-ali	host, just a template! : The name of this host template : This template inherits other values from the gene : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check retries at 1 minute intervals : Check each Linux host 10 times (max) ive : Default command to check Linux hosts : Linux admins hate to be worken up so we call not
PLATE? # # Linux #define # # ate # # # # # # # # # # # #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period</pre>	is NOT a real H linux-server generic-host 24x7 5 1 10 check-host-ali workhours	host, just a template! : The name of this host template : This template inherits other values from the gene : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check retries at 1 minute intervals : Check each Linux host 10 times (max) ive : Default command to check Linux hosts : Linux admins hate to be woken up, so we only not
PLATE? # # Linux #define # # ate # # # # # # # # # # # # # # # # # #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period</pre>	is NOT a real b linux-server generic-host 24x7 5 1 10 check-host-ali workhours	host, just a template! ; The name of this host template ; This template inherits other values from the gene ; By default, Linux hosts are checked round the clo ; Actively check the host every 5 minutes ; Schedule host check retries at 1 minute intervals ; Check each Linux host 10 times (max) ive ; Default command to check Linux hosts ; Linux admins hate to be woken up, so we only not
PLATE? # # Linux #define # # ate # # # # # # day # from	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period</pre>	is NOT a real b linux-server generic-host 24x7 5 1 10 check-host-ali workhours	host, just a template! : The name of this host template : This template inherits other values from the gene : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check retries at 1 minute intervals : Check each Linux host 10 times (max) ive : Default command to check Linux hosts : Linux admins hate to be woken up, so we only not
PLATE ? # # Linux # define # # # # # # # # # day # from #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period</pre>	is NOT a real b linux-server generic-host 24x7 5 1 10 check-host-ali workhours	host, just a template! : The name of this host template : This template inherits other values from the gend : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check retries at 1 minute intervals : Check each Linux host 10 times (max) ive : Default command to check Linux hosts : Linux admins hate to be woken up, so we only not: : Note that the notification_period variable is be: : the value that is inherited from the generic-host
PLATE? # # Linux #define # # # # # # # # # day # from #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period</pre>	is NOT a real b linux-server generic-host 24x7 5 1 10 check-host-ali workhours	host, just a template! : The name of this host template : This template inherits other values from the gend : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check retries at 1 minute intervals : Check each Linux host 10 times (max) ive : Default command to check Linux hosts : Linux admins hate to be woken up, so we only not : Note that the notification_period variable is be : the value that is inherited from the generic-host : Resend notifications every 2 hours
PLATE ? # # Linux # define # # ate # # # # # day # from # #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period </pre>	is NOT a real b linux-server generic-host 24x7 5 1 10 check-host-ali workhours	<pre>host, just a template! The name of this host template This template inherits other values from the gend By default, Linux hosts are checked round the clo Actively check the host every 5 minutes Schedule host check retries at 1 minute intervals Check each Linux host 10 times (max) ive : Default command to check Linux hosts Linux admins hate to be woken up, so we only not: Note that the notification_period variable is be: the value that is inherited from the generic-host Resend notifications every 2 hours Only send notifications for specific host states </pre>
PLATE ? # # Linux # define # # ate # # # # day # from # # # # #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period notification_period </pre>	is NOT a real H linux-server generic-host 24x7 5 1 10 check-host-ali workhours 120 d,u,r admins	host, just a template! : The name of this host template : This template inherits other values from the gend : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check retries at 1 minute intervals : Check each Linux host 10 times (max) ive : Default command to check Linux hosts : Linux admins hate to be woken up, so we only not: : Note that the notification_period variable is be: : the value that is inherited from the generic-host : Resend notifications every 2 hours : Only send notifications for specific host states : Note for the term of the term of the default
PLATE ? # # Linux # define # # ate # # # day # from # # # # # # # # # # # # #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period motification_options contact_groups revister</pre>	is NOT a real H linux-server generic-host 24x7 5 1 10 check-host-ali workhours 120 d,u,r admins 0	host, just a template! : The name of this host template : This template inherits other values from the gene : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check retries at 1 minute intervals : Check each Linux host 10 times (max) ive : Default command to check Linux hosts : Linux admins hate to be woken up, so we only not : Note that the notification_period variable is be : the value that is inherited from the generic-host : Resend notifications every 2 hours : Only send notifications for specific host states : Note The STER THUS DEFINITION - UTS NOT & REAL HE
PLATE ? # # Linux # define # ate # # # # # from # # # # # PLATE ? *	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period notification_options contact_groups register</pre>	is NOT a real b linux-server generic-host 24x7 5 1 10 check-host-ali workhours 120 d,u,r admins 0	host, just a template! ; The name of this host template ; This template inherits other values from the gene ; By default, Linux hosts are checked round the clo ; Actively check the host every 5 minutes ; Schedule host check retries at 1 minute intervals ; Check each Linux host 10 times (max) ive ; Default command to check Linux hosts ; Linux admins hate to be woken up, so we only not ; Note that the notification_period variable is be ; the value that is inherited from the generic-host ; Resend notifications every 2 hours ; Only send notifications for specific host states ; Notifications get sent to the admins by default ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HO
PLATE ? # # Linux # define # ate # # # # # # # # from # # # PLATE ? #	<pre>} host definition template - This host{ name use check_period check_interval retry_interval max_check_attempts check_command notification_period notification_options contact_groups register }</pre>	is NOT a real b linux-server generic-host 24x7 5 1 10 check-host-ali workhours 120 d,u,r admins 0	host, just a template! : The name of this host template : This template inherits other values from the gene : By default, Linux hosts are checked round the clo : Actively check the host every 5 minutes : Schedule host check retries at 1 minute intervals : Check each Linux host 10 times (max) ive : Default command to check Linux hosts : Linux admins hate to be woken up, so we only not : Note that the notification_period variable is be : the value that is inherited from the generic-host : Resend notifications every 2 hours : Only send notifications for specific host states : Notifications get sent to the admins by default : DONT REGISTER THIS DEFINITION - ITS NOT A REAL HO

Figure 8: Nagios hosts.cfg top-level definitions

Host availability parameters are shown in the screenshot above:

•	check_period	(24x7)
•	check_interval	(5 mins)
•	retry interval	(1 min)
•	max_check_attempts	(10)
•	check_command	(check_host_alive which is based on check_ping)

define	host{	
	name	host_10.191 ; hosts on the 10.191 network
	use	generic-host ; inherits from generic-host
	parents	bino ; bino is the router from 10
	check_command	check-host-alive
	contact_groups	admins
	register	0 ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST
	}	
define	host {	
ucrinc	nosti	hast 172 31 100 32 ; hosts on the 172 31 100 32 network
		reneric_host · inherits from generic_host
	narents	aroun=100-r3; $aroun=100-r3$ is the router from 172 31 100 32
	check command	check-host-alive
	contact groups	admine
	register	A : DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST. JUST
	}	
define	host{	
	name	host_172.30.100 ; hosts on the 172.30.100 network
	use	generic-host ; inherits from generic-host
	parents	group-100-r1 ; group-100-r1 is the router from 172.31.100.32
	check_command	check-host-alive
	contact_groups	admins
	register	0 ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL HOST, JUST
	}	

Figure 9: Nagios hosts.cfg showing host template definitions

Subsequent definitions of sub-groups and real hosts will follow. Note the use of the "parents" stanza to denote the network node that provides access to the device. This means that Nagios can tell the difference between a node that is down and a node that is unreachable because its access router is down.

```
#
# Now start defining real hosts
# Hosts on the 10.191 network
define host{
                                group-100-r1
        host_name
        use
                                host_10.191
                                                        ; Name of host template to use
        alias
                                group-100-r1.class.example.org
        address
                                group-100-r1.class.example.org
        3
# Hosts on the 172.16.100.32 network
define host{
        host name
                                         group-100-r3
                                         host_172.31.100.32
        use
                                         group-100-r2
        parents
        alias
                                         group-100-r3.class.example.org
                                         group-100-r3.class.example.org
        address
        }
define host{
                                         group-100-s1
        host name
                                         host 172.31.100.32
        use
        alias
                                         group-100-s1.class.example.org
        address
                                         group-100-s1.class.example.org
        }
```

Figure 10: Nagios hosts.cfg file showing real host definitions

Hosts can be defined to be a member of one or more host groups. This then makes subsequent configuration more scalable (for example, a service can be applied to a host group rather than to individual hosts). Host groups are typically defined in hosts.cfg.

```
# HOST GROUPS
# create more than one hostgroup
define hostgroup{
      hostgroup_name routers
      alias
                  routers
                 bino, group-100-r1, group-100-r2, group-100-r3
      members
define hostgroup{
      hostgroup_name nagios
      alias
                 nagios
      members
                 nagios, nagios3
define hostgroup{
      hostgroup_name servers
      alias
                  servers
                 bino, tino, server, nagios, nagios3
      members
define hostgroup{
      hostgroup_name clients
      alias
                 clients
                 group-100-s1, group-100-c1, group-100-c2, group-100-c3, group-100-a1
      members
      3
define hostgroup{
      hostgroup_name raddle
      alias
                 raddle
                 server, group-100-r1, group-100-r2, group-100-r3, group-100-s1, group-100-c1, group-100-c2, group-100-c3, group-100-a1
      members
}
```

Figure 11: Nagios hosts.cfg host group definitions

Host groups are also used in the GUI to display data based on host groups.



Figure 12: Nagios Host group summary

Whenever changes have taken place to any configuration file, the command:

/etc/init.d/nagios reload

should be used. This does not stop and start the Nagios processes (use stop | start | restart | status to control the background processes) – the reload parameter simply rereads the configuration file(s). There is also a handy command to verify that your configuration files are legal and consistent, before actually performing the reload:

/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

All objects to be managed need defining in the Nagios configuration files – there is no form of automatic discovery; however the ability to create object templates and thus an object hierarchy, makes definitions flexible and easy, once you have defined your hierarchies.

A great benefit of this configuration file is the ability to denote the network devices that provide access to specific nodes (parent / child relationship). This means that a map hierarchy can be displayed and also means that node reachability is encoded. If, for example, all nodes on the 172.31.100.32 network inherit from a template that includes a "parents" group-100-r3" stanza, when group-100-r3 goes down then Nagios knows that all nodes in that network are unreachable (rather than down). Defining multiple parents for a meshed network seemed problematical though.

Nagios automatically generates a topology map, based on the the "parents" stanzas in the configuration files. Colour-coding provides status for nodes.



Figure 13: Nagios Status map

6.2 Availability monitoring

Nagios availability monitoring focuses much more on systems than on networks . Nagios provides a large number of official plugins for monitoring; in addition there are other community plugins available, or you can write your own. The official plugins should be installed alongside the base Nagios. The executables can be found in /usr/local/nagios/libexec (use <plugin name> --help for usage on each plugin). The official plugins include:

check_ping	configurable ping test with warning & critical thresholds
check_snmp	generic SNMP test to get MIB OIDs & test return values
check_ifstatus	check SNMP ifOperStatus against ifAdminStatus for all Administratively up interfaces
check_ssh	check that the ssh port can be contacted on a remote host
check_by_ssh	use ssh to run command on remote host
check_nt	check Windows parameters (disk, cpu, services, etc). Needs NSClient++ agent installed on Windows targets
check_nrpe	check remote Linux parameters (disk, cpu, processes, etc). Needs NRPE agent installed on Unix / Linux target

Nagios has two separate concepts -host monitoring and *service* monitoring and there is a known relationship between the state of the host and the state of its services.

Host monitoring is a reachability test and will generally use the check_ping Nagios plugin. If you have devices that support SNMP but do not support ping (perhaps because there is a firewall in the way that blocks ping), then the check_ifstatus plugin works well to test all interfaces on a device and compares the SNMP administrative status with the operational status. Host monitoring is defined in the Nagios configuration files with the "check_command" stanza, where typically this is defined at a high level of the host definition hierarchy but can be overridden for sub-groups or specific hosts. For example, in hosts.cfg:

defin	e host {		
	host_name	group-100-a1	
	use	host_172.31.100	;Inherits from this parent class
	parents	group-100-r2	;This is n/w route to device
	alias	group-100-al.clas	s.example.org
	address	group-100-al.clas	s.example.org
	check_command	check_ifstatus	;SNMP status check, not ping
	}		

A summary of host status is given on the "Tactical Overview" display. The "Host Detail" display then gives further information for each device. The hosts monitored using check_ping show the Round Trip Average (RTA). Note that group-100-a1 is monitored using the check_ifstatus plugin so shows different Status Information.

🥘 Nagios - Mozilla Firefox 📃 🗆 🗙									
File Edit View History Bookmarks Tools Help									
< - 🔶 - 🥑 😣 🏠	(a) → - C (a) (b) http://nagios3/nagios/								
group-100-a1.class.e	group-100-a1.class.exa 🛛 Nagios 🔹								
General ● Home ● Documentation	Current Netw Last Updated: We Updated every 90 Nagios® 3.0.1 - <u>w</u> Logged in as <i>nag</i> .	vork Statu ed Jul 2 12:05 seconds www.nagios.or iosadmin	s :11 BST 2008 9		Up Do	Host Status Totals	Service Status Totals Ok Warning Unknown Critical Pending 32 0 0 3 0 All Problems All Types		
Monitoring Tactical Overview Service Detail Host Detail	<u>View Service Stat</u> <u>View Status Overv</u> <u>View Status Sum</u> <u>View Status Grid</u>	Miew Service Status Detail For All Host Groups All Problems All Types All Problems All Types Miew Status Overview For All Host Groups 2 13 Miew Status Grid For All Host Groups 3 35							
 Hostgroup Overviev Hostgroup Summar Hostgroup Grid Servicegroup Overv Servicegroup Summ Servicegroup Grid 					Host St	atus Details For All Host Groups			
• Status Map	Host 🚹	Status 个	Last Chec	:k ↑	Duration 🐴	Status Information			
3-D Status Map	bino 🚯	UP	02-07-2008 12	2:02:08	1d 23h 34m 42s	PING OK - Packet loss = 0%, RTA = 0).30 ms		
Service Problems	<u>group-100-a1</u> 🚯	UP	02-07-2008 12	2:04:08	0d 0h 28m 6s	OK: host 'group-100-a1.class.example. unused: 0	.org', interfaces up: 2, down: 0, dormant: 0, excluded: 0,		
Host Problems	group-100-c1 🕵	UP	02-07-2008 12	2:00:15	0d 3h 9m 53s	PING OK - Packet loss = 0%, RTA = 1	42.80 ms		
Unhandled Network Outages	group-100-c2	UP	02-07-2008 12	2:04:25	0d 3h 9m 33s	PING OK - Packet loss = 0%, RTA = 2	216.36 ms		
Cham Uset	group-100-c3	UP	02-07-2008 12	2:02:55	0d 3h 9m 33s	PING OK - Packet loss = 0%, RTA = 1	13.08 ms		
Show Host:	group-100-r1	UP	02-07-2008 12	2:01:25	0d 4h 37m 15s	PING OK - Packet loss = 0%, RTA = 2	24.50 ms		
	group-100-r2 🚯	UP	02-07-2008 12	2:01:05	0d 3h 15m 5s	PING OK - Packet loss = 0%, RTA = 8	3.56 ms		
© Comments	group-100-r3 🚯	UP	02-07-2008 12	2:03:25	0d 3h 9m 43s	PING OK - Packet loss = 0%, RTA = 1	34.61 ms		
Downtime	group-100-s1 🌇	UP	02-07-2008 12	2:02:55	0d 3h 9m 33s	PING OK - Packet loss = 0%, RTA = 1	21.06 ms		
Process Info	nagios 🗐 🗙 😘	DOWN	30-06-2008 20	0:46:49	69d 18h 56m 41s	CRITICAL - Host Unreachable (nagios.	skills-1st.co.uk)		
Performance Info Scheduling Queue	nagios3 💦	UP	02-07-2008 12	2:04:35	69d 23h 13m 7s	PING OK - Packet loss = 0%, RTA = 0).05 ms		
- benedaling Quede	server 😽	UP	02-07-2008 12	2:00:05	69d 23h 12m 58s	PING OK - Packet loss = 0%, RTA = 0).56 ms		
Reporting	tino 🐕 🗩 🖡	DOWN	02-07-2008 12	2:02:28	69d 23h 9m 4s	CRITICAL - Host Unreachable (tino.ski	lls-1st.co.uk)		
 Trends Availability Alert Histogram 					13 M	atching Host Entries Displayed			

Figure 14: Nagios Host Detail display

Availability monitoring, especially for "computers" rather than network devices, can mean many things. Nagios provides many plugins for port monitoring, including generic TCP and UDP monitors. The check_snmp plugin could be used to check SNMP parameters from the Host Resources MIB (if a target supports this). Nagios also provides remote agents, NSClient++ for Windows and NRPE for Unix / Linux systems, which provide a much more customisable definition of system monitoring.

Services are typically defined in services.cfg. As with host definitions, services can be defined in a class hierarchy where characteristics of an object are inherited from its parent.

# Gen # JC	eric service definition template - - generic-service defined in templ	- This is NOT a real s lates.cfg, which also	service define	, just a template! s local-service
#defi	ne service{			
#	name	generic-service	;	The 'name' of this service template
#	active checks enabled	1	;	Active service checks are enabled
#	nassive checks enabled	1	;	Passive service checks are enabled/accepted
#	narallelize check	1		Active service checks should be narallelized (disabling this
erfor	mance urohlems)	1. The		notito outtoo ononio ononia po parattoridoa taroabring unic
#	obsess over service	1	:	We should obsess over this service (if necessary)
#	check freshness	0		Default is to NOT check service 'freshness'
#	notifications enabled	1		Service notifications are enabled
#	event handler enabled	1		Service event handler is enabled
#	flan detection enabled	1		Flan detection is enabled
#	failure prediction enabled	1		Failure prediction is enabled
Ħ	process perf data	Î		Process performance data
tt	retain status information	1		Retain status information across program restarts
#	retain nonstatus information	1		Retain non-status information across program restarts
#	is uplatile	Ā		The service is not uplatile
#	check period	24.7		The service can be checked at any time of the day
tt	max check attempts	3		Re-check the service up to 3 times in order to determine its
#	normal check internal	10		Check the service every 10 minutes under normal conditions
#	retru check internal	2		Re-check the service every two minutes until a hard state ca
**	contact groups	admins		Notifications get sent out to everyone in the 'admins' group
**	notification ontions		1	Send notifications about warning unknown critical and nec
**	notification_options	60	1	Re-notify shout service moblems evenu hour
**	notification_nemicd	24-7	1	Notifications can be cent out at any time
**	notification_perioa	0	:	NOUTIFICATIONS CAN BE SENT OUT AT ANY LINE DON'T DECISTED THIS DEFINITION _ ITS NOT A DEAL SEDUICE THE
#	}	0		DON'T ALGISTEN THIS DEFINITION - TIS NOT H ALAL SERVICE, JUST
# Loc	al service definition template - 1	This is NOT a real ser	rvice,	just a template!
#defi	ne seruice{			
Ħ	name	local-service		The name of this service template
#	lise	generic-service		Internit default values from the generic-service definition
#	max check attempts	4		Re-check the service up to 4 times in order to determine its
#	normal check internal	5		Check the service evenu 5 minutes under normal conditions
#	normu check interval	1		Re-check the service evenu minute until a hand state can be
#	negisten	0		DONT RECISTER THIS DEFINITION _ ITS NOT A REAL SERVICE THIS
#	}	v	,	
# ser	vice definition template for ping	check - This is NOT a	a real	service, just a template!
defin	e seruice{			
	name	ning-service	; Т	he name of this service template
	use	generic-service		Inherit default values from the generic-service definition
	max check attempts	4		Re-check the service up to 4 times in order to determine its
	normal check interval	5		Check the service every 5 minutes under normal conditions
	retru check interual	1		Re-check the service every minute until a hard state can be d
	register	Ā		DONT REGISTER THIS DEFINITION - ITS NOT A REAL SERVICE JUST
	}			
	1			

| Figure 15: Nagios service.cfg top-level objects

Again, note the check_period,max_check_attempts, normal_check_interval and retry_check_interval stanzas. More specific service definitions can be then be defined, inheriting characteristics of parents through the "use" stanza:

```
jane@bino:~ - Shell - Konsole <3>
Session Edit View Bookmarks Settings Help
# Define a service to "ping" non-raddle machines
define service{
                                        ping-service
                                                             ; Name of service template to use
        use
        hostgroup_name
                                        servers
        service_description
                                        PING
                                        check_ping !200.0,20% !500.0,60%
        check command
# Define a service to "ping" raddle machines - longer ping return-trip time
define service{
                                                             ; Name of service template to use
        use
                                        ping-service
        hostgroup_name
                                        raddle
        service_description
                                        PING
                                        check_ping 1300.0,20% 1500.0,60%
        check command
# Define a service to check the disk space of the root partition
# on the local machine. Warning if < 10% free, critical if
#
 < 5% free space on partition.
define service{
                                                              ; Name of service template to use
        use
                                        local-service
        host name
                                         nagios3
        service_description
                                        Root Partition
        check_command
                                        check_local_disk!10%!5%!/
 Define a service to check DNS resolution for www.skills-1st.co.uk on bino
 The name to look up is defined in the check_dns stanza in commands.cfg
# The host_name parameter here is the DNS server to use in a local nslookup command (ie. bino)
define service{
                                                              ; Name of service template to use
                                        local-service
        use
        host name
                                        bino
                                        DNS Check
        service_description
        check_command
                                        check_dns
# Define a service to check SNMP on bino
define service{
                                                                ; Name of service template to use
        use
                                        generic-service
        host name
                                        bino
                                        SNMP Check
        service_description
                                        check_snmp!-C public -o sysUpTime.0
        check_command
# EOF
```

Figure 16: Nagios services.cfg showing specific services

Note that services can be applied either to groups of hosts (hostgroup_name) or to specific hosts (host_name).

As with hosts, it is possible to create groups of services to improve the flexibility of configuration and the display of services.

Also note that some services run commands that are inherently local to the Nagios system eg. check_local_disk. The check_dns command runs nslookup on the Nagios system but the host_name parameter can be used to specify the DNS server to query from. The commands are actually specified in the configuration file commands.cfg, which, in turn, calls executable plugins in /usr/local/nagios/libexec.

😻 Nagios - Mozilla Firefox 📃 🗆 🗙									
File Edit View History Bookmarks Tools Help									
 - -	▶ http://n	agios3/nagio	s/					- D Google	
Nagios		OpenNMS	Web Conso	le 🖸					
<u>N</u> agios	Current Network Status Last Updated: Wed Jul 30 12:07:37 BST 2008			08	Host Status Totals			Service Status Totals	
General	Updated ever Nagios® 3.0.		11	2	0	0 16 0 0 2 0			
Home Documentation	Logged in as <i>nagiosadmin</i> View History For all hosts View Notifications For All Hosts					All Problem	1s <u>All Types</u> 13	All Problems All Types 2 18	
Monitoring	View Host Status Detail For All Hosts								
 Tactical Overview Service Detail Host Detail Host group Overview Hostgroup Summary 	Service Status Details For All Hosts								
Hostgroup Grid Servicegroup Overvie	Host 🚹	Service 个	Status 🚹	Last Che	ck 个 🗌	Duration 个	Attempt 个	Status Information	
Servicegroup Summar Servicegroup Grid	<u>bino</u>	DNS Check	ок	30-07-2008 1	2:05:18	22d 1h 53m 1s	1/2	DNS OK: 0.014 seconds response time. www.skills-1st.co.uk returns 212.74.28.155	
Status Map		PING	0K	30-07-2008 1	2:06:55	97d 23h 17m 16s	1/4	PING OK - Packet loss = 0%, RTA = 0.42 ms	
© Service Problems	aroun 100 e1		OK	20.07.2008 1	2.00.27	200 1711 45111 528	1/3	Siving OK - Interactions (14490143) 1 day, 15, 15,01,45	
OUnhandled	group-100-c1	PING	OK	20.07.2008 1	2.05.50	0d 0h 41m 47 s	1/4	PING OK - Packet loss = 0%, RTA = 103.51 ms	
Outproblems Outproblems	group-100-c2	PING	OK	20.07.2000 1	2.03.36	0d 1n 24m 1s	1/4	PING OK - Packet loss = 0%, RTA = 72.01 ms	
Network Outages	group-100-c3	PING	UK	30-07-2008 1	2:03:13	Ud 1h 14m 24s	1/4	PING OK - Packet loss = 0%, RTA = 139.93 ms	
Show Host:	group-100-r1	PING	UK	30-07-2008 1	2:03:59	Ud 2h 3m 38s	1/4	PING OK - Packet loss = U%, RTA = 7.48 ms	
	group-100-r2	PING	OK	30-07-2008 1	2:05:45	0d 2h 1m 52s	1/4	PING OK - Packet loss = 0%, RTA = 140.70 ms	
© Comments	group-100-r3	PING	OK	30-07-2008 1	2:04:22	0d Oh 58m 15s	1/4	PING OK - Packet loss = 0%, RTA = 72.29 ms	
Downtime	group-100-s1	PING	OK	30-07-2008 1	2:06:08	0d 1h 41m 29s	1/4	PING OK - Packet loss = 0%, RTA = 70.92 ms	
Performance Info	nagios 🗙	PING 🕺		30-07-2008 1	2:04:16	22d 2h 50m 3s	1/4	CRITICAL - Host Unreachable (nagios.skills-1st.co.uk)	
Scheduling Queue	nagios3	Current Load	OK	30-07-2008 1	2:04:25	97d 23h 14m 46s	1/2	OK - load average: 0.01, 0.02, 0.00	
Reporting		Current Users PING	OK	30-07-2008 1	2:06:11	97d 23h 13m 0s 97d 23h 16m 23s	1/2 1/4	USERS OK - 6 users currently logged in PING OK - Packet loss = 0% RTA = 0.06 ms	
Trends Availability		Root Partition	OK	30-07-2008 1	2:07:24	97d 22h 56m 37s	1/2	DISK OK - free space: / 788 MB (16% inode=69%):	
Alert Histogram		Total Processes	ок	30-07-2008 1	2:06:20	97d 22h 54m 51s	1/2	PROCS OK: 46 processes with STATE = RSZDT	
Alert History Alert Summary	CONT	DINC	OK	20.07.2009.1	2.07.20	0d 1h 20m 9a	174	DINC OV Desket less = 0% DTA = 0.59 mg	
Notifications Event Log	Server	PASV		30-07-2008	2.07.25		1/4	FING OK - Facket loss - 0.6, RTA - 0.55 ms	
		PING 110	CRITICAL	30-07-2008 1	0:10:01	22d 1h 54m 18s	1/4	CRITICAL - Host Unreachable (tino.skills-1st.co.uk)	
Configuration View Config					1	8 Matching Servic	e Entries Displa	ayed	

Figure 17: Nagios Service detail

Service *dependencies* are an advanced feature of Nagios that allow you to suppress notifications and active checks of services based on the status of one or more other services (that may be on other hosts).

Both host and service monitoring can be configured to generate events on failure (and this is the default).

6.3 Problem management

Nagios's event system displays events generated by Nagios's own host and service monitors. There is no built-in capability to collate events received as SNMP TRAPs or syslog messages. When an event is generated, it can be configured so that

notification(s) are generated to one or more users or groups of users. It is also possible to create automated responses to events (typically scripts).

Note that Nagios tends to use the terms event and alert interchangeably.

6.3.1 Event console

The Nagios Event Log is displayed from the left-hand menu:



Figure 18: Nagios Event Log

By default, the event log is displayed in one-hourly sections. The log shows the event status and also shows whether a Notification has been generated (the megaphone symbol). This display is effectively simply showing /usr/local/nagios/var/nagios.log.

Under the Reporting heading on the left-hand menu, there are further options to display information on events (alerts). The *Alert History* is effectively the same as the *Event Log*. The *Alert Histogram* produces graphs for either a host or service with customisable parameters.

<u>File Edit View History</u>	Bookmarks Tools Help								
< - 🔶 - 🕑 🐼 🚮	▶ http://nagios3/nagios/		• D						
№ Nagios	😰 🗋 OpenNMS Web Console 🛛 🚺 State Types								
▲ General ● Home ● Documentation	Host Alert Histogram Last Updated: Thu Jul 31 12:42:32 BST 2008 Nagios® 3.0.1 - <u>www.nagios.org</u> Logged in as <i>nagiosadmin</i> Step 3: Sel	lect Report Options							
Monitoring									
Tactical Overview	Report Period:	Last 7 Days	•						
Service Detail Host Detail	If Custom Report Period								
Hostgroup Overviev Hostgroup Summary	Start Date (Inclusive):	July 1 2008	}						
Hostgroup Grid Servicegroup Overv	End Date (Inclusive):	July July 31 2008	3						
Servicegroup Summ Servicegroup Grid									
Status Map 3-D Status Map	Statistics Breakdown:	Day of the Month 🚽							
Service Problems Automatical	Events To Graph:	All host events	•						
Host Problems	State Types To Granh	Hard and soft states	-						
Network Outages									
Show Host:	Assume State Retention.	Yes •							
	Initial States Logged:	No 🗾							
Comments Downtime	Ignore Repeated States:	No 🚽							
Process Info		Create Report							
Performance Info Scheduling Queue									
Reporting									
• Trends									
 Availability Alert Histogram 									
Alert History Alert Summary									
 Notifications Event Log 									

Figure 19: Nagios Configuration for Alert Histogram

Note in the figure above that a host / service selection has already been prompted for and, having selected "host", the specific host has been supplied. The following figure shows the resulting graph. Note the blue links towards the top left of the display providing access to a filtered view of the events log (View History for this Host) and to notifications for this host.



Figure 20: Nagios Alert Histogram for host group-100-r1

The Alert Summary menu option can provide various reports, specific to hosts or services.

🎯 Nagios - Mozilla Fire	fox			_				
<u>F</u> ile <u>E</u> dit ⊻iew Hi <u>s</u> tory	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp			0				
< - 🔶 - 🥑 🐼 🏠	N http://nagios3/nagios/		🔹 🕨 💽	Q)				
Nagios	📮 🗋 OpenNMS Web Console 🛛 🛛 🚺 State	Types 💿		•				
Nagios° [▲] General ® Home	Alert Summary Report Last Updated: Thu Jul 31 13:02:07 BST 2008 Nagios® 3.0.1 - <u>www.nagios.org</u> Logged in as <i>nagiosadmin</i>	Standard Penorts						
Documentation	Depart Type:	25 Most Decent Herd Alerte	-1					
Monitoring	Report Type.	25 Most Recent Hard Alerts	<u> </u>					
Tactical Overview Service Detail		Create Summary Report!						
Host Detail Host group Overview	c	ustom Report Options:						
Hostgroup Summary	Rep	ort Type Most Recent Alerts	•					
Servicegroup Overv								
Servicegroup Summ Servicegroup Grid	Repor	t Period: Last 7 Days	•					
Status Map Status Map	If Custom Report Period							
© Service Problems	Start Date (Ir	nclusive): July 🚽 1 🛛 2	008					
© Unhandled © Host Problems © Unhandled © Network Outages	End Date (Ir	nclusive): July 💽 31 2	008					
Show Host:	Limit To Ho	ostgroup: ** ALL HOSTGROUPS	** 🗸					
	Limit To Servi	cegroup: ** ALL SERVICEGROU	IPS ** •					
© Comments © Downtime	Limit	To Host: ** ALL HOSTS **	_					
Process Info Performance Info	Ale	rt Types: Host and Service Alerts	•					
Scheduling Queue	Stat	te Types: Hard and Soft States	Ī					
Reporting Trends	Hos	st States: All Host States	•					
Availability Alert Histogram	Servic	e States: All Service States	•					
 Alert History Alert Summary 	Max L	ist Items: 25						
 Notifications Event Log 		Create Summary Repo	ort!					
Configuration								
Find: retry_in		h case 🛛 A Phrase not found						

Figure 21: Nagios Alert Summary configuration options

Limiting the report to a specific host, group-100-r1, produces the following report.
🎯 Nagios - Mozilla Fire	fox		
<u>F</u> ile <u>E</u> dit <u>V</u> iew History	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		0
🤹 • 🔶 • 🕑 🐼 🏠	N http://nagios3/nagios/	-	
N Nagios	🔲 🗋 OpenNMS Web Console 🛛 🚺	State Types	•
Nagios [®] General ® Home ® Documentation	Alert Summary Report Last Updated: Thu Jul 31 13:08:02 BST 2008 Nagios® 3.0.1 - <u>www.nagios.org</u> Logged in as <i>nagiosadmin</i>	Most Recent Alerts For Host 'group-100-r1' 24-07-2008 13:08:02 to 31-07-2008 13:08:02 Duration: 7d 0h 0m 0s	Report Options Summary: Alert Types: Host & Service Alerts State Types: Soft & Hard States Host States: Up, Down, Unreachable Service States: Ok, Warning, Unknown, Critical Generate New Report
Monitoring Tactical Overview Service Detail Host Detail Overview	Time Alert Type Host S	Displaying all 23 matching alerts Service State State Type Information	
 Hostgroup Summar Hostgroup Grid Servicegroup Overv Servicegroup Summ Servicegroup Grid Status Man 	31-07-2008 10:37:06 Service Alert group-100-r1 31-07-2008 10:36:06 Host Alert group-100-r1 31-07-2008 10:17:26 Host Alert group-100-r1 31-07-2008 10:17:26 Host Alert group-100-r1 31-07-2008 10:17:26 Host Alert group-100-r1 31-07-2008 10:17:06 Service Alert group-100-r1	PING OK HARD PING OK - Packet lo V/A UP HARD PING OK - Packet lo V/A DOWN HARD CRITICAL - Host Uni PING CRITICAL HARD CRITICAL - Host Uni V/A DOWN HARD CRITICAL - Host Uni	ss = 0%, RTA = 12.17 ms ss = 0%, RTA = 17.06 ms eachable (group-100-r1.class.example.org) eachable (group-100-r1.class.example.org)
 3-D Status Map Service Problems Unhandled Host Problems Unhandled 	31-07-2008 10:16:16 Host Alert group-100-r1 31-07-2008 10:15:06 Host Alert group-100-r1 31-07-2008 10:14:06 Host Alert group-100-r1 30-07-2008 15:07:06 Service Alert group-100-r1 30-07-2008 15:07:16 Service Alert group-100-r1 30-07-2008 15:06:16 Service Alert group-100-r1	V/A DOWN SOFT CRITICAL - Host Unit V/A DOWN SOFT CRITICAL - Host Unit V/A DOWN SOFT CRITICAL - Host Unit PING OK SOFT PING OK Packet lo PING CRITICAL SOFT PING CRITICAL - Pa	reachable (group-100-r1.class.example.org) reachable (group-100-r1.class.example.org) reachable (group-100-r1.class.example.org) ss = 0%, RTA = 7.45 ms cket loss = 44%, RTA = 6298.01 ms
Network Outages Show Host:	30-07-2008 15:05:06 Service Alert group-100-r1 30-07-2008 14:00:16 Host Alert group-100-r1 30-07-2008 14:00:06 Service Alert group-100-r1 30-07-2008 14:00:06 Service Alert group-100-r1 30-07-2008 13:59:36 Host Alert group-100-r1	DING CRITICAL SOFT PING CRITICAL - Pa V/A UP SOFT PING OK - Packet lo DING OK SOFT PING OK - Packet lo V/A DOWN SOFT PING OK - Packet lo	icket loss = 0%, RTA = 649.55 ms ss = 0%, RTA = 9.96 ms ss = 0%, RTA = 7.49 ms reachable (group-100-r1.class.example.org)
© Comments © Downtime © Process Info	30-07-2008 13:59:16 Service Alert group-100-r1 30-07-2008 13:56:16 Host Alert group-100-r1 30-07-2008 13:55:56 Host Alert group-100-r1	PING CRITICAL SOFT PING CRITICAL - Pa V/A UP SOFT PING OK - Packet lo V/A DOWN SOFT PING CRITICAL - Pa	cket loss = 100% ss = 0%, RTA = 4.31 ms cket loss = 79%, RTA = 21101.40 ms
 Performance Info Scheduling Queue 	30-07-2008 10:04:11 Service Alert <u>group-100-r1</u> F 30-07-2008 10:03:01 Host Alert <u>group-100-r1</u> N 20.07, 2009 10:02:11 Host Alert	PING OK HARD PING OK - Packet lo V/A UP HARD PING OK - Packet lo V/A DOMNN HARD Chart Chart Timed	ss = 0%, RTA = 5.73 ms ss = 0%, RTA = 8.13 ms
Reporting Trends Availability Alert Histogram Alert Summary Notifications Event Log	su-u7-2008 10:02:11 Host Alert group-100-r1 30-07-2008 10:00:31 Host Alert group-100-r1 30-07-2008 09:59:11 Service Alert group-100-r1 30-07-2008 09:59:01 Host Alert group-100-r1 30-07-2008 09:57:21 Host Alert group-100-r1	V/A DOWN HARD (Host Check Timed) V/A DOWN SOFT (Host Check Timed)	Out) Out) icket loss = 100% Out) Out)
Configuration		□ Mat <u>c</u> h case	

Figure 22: Nagios Alert Summary for group-100-r1

6.3.2 Internally generated events

Nagios has the concept of *soft* errors and *hard* errors to allow for occasional glitches in host and service monitoring. Any host or service monitor can specify or inherit parameters for the check interval under OK conditions, the check interval under non-OK conditions and the number of check attempts that will be made.

• Host parameters

0	check_interval	default 5 mins (check interval when host OK)	

- retry_interval default 1 min (check interval when host non-OK)
- \circ max-check_attempts default 4 (number of attempts before HARD event)
- Service parameters
 - \circ normal_check_interval default 10 mins
 - \circ retry_check_interval default 2 mins

• max_check_attempts default 3 (number of attempts before HARD event)

When a non-OK status is detected, a soft error is generated for each sampling interval until max_check_attempts are exhausted, after which a hard event will be generated. At this point, the polling interval reverts to the check_interval rather than the retry_interval.



Figure 23: Nagios Event Log showing hard and soft events

Note from the earlier figure showing the topology layout, that group-100-r3 sits behind group-100-r1. Each of these host devices is being polled every 5 minutes when in an OK state (or max_check_attempts has been exceeded) and every 1 minute when a problem has arisen. The actual problem that has caused the event log shown above, is that group-100-r1 has failed; however, group-100-r3 is polled first and results in the first event for this device with a status of DOWN and a state type of SOFT.

Subsequently, group-100-r1 is polled and found to be DOWN which results in the associated poll to group-100-r3 receiving a status of UNREACHABLE and a state type

of SOFT. The third poll of group-100-r3 again has a status of UNREACHABLE and a state type of SOFT.

The next event for group-100-r3 is a service ping monitor (which runs every 5 minutes for this device). Note that this event has a state type of HARD – this is because Nagios knows that the host status associated with this service monitor is already UNREACHABLE (or DOWN).

The fourth event results in a state type of HARD and the status of UNREACHABLE. The hard event also generates a notification.

6.3.3 SNMP TRAP reception and configuration

Nagios's own documentation says that it is not a replacement for a full-blown SNMP management application. It has no simple way to receive SNMP TRAPs or to parse them.

It is possible to integrate SNMP TRAPs by sending them to Nagios as "passive checks" but this will require significant effort. The documentation suggests using a combination of net-snmp and the SNMP TRAP Translator (SNMPTT) packages.

6.3.4 Nagios notifications

In Nagios, the terms *event* and *alert* are used interchangeably.

There is a comprehensive mechanism for notifications which is driven by parameters on the host and service checks. There is also configuration for notifications on a percontact basis; each check can have a *contact_groups* stanza specifying who to contact. Contacts can appear in several different contact groups (although only a single notification will be sent to any individual). Notifications are *only* generated for HARD status type events, not SOFT ones.

Whether notifications are sent depends on the following parameters / characteristics (in this order);

•	notifications_enabled	global on/off parameter
•	Each host / service can have schedule	d downtime – no notifications in downtime
•	Each host / service can be "flapping" -	no notifications if flapping
•	Host notification_options (d,u,r)	specifies notifications on down, unreachable, recovery events
•	Service notification_options (w,u,c,r)	specifies notifications on service warning, unreachable, critical, recovery events
•	Host / service notification_period	notifications only sent during this period (eg. 24x7, workdays,)
•	Host / service notification_interval	if notification already sent, problem still extant and notification_period exceeded then send another notification

Once each of these filters for notification has been tested and passed, *contact* filters are then applied for each contact in the group(s) indicated in the host or service *contact_groups* stanza. Here is the default definition:

######################################	######################################		
********		***********************	
********	*******************************	***********************	
# Generic define con	contact definition template - ntact{	This is NOT a real conta	act, just a template!
ne	ame	generic-contact	; The name of this contact template
S	ervice notification period	24x7	; service notifications can be sent anutime
h	ost notification period	24x7	; host notifications can be sent anutime
S	ervice notification options	w,u,c,r,f,s	; send notifications for all service states, flapping events, and schedule
e events			
h	ost_notification_options	d,u,r,f,s	; send notifications for all host states, flapping events, and scheduled oe
Jents			
si hi ri	ervice_notification_commands ost_notification_commands egister	notify-service-by-email notify-host-by-email 0	; send service notifications via email ; send host notifications via email ; DONT REGISTER THIS DEFINITION - ITS NOT A REAL CONTACT, JUST A TEMPLATE!fl

Figure 24: Nagios Default contact definition

Notifications for hosts and services can be sent 24x7. They are sent for all types of events and use a Nagios command that drives the email system. As with all other Nagios configurations, more specific users and groups of users can be defined which change any of these parameters.

An event has to satisfy the global criteria, the specific host / service criteria and the contact criteria, before a notification is actually sent.

Remember from the Alerts Histogram report, it is possible to see notifications for a particular host.



Figure 25: Nagios Host Notifications

6.3.5 Automatic responses to events – event handlers

Nagios can run automatic actions (event handlers) when a service or host:

- Is in a SOFT problem state
- Initially goes into a HARD problem state
- Initially recovers from a SOFT or HARD problem state

There is a global parameter, *enable_event_handlers* which must take the value 1 (true), before any automation can take place.

There are two global parameters, *global_host_event_handler* and *global_service_event_handler* which can be used to run commands on all host / service events. These might be used, say, to log all events to an external file.

In addition, individual host and services (or groups of either) can have their own *event_handler* directive and their own *event_handler_enabled* directive. Note that if the global *enable_event_handlers* is off then no individual host / service will run event handlers. Individual event handlers will run immediately after and global event handler.

Typically, an event handler will be a script or program, defined in the Nagios commands.cfg file, to run any external program. The following parameters will be passed to the event handler:

For Services: \$SERVICESTATE\$, \$SERVICESTATETYPE\$, \$SERVICEATTEMP\$

For Hosts: \$HOSTSTATE\$, \$HOSTSTATETYPE\$, \$HOSTATTEMPT\$

Event handler scripts will run with the same user privilege as that which runs the nagios program.

Sample event handler scripts can be found in the *contrib/eventhandlers/* subdirectory of the Nagios distribution. Here is the sample submit_check_results command:



Figure 26: Nagios Sample submit_check_result command for event handler from contrib directory

6.4 Performance management

Nagios does not have performance data collection and reporting out-of-the-box; however, it does provide configuration parameters such that any host check or service check may also return performance data, provided the plugin supplies such data. This data can then either be processed by a Nagios command or the data can be written to a file to be processed asynchronously either by a Nagios command or by some other mechanism – mrtg, RRDTool and Cacti may all be contenders for the post-processing.

There are a number of global parameters that control the collection of performance data, typically in /usr/local/nagios/etc/nagios.cfg:

•	process_performance_data	global on/off switch
•	host_perfdata_command	Nagios command to be executed on data
•	service_perfdata_command	Nagios command to be executed on data
•	host_perfdata_file	datafile for asynchronous processing
•	service_perfdata_file	datafile for asynchronous processing

• Note – either use the command parameter for data processing when the data is retrieved, **or** use the data file for later processing

- host_perfdata_file_processing_interval
- process data file every <n> seconds

Nagios command to process data

- service_perfdata_file_processing_interval process data file every <n> seconds
- host_perfdata_file_processing_command
- service_perfdata_file_processing_command Nagios command to process data
- host_perfdata_file_template format of data file
- service_perfdata_file_template format of data file

```
🧧 jane@bino:~ - Shell - Konsole <2>
```

Session Edit View Bookmarks Settings Help	
# PROCESS PERFORMANCE DATA OPTION # This determines whether or not Nagios will process performance data returned from service and host checks. #If this option is enabled, host performance data will be processed using the host_perfdata_command #(defined below) and service performance data will be processed using the service_perfdata_command (also # defined below). Read the HTML docs for more information on performance data. # Values: 1 = process performance data, 0 = do not process performance data process_performance_data=1	
 # These commands are run after every host and service check is performed. These commands are executed only # if the enable_performance_data option (above) is set to 1. The command argument is the short name of a # more information on performance data. # Don't use these - use data files option below - JC # host_perfdata_command=process-host-perfdata # service_perfdata_command=process-service-perfdata 	
<pre># HOST AND SERVICE PERFORMANCE DATA FILES # These files are used to store host and service performance data. Performance data is only written to # these files if the enable_performance_data option (above) is set to 1. host_perfdata_file=/tmp/host-perfdata service_perfdata_file=/tmp/service-perfdata</pre>	
<pre># HOST AND SERVICE PERFORMANCE DATA FILE TEMPLATES # These options determine what data is written (and how) to the performance data files. The templates #may contain macros, special characters (\t for tab, \r for carriage return, \n for newline) and plain text. #A newline is automatically added after each write to the performance data file. Some examples of what #you can do are shown below. host_perfdata_file_template=LHOSTPERFDATA]\t\$TIMET\$\t\$HOSTNAME\$\t\$HOSTEXECUTIONTIME\$\t\$HOSTOUTPUT\$\t\$HOSTPERFDATA\$ service_perfdata_file_template=LSERVICEPERFDATA]\t\$TIMET\$\t\$HOSTNAME\$\t\$SERVICEDESC\$\t\$SERVICEEXECUTIONTIME\$\t\$SERVICEATENCY\$</pre>	Nt
<pre># HOST AND SERVICE PERFORMANCE DATA FILE MODES # This option determines whether or not the host and service performance data files are opened in #write ("w") or append ("a") mode. If you want to use named pipes, you should use the special pipe ("p") mode # which avoid blocking at startup, otherwise you will likely want the defult append ("a") mode. host_perfdata_file_mode=a service_perfdata_file_mode=a</pre>	
<pre># HOST AND SERVICE PERFORMANCE DATA FILE PROCESSING INTERVAL # These options determine how often (in seconds) the host and service # performance data files are processed using the commands defined # below. A value of 0 indicates the files should not be periodically # processed. host_perfdata_file_processing_interval=0 service_perfdata_file_processing_interval=0</pre>	
<pre># HOST AND SERVICE PERFORMANCE DATA FILE PROCESSING COMMANDS # These commands are used to periodically process the host and # service performance data files. The interval at which the # processing occurs is determined by the options above. host_perfdata_file_processing_command=process-host-perfdata-file service_perfdata_file_processing_command=process-service-perfdata-file</pre>	•
790,0-1 65	× •
	29

Figure 27: Nagios Performance parameters in nagios.cfg

The default is that process_performance_data=0 (ie. off) and all the other parameters are commented out.

In addition to the global parameters, each host and service needs to either explicitly configure or inherit a definition for:

• process_perf_data = 1 1 = data collection on, 0 = data collection off

By default, the *generic_host* and *generic_service* template definitions set these parameters to $\mathbf{1}$ (on).

If a Nagios plugin is able to provide performance data, it is returned after the usual status information, separated by a | (pipe) symbol. It can be retrieved as the \$HOSTPERFDATA\$ or \$SERVICEPERFDATA\$ macro. It is then upto your Nagios commands to interpret and manipulate that data.

The next figure shows performance data that has been gathered into /tmp/serviceperfdata using the default service_perfdata_file_template where the last field is the \$SERVICEPERFDATA\$ value (if the plugin delivers performance data).

💻 jane@bino:~ - Shell -	Konsole <2>			
Session Edit View Bo	okmarks Settings	s Help		
[SERVICEPERFDATA]	1217865172 4 28 155 time=0	bino DNS Check	0.033 0.02	5 DNS DK: 0.017 seconds response time. www.skills- 🔺
[SERVICEPERFDATA]	1217865192	bino SNMP Check	0.093 0.04	0 SNMP OK - Timeticks: (30534541) 3 days, 12:49:05
.41 DISMAN-EVENT-MI	B::sysUpTimeInst	ance=Timeticks: (3053454	1) 3 days, 12	:49:05.41
[SERVICEPERFDATA]	1217865252	group-100-r3 PING	4.188 0.13	2 PING OK - Packet loss = 0%, RTA = 120.84 ms
[SERVICEPERFDATA]	1217865272	nagios PING 3.030	0.086 CRIT	ICAL - Host Unreachable (nagios.skills-1st.co.uk)
[SERVICEPERFDATA]	1217865272	group-100-c2 PING	4.297 0.13	9 PING CRITICAL - Packet loss = 0%, RTA = 937.61 m
s				
[SERVICEPERFDATA]	1217865282	nagios3 Current Users	0.016 0.04	6 USERS OK - 5 users currently logged in users=5;
20;50;0		3		· · · · · · · · · · · · · · · · · · ·
[SERVICEPERFDATA]	1217865292	aroun-100-s1 PING	4.122 0.03	3 PING OK - Packet loss = 0%, RTA = 93.32 ms
I SERVICEPERFDATA1	1217865292	aroun-100-r1 PING	4.035 0.10	0 PING OK - Packet loss = 0%, RTA = 8.36 ms
I SEBUICEPERFDATA 1	1217865302	nagios3 Boot Partition	0.010 0.24	5 DISK OK - free snace: / 784 MB (16% inode=69%):
2=4001MB:4536:4788:0:50	41	Sector Se		
I SEBUICEPERFDATA1	1217865332	server PING 4.585	0.214 PING	OK - Packet loss = 0%, BTA = 0.70 ms
I SEBUICEPERFDATA 1	1217865332	aroun-100-c2 PING	4.092 0.04	1 PING OK - Packet loss = 0% . RTA = 134.27 ms
I SEBUICEPERFDATA 1	1217865342	hino PING 4.019	0.156 PING	ΩK - Packet loss = $\Omega \gamma$. BTA = Ω 35 ms
ISEBUICEPERFDATA1	1217865362	aroun-100-c1 PING	4 130 0.08	7 PING OK - Packet loss = 0% , RTA = 98 93 ms
ISERUICEPEREDATA1	1217865382	group-100-c3 PING	4 114 0 00	8 PING OK - Packet loss = 0% RTA = 81 77 ms
ISFRILICEPEREDATA 1	1217865402	group-100-r2 PING	4 172 0 22	5 PING OK - Packet loss = 0% RTA = 150 30 ms
ISERUICEPEREDATA 1	1217865432	nagios3 Current Load	0.011 0.05	6 OK - load auerage: 0.03. 0.04. 0.01 load1=0
030:5 000:10 000:0: loa	45=0 040:4 000:6	000:0: load15=0 010:3 0	0.011 0.03	b bh ibuu uociuge: 0.03, 0.01, 0.01 ibuu1-0.
ISFRILICEPEREDATA1	1217865462	pagios3 PING 4 A14	0 233 PING	OK - Packet loss = AV RTA = A A5 ms
ISERUICEPEREDATA 1	1217865472	nagios3 Total Processes	0.027 0.18	8 PROCS OK: 45 mocesses with STATE = RSZDT
ISERUICEPEREDATA 1	1217865472	hino DNS Check	0.025 0.20	3 DNS DK' A A13 seconds response time www.skills-
1st co uk returns 212 7	4 28 155 time=0	0131115::::0 000000	0.000 0.20	5 Mile on Store Sconds response time, WWW.SKIIIS
ISTRILICEPEREDATA 1	1217865552	aroun-100-r3 PING	4 513 0 17	3 PING OK - Packet loss = 0% RTA = 185 76 ms
	1011000000	group too 15 1 Ind	1.515 0.16	5 HIM ON THERE TOSS - 0/, JUN - 105.10 MS
"/tmp/service-perfdata"	[readonly] 570	lines100%		570,60-81 Bot 🔽
🛃 🖷 Shell				<u>A</u>

Figure 28: Nagios Performance data collected into /tmp/service-perfdata

The most recent performance data gathered for hosts and services can also be seen from the *Host Detail* or *Service Detail* menu options.



Figure 29: Nagios Performance data highlighted DNS Check service

6.5 Nagios summary

Nagios is a mature *systems* management tool whose documentation is much better than the other open source offerings. It's strength is in checking availability of hosts and services that run on those hosts. Support for network management is less strong as there is no automatic discovery; however it *is* possible to configure simple network topologies and it includes the concept of a set of devices being UNREACHABLE (rather than DOWN) if there is a network single-point-of-failure. Handling meshed networks with multiple routing paths to a network is problematical.

Since all monitoring is performed by plugins, some of which come with the product and some of which are available as community contributions, the tool is as flexible as anyone requires. There are a large number of plugins available and you can also write your own.

One of the standard plugins is *check_snmp* which can be used to query any host for any SNMP MIB variable; this obviously requires the target to support SNMP and the MIB in question.

It is also possible to run checks on remote hosts by installing the NRPE agent (available for both Unix / Linux and Windows hosts) and the required Nagios plugins, on the remote system. The check_nrpe plugin must also be installed on the Nagios system. This allows plugins designed to be run local to the Nagios system, to be run on remote hosts. With NRPE agents, checks are run on a scheduled basis, initiated from the Nagios system.

Another alternative is to install the NSCA addon to remote systems. This permits remote machines to run their own periodic checks and report the results back to Nagios, which can be defined as *passive* service checks.

The event subsystem of Nagios is less powerful and configurable than some of the other offerings – it has less focus on an "event console" but includes more information about host and service events from other menus. Nagios has no easy built-in way to collect and process SNMP TRAPs.

If you want lots of performance graphs then Nagios alone is not going to deliver easily.

In summary, Nagios seems good for monitoring a relatively small number of systems, provided you don't need historical performance reporting.

7 OpenNMS

OpenNMS presents itself as "the first Enterprise-grade network management platform developed under the Open Source model". It is a Java application that runs under several flavours of Linux. A VM ware Virtual Machine (VM) is also available with the latest release of OpenNMS, which makes initial evaluation very easy without having to go through a full build process. There is also an online demo system which appears to be monitoring real kit which gives a good "first taste" of the product.

The following section is based on the VM download which is OpenNMS 1.5.93 based on Mandriva - it worked very easily. The VM was setup for DHCP but I modified the Operating System files to use a local fixed address, with the VM network bridged to my local environment.

To access the OpenNMS Web Console, point your browser at <u>http://opennms:</u> <u>8980/opennms/</u>. The default logon id is admin with a password of admin .

Here is a screenshot of the main default window of OpenNMS.

🧿 OpenNMS Web Console - Mozil	la Firefox						
Eile Edit View History Bookmarks Tools Help							
 - C 10 11 12 12 13 14 <li< td=""><td colspan="7">🖨 🔹 🐟 - 🧭 💿 🏠 🗋 http://opennms:8980/opennms/index.jsp</td></li<>	🖨 🔹 🐟 - 🧭 💿 🏠 🗋 http://opennms:8980/opennms/index.jsp						
📕 👷 Firefox Support 💹 Plug-in FA	Q CRSS Feeds						
OpenNMS Web Console	Nagios 🖂			·			
open NMS [®]	Node List Search Outages Path Outages D	Pashboard Events Alarms	Notifications Assets	Web Console User: admin (Notices On) - Log out 30-Jun-2008 23:43 GMT-05:00 Reports Charts Surveillance Map Admin Help			
Home Nodes with Outages	Percentage change over past 24 hou	rs		Notification			
hp7410 (18 hours)	Categories	Outages	Availability	You: 6 outstanding notices (Check)			
switch.skills-1st.co.uk (3 days)	Network Interfaces	3 of 36	86.691%	All: 6 outstanding notices (Check)			
Ciscolakina Isticoluk (5 daya)	Web Servers	2 of 12	83.927%				
	Email Servers	0 of 0	100.000%	Resource Graphs			
	DNS and DHCP Servers	0 of 10	94.905%	Choose a node 💌			
	Database Servers	0 of 2	99.976%	KSC Reports			
	JMX Servers	0 of 0	100.000%	No KSC reports defined			
	Other Servers	0 of 16	95.195%				
	Total	Outages	Availability				
	Overall Service Availability	5 of 79	89.874%				
OpenNM	S Copyright © 2002-2008 The OpenNMS Group, I	inc. OpenNMS® is a register	ed trademark of The Ope	nNMS Group, Inc.			

Figure 30: Main default window for OpenNMS

The following sections will describe how to configure different aspects of OpenNMS by editing xml configuration files. It is possible to configure many aspects of OpenNMS using GUI-driven menus. See section 7.5 "Managing OpenNMS" for a brief description.

7.1 Configuration – Discovery and topology

7.1.1 Interface discovery

OpenNMS uses a straightforward file for interface discovery – by default this is /opt/opennms/etc/discovery-configuration.xml . It comes with some commented-out defaults, so by default it discovers nothing! This file needs modifying to specify include ranges and exclude ranges to ping; specific IP addresses for discovery can also be configured. The first stanza specifies the characteristics of the ping discovery mechanism. If there is a response within the timeout, a "new suspect" event is generated.

In the above example, ping discovery will start 300,000 ms (5 minutes) after OpenNMS has started up; the discovery process will be restarted every 86,400,000 ms (24 hours); 1 ping will be sent per second; the timeout for a ping will be 800 ms and there will be 3 ping retries before the discovery process gives up on an address. All devices on the Class C 10.0.0.0 network will be polled (with only 2 retries but a 3 second timeout). The 10 devices 172.30.100.1 through 10 will be polled for with the default characteristics. The specific node 10.191.101.1 will be polled.

All that the discover process does is to generate "new suspect" events that are then used by other OpenNMS processes. If the device does not respond to this ping polling then it will not be added to the OpenNMS database.

Another way to generate such events (say for a box that does not respond to ping), is to use a provided Perl script:

/opt/opennms/bin/send-event.pl –interface <ip addr> uei.opennms.org/internal/discovery/newsuspect

7.1.2 Service discovery

When a "new suspect" event has been generated by the discovery process it is the capabilities daemon, *capsd*, that takes over and discovers services on a system. capsd is configured using /opt/opennms/etc/capsd-configuration.xml . Thus, discovery in OpenNMS consists of two parts: discovering an IP address to monitor (the discover process) and then discovering the services supported by that IP address (the capsd process).

The basic monitored element is called an "interface", and an interface is uniquely identified by an IP address. Services are mapped to interfaces, and if a number of interfaces are discovered to be on the same device (either via SNMP or SMB) then they may be grouped together as a "node".

capsd uses a number of plugins supplied with OpenNMS, to discover services. Each service has a <protocol-plugin> stanza in capsd-configuration.xml. For example:

```
<protocol-plugin protocol="SSH" class-name="org.opennms.netmgt.capsd.TcpPlugin"
scan="on" user-defined="false">
        <property key="banner" value="SSH"/>
        <property key="port" value="22"/>
        <property key="timeout" value="3000"/>
```

```
<property key="retry" value="1"/></protocol-plugin>
```

This defines a service (protocol) called SSH that tests TCP port 22 using the TCP plugin. It will look for the string "SSH" to be returned. Timeout is 3 seconds with 1 retry.

The first protocol entry in capsd-configuration.xml is for ICMP.

</protocol-plugin>

It is possible to apply protocols to specific address ranges or exclude protocols from address ranges (the default is inclusion).

```
<protocol-plugin protocol="ICMP"
```

</protocol-plugin>

Note the "scan=off" for IP addresses 172.31.100.1 - 15.

The SNMP protocol is special in that, if supported, it provides a way to collect performance data as well as poll for availability management information. SNMP parameters for different devices and ranges of devices are specified in /opt/opennms/etc/snmp-config.xml. Here is a sample:

```
</snmp-config>
```

The first stanza in snmp-config.xml provides global default parameters for SNMP access. Variations in any of these global parameters can be made using a "definition" stanza and either a range or a specific statement. This file is used both for discovery and for collecting performance data.

When testing SNMP, capsd makes an attempt to receive the sysObjectID MIB-2 variable (.1.3.6.1.2.1.1.2.0). If successful, then extra discovery processing takes place. First, three threads are generated to collect the data from the SNMP MIB-2 system tree and the ipAddrTable and ifTable tables. If, for some reason, the ipAddrTable or ifTable are unavailable, the process stops (but the SNMP system data may show up on the node page).

Second, all of the IP addresses in the ipAddrTable are run through the capsd capabilities scan. Note that this is regardless of how management is configured in the configuration file. This only happens on the initial scan and on forced rescans. On normal rescans (by default, every 24 hours), IP addresses that are "unmanaged" in capsd are not polled.

Third, every IP address in the ipAddrTable that supports SNMP is tested to see if it maps to a valid ifIndex in the ifTable. If this is true, the IP address is marked as a secondary SNMP interface and is a contender for becoming the primary SNMP interface.



Figure 31: OpenNMS node detail for a switch showing switch ports

The first stanza in capsd-configuration.xml defines service polling parameters:

```
<capsd-configuration rescan-frequency="86400000"
initial-sleep-time="300000"
management-policy="managed"
max-suspect-thread-pool-size = "6"
max-rescan-thread-pool-size = "3"
abort-protocol-scans-if-no-route = "false">
```

This defines that capsd will wait 5 minutes after OpenNMS starts before starting the capsd discovery process. It will rescan to discover services every 24 hours. The default management policy for all IP addresses found in "new suspect" events will be to scan for each of the services. This "managed" parameter can be overridden at the end of capsd-configuration.xml by unmanaged-range stanzas:

```
<ip-management policy="unmanaged">
        <specific>0.0.0.0</specific>
        <range begin="127.0.0.0" end="127.255.255.255"/>
</ip-management>
```

When a "new suspect" event is generated, provided the IP address is in a "managed" management-policy range, the IP address is checked for each of the services in capsd-configuration.xml, starting from the top.

If the device does not respond to any configured service then, even if triggered with send_event.pl, it will not be added to the OpenNMS database. Look in /opt/opennms/logs/daemon/discovery.log for debugging information.

7.1.3 Topology mapping and displays

OpenNMS does not use a topology mapping function in the core code (indeed, some of its proponents are vociferous that you do not need a mapping ability). There *is* a mapping capability if you use an Internet Explorer web browser with a specific Adobe Scalable Vector Graphics (SVG) plugin – this is only supported in IE and did not work for me. There is also a maps-on-firefox code branch but performance is said to be poor and the maillists suggest that neither mapping capability is heavily used.

A Node List is available from the main menu where each node name is a link to a detailed node page.



Figure 32: OpenNMS Node List of discovered nodes

group-10	0-r1.class.example	e.org No	ode OpenN	MS Web C	onsole - Mo	zilla F	irefox						
ile <u>E</u> dit <u>V</u> i	ew Hi <u>s</u> tory <u>B</u> ookr	marks <u>T</u> e	ools <u>H</u> elp										
group-10	0-r1.class.exa 🕻	Na Na	gios										
Home / Sea Node: group View Events	orch / Node o-100-r1.class.exa View Alarms Asset Inf	mple.org o Telnet	Resource Gr	aphs Rescan	Admin Upda	te SNM	IP						
General (St	atus: Active)				Notificati	on							
View Node Lir	nk Detailed Info				You: Outs You: Ackr	tandin Iowled	ig: (Check) Iged: (Check)						
Availability	5	_			Pacant Ex	ante							
Availability	(last 24 hours)	89.2429	6		E uner	20/06	6/09 16:49:52	No	rm al	Interface 172 20	100 1 is up		
		Overall	89.28	36%	1 44965	30/00	0/00 10.40.32	NO	innai	Internace 172.30.	100.1 is up.		
		ICMP	89.28	36%	44923	30/06	6/08 16:47:35	Mir	nor	Interface 172.30.	100.1 is down.		
10.191.100	.4	Router	Not M	Ionitored	43842	30/06	6/08 14:40:58	Mir	nor	Alarm #281 for n interface:10.191.	ode:group-100-r1.class.ex. 100.4; service:SNMP; was	ample.org; escalated.	
		SNMP	Not M	Ionitored	F 10000	20/04	6/09 12:40-56	Mir		Alarm #281 for n	ode:group-100-r1.class.ex	ample.org;	
		StrafePi	ng Not M	Ionitored	1 43333	30/00	0/08 13:40:30	MII		interface:10.191.	100.4; service:SNMP; was	escalated.	
-		Telnet	Not M	lonitored	F 42752	F 42752 30/06/08 12:40:53		Mir	nor	SNMP data collection on interface 10.191.100.4 failed.			
	8	Overall	89.19	97%	Acknowle	dge	Reset	More					
		ICMP	89.19	97%					_				
172.30.100	.1	Router	Not M	Ionitored	Recent Ou	itages							
		SNMP	Not M	Ionitored	Interface		Service	Lost			Regained	Outage	ID
	0	StrafePi	ng Not M	lonitored	172.30.100	.1	ICMP	30/06/08 16:47:35		16:47:35	30/06/08 16:48:52	102	
		Telnet	Not M	lonitored	172.30.100	.1	ICMP	29/0	6/08	23:36:44	30/06/08 01:45:35	57	
SNMP Attrib Name	utes group-100-r1.class.ex	ample.org			10.191.100	.4	ІСМР	29/0	6/08	23:36:44	30/06/08 01:45:35	58	
Location	Virtual comms rack 10	10											
Contact	Andrew.Findlay@skills	-1st.co.uk											
Description	Cisco Internetwork Op 7200 Software (C7200 SOFTWARE (fc1).Copy IncCompiled Tue 11-	erating Sy: I-DS-M), Ve rright (c) 19 Jul-00 02:0	stem Software . Irsion 12.0(12), 186-2000 by ciso 9 by htseng	IOS (tm) RELEASE co Systems,									
Interfaces Interface		Index	Description	IfAlias									
10.191.100.4 (group-100-	1 r1.class.example.org)	2	astEthernet0/0	Main site network									
172.30.100.	L 1.class.example.org)	3 9	Serial1/0	E1 line to remote									

Figure 33: OpenNMS node detail for group-100-r1

Note the services that have been discovered for the node. The list of services per interface are those that have been actually detected; whether they are "Monitored" or not will be discussed in the next section.

7.2 Availability monitoring

OpenNMS performs availability monitoring by polling devices with processes known as *monitors* which connect to a device and perform a simple test. Polling only happens to an interface that has already been discovered by capsd.

The configuration file for polling is /opt/opennms/etc/poller-configuration.xml. There are many similarities between this and capsd-configuration.xml; however the monitors are defined with "monitor service" stanzas (rather than "protocol" stanzas), which define the Java class to use for monitoring.

<monitor< th=""><th>service="DominoIIOP"</th><th>class-name="org.opennms.netmgt.poller.DominoIIOPMonitor"/></th></monitor<>	service="DominoIIOP"	class-name="org.opennms.netmgt.poller.DominoIIOPMonitor"/>
<monitor< td=""><td>service="ICMP"</td><td><pre>class-name="org.opennms.netmgt.poller.IcmpMonitor"/></pre></td></monitor<>	service="ICMP"	<pre>class-name="org.opennms.netmgt.poller.IcmpMonitor"/></pre>
<monitor< td=""><td>service="Citrix"</td><td><pre>class-name="org.opennms.netmgt.poller.CitrixMonitor"/></pre></td></monitor<>	service="Citrix"	<pre>class-name="org.opennms.netmgt.poller.CitrixMonitor"/></pre>
<monitor< td=""><td>service="LDAP"</td><td><pre>class-name="org.opennms.netmgt.poller.LdapMonitor"/></pre></td></monitor<>	service="LDAP"	<pre>class-name="org.opennms.netmgt.poller.LdapMonitor"/></pre>
<monitor< td=""><td>service="HTTP"</td><td><pre>class-name="org.opennms.netmgt.poller.HttpMonitor"/></pre></td></monitor<>	service="HTTP"	<pre>class-name="org.opennms.netmgt.poller.HttpMonitor"/></pre>
<monitor< td=""><td>service="HTTP-8080"</td><td><pre>class-name="org.opennms.netmgt.poller.HttpMonitor"/></pre></td></monitor<>	service="HTTP-8080"	<pre>class-name="org.opennms.netmgt.poller.HttpMonitor"/></pre>
<monitor< td=""><td>service="HTTP-8000"</td><td><pre>class-name="org.opennms.netmgt.poller.HttpMonitor"/></pre></td></monitor<>	service="HTTP-8000"	<pre>class-name="org.opennms.netmgt.poller.HttpMonitor"/></pre>
<monitor< td=""><td>service="HTTPS"</td><td><pre>class-name="org.opennms.netmgt.poller.HttpsMonitor"/></pre></td></monitor<>	service="HTTPS"	<pre>class-name="org.opennms.netmgt.poller.HttpsMonitor"/></pre>
<monitor< td=""><td>service="SMTP"</td><td><pre>class-name="org.opennms.netmgt.poller.SmtpMonitor"/></pre></td></monitor<>	service="SMTP"	<pre>class-name="org.opennms.netmgt.poller.SmtpMonitor"/></pre>
<monitor< td=""><td>service="DHCP"</td><td><pre>class-name="org.opennms.netmgt.poller.DhcpMonitor"/></pre></td></monitor<>	service="DHCP"	<pre>class-name="org.opennms.netmgt.poller.DhcpMonitor"/></pre>
<monitor< td=""><td>service="DNS"</td><td><pre>class-name="org.opennms.netmgt.poller.DnsMonitor" /></pre></td></monitor<>	service="DNS"	<pre>class-name="org.opennms.netmgt.poller.DnsMonitor" /></pre>
<monitor< td=""><td>service="FTP"</td><td>class-name="org.opennms.netmgt.poller.FtpMonitor"/></td></monitor<>	service="FTP"	class-name="org.opennms.netmgt.poller.FtpMonitor"/>
<monitor< td=""><td>service="SNMP"</td><td><pre>class-name="org.opennms.netmgt.poller.SnmpMonitor"/></pre></td></monitor<>	service="SNMP"	<pre>class-name="org.opennms.netmgt.poller.SnmpMonitor"/></pre>
<monitor< td=""><td>service="0racle"</td><td>class-name="org.opennms.netmgt.poller.TcpMonitor"/></td></monitor<>	service="0racle"	class-name="org.opennms.netmgt.poller.TcpMonitor"/>
<monitor< td=""><td>service="Postgres"</td><td><pre>class-name="org.opennms.netmgt.poller.TcpMonitor"/></pre></td></monitor<>	service="Postgres"	<pre>class-name="org.opennms.netmgt.poller.TcpMonitor"/></pre>
<monitor< td=""><td>service="MySQL"</td><td>class-name="org.opennms.netmgt.poller.TcpMonitor"/></td></monitor<>	service="MySQL"	class-name="org.opennms.netmgt.poller.TcpMonitor"/>
<monitor< td=""><td>service="Sybase"</td><td><pre>class-name="org.opennms.netmgt.poller.TcpMonitor"/></pre></td></monitor<>	service="Sybase"	<pre>class-name="org.opennms.netmgt.poller.TcpMonitor"/></pre>
<monitor< td=""><td>service="Informix"</td><td>class-name="org.opennms.netmgt.poller.TcpMonitor"/></td></monitor<>	service="Informix"	class-name="org.opennms.netmgt.poller.TcpMonitor"/>
<monitor< td=""><td>service="SQLServer"</td><td>class-name="org.opennms.netmgt.poller.TcpMonitor"/></td></monitor<>	service="SQLServer"	class-name="org.opennms.netmgt.poller.TcpMonitor"/>
<monitor< td=""><td>service="SSH"</td><td><pre>class-name="org.opennms.netmgt.poller.TcpMonitor"/></pre></td></monitor<>	service="SSH"	<pre>class-name="org.opennms.netmgt.poller.TcpMonitor"/></pre>
<monitor< td=""><td>service="IMAP"</td><td><pre>class-name="org.opennms.netmgt.poller.ImapMonitor"/></pre></td></monitor<>	service="IMAP"	<pre>class-name="org.opennms.netmgt.poller.ImapMonitor"/></pre>
<monitor< td=""><td>service="POP3"</td><td><pre>class-name="org.opennms.netmgt.poller.Pop3Monitor"/></pre></td></monitor<>	service="POP3"	<pre>class-name="org.opennms.netmgt.poller.Pop3Monitor"/></pre>
<monitor< td=""><td>service="NSClient</td><td>class-name="org.opennms.netmgt.poller.NsclientMonitor"/></td></monitor<>	service="NSClient	class-name="org.opennms.netmgt.poller.NsclientMonitor"/>
<monitor< td=""><td>service="NSClientpp</td><td>class-name="org.opennms.netmgt.poller.NsclientMonitor"/></td></monitor<>	service="NSClientpp	class-name="org.opennms.netmgt.poller.NsclientMonitor"/>
<monitor s<="" td=""><td>ervice="Windows-Task-Schedu</td><td>ler" class-name="org opennms netmat poller Win32ServiceMonitor"/></td></monitor>	ervice="Windows-Task-Schedu	ler" class-name="org opennms netmat poller Win32ServiceMonitor"/>

Preceding the "monitor service" stanzas in poller-configuration.xml are the definitions of "services". These look very similar to the entries in capsd-configuration.xml (which makes sense as this is the regular polling definitions for the *same* services that capsd has already found); however parameters in the poller file may well take different values (for example, the discovery service may be allowed longer timeouts and more retries than the polling service).

Note that the default poller-configuration.xml has the SNMP monitor service turned off.

Services may be defined several times with different parameters – each service will obviously require a unique name. This is so that different devices can receive availability monitoring with different characteristics.

For availability polling, devices are grouped together in *packages*, where a package defines:

- target interfaces
- services including the polling frequency

- a downtime model (which controls how the poller will dynamically adjust its polling on services that are down)
- an outage calendar that schedules times when the poller is *not* to poll (i.e. scheduled downtime).

There are two packages defined in the default poller-configuration.xml file, example1 and a separate package, strafer, to monitor StrafePing. A package definition must include a single "filter" stanza; it may also have "specific", "include-range" and "exclude-range" stanzas. Here is the start of the default, as shipped:

```
<package name="example1">
        <filter>IPADDR != '0.0.0.0'</filter>
        <include-range begin= 1.1.1.1 end= 254.254.254.254 />
```

It is then followed by the list of services pertinent to that package – example1 includes many of the services, with each service set to *status="on"* except SNMP.

The opening stanza in poller-configuration.xml controls the overall behaviour of polling:

```
<poller-configuration threads="30"
    serviceUnresponsiveEnabled="false"
    nextOutageId= SELECT nextval('outageNxtId')
    xmlrpc= false >
    <node-outage status="on"
        pollAllIfNoCriticalServiceDefined="true">
        <critical-service name="ICMP"/>
        </node-outage>
```

30 threads are available for polling. The basic event that is generated when a poll fails is called "NodeLostService". If more than one service is lost, multiple NodeLostService events will be generated. If all the services on an interface are down, instead of a NodeLostService event, an "InterfaceDown" event will be generated. If all the interfaces on a node are down, the node itself can be considered down, and this section of the configuration file controls the poller behaviour should that occur. If a "NodeDown" event occurs and *node-outage status="on"* then all of the InterfaceDown and NodeLostService events will be suppressed and only a NodeDown event will be generated. Instead of attempting to poll all the services on the down node, the poller will attempt to poll only the "critical-service". Once the critical service returns, the poller will then resume polling the other services.

Note in the following screenshot that six services have been discovered on the 10.0.0.95 interface of the node called deodar.skills-1st.co.uk, of which four are monitored. The two interfaces on the 172.16 network have been detected through SNMP queries but there is no monitoring of any services on these networks. There are no current issues with deodar and availability has been 100% over the last 24 hours.

🎯 deodar.skills-1st.co.uk	(Node OpenNM	S Web Console - I	Mozilla Firefox				
<u>File</u> <u>E</u> dit <u>V</u> iew History <u>E</u>							
🤙 • 💩 • 🤁 🐼 🏠 [🔹 🐟 🗸 🙋 🔗 🎊 🗅 http://opennms:8980/opennms/element/node.isp?node=20. 🔹 🔊 🖸						
N Nagios	B deodar sl	rille-1et co 🛛 🔯			a Categor		et: Par D
open NMS	OPENNMS 03-Jul-2008 03:46 GMT-05:00						
	Node List Se	arch Outages Path	Outages Dashboa	rd Events Alarms	Notifications	Assets Reports Charts Surveillance Map	Admin Help
Home / Search / Node Node: deodar.skills-1st.c View Events View Alarms Ass	co.uk set Info Resource	Graphs Rescan Adm	in Update SNMP				
General (Status: Active)			Notification				
View Node Link Detailed Info			You: Outstar You: Acknow	nding: (Check) vledged: (Check)			
Availability (last 24 hours)	100.000%		Recent Even	ts			
Availability (last 24 riours)	Overall	100.000%	66350	02/07/08 07:09:26	Normal	A services scan has been completed on this no	de.
	DNS	100.000%	52625	01/07/08 07:02:17	Normal	A services scan has been completed on this no	de.
	ICMP	100.000%	39716	30/06/08 06:56:36	Normal	A services scan has been completed on this no	de.
10.0.0.95	Router	Not Monitored	□ 27442	29/06/08 06:50:07	Normal	A services scan has been completed on this no	de.
	SNMP	100.000%	□ 26252	29/06/08 04:25:50	Normal	A services scan has been completed on this no	de.
	SSH	100.000%	Acknowledg	e Reset	More		
	StrafePing	Not Monitored					
172.16.224.1	Overall	Not Monitored	Recent Outa	ges			
172.16.225.1	Overall	Not Monitored	There have be	en no outages on this r	ode in the la	st 24 hours.	
SNMP Attributes							
Name deodar							
Object ID .1.3.6.1.4.1.807	2.3.2.10						
Location Cedar Chase	Location Cedar Chase						
Contact Jane Curry	Contact Jane Curry						
Description Linux deodar 2.	6.18.8-0.5-default #1 SI	MP Fri Jun 22					_
12:17:53 010 2	00/ x86_64						
Interfaces							
Interface	Index	Description					
10.0.0.95 (deodar.skills-1st.c	o.uk) 2	eth0					
172.16.224.1	4	vmnet1					
172.16.225.1	5	vmnet8					•

Figure 34: OpenNMS node detail with monitored services

OpenNMS includes a standard set of Availability reports. They can be selected from the Reports menu:



Figure 35: OpenNMS Availability reports menu

Here is a sample:



Figure 36: OpenNMS Overall service availability report

Note that there is an /opt/opennms/etc/examples directory with extra samples of all the OpenNMS configuration files.

Also note that OpenNMS needs recycling if any configuration files have been modified. Use:

/etc/init.d/opennms stop

/etc/init.d/opennms start

7.3 Problem management

For problem management, OpenNMS has the concepts of:

- Events all sorts of both good and bad news
- Alarms "important" events
- Notifications typically email or pager but could be other methods

The events subsystem is driven by the eventd process which listens on port 5817. Outof-the-box, eventd receives internal events from OpenNMS (such as "new suspect" events) and SNMP TRAPs. It is possible to also configure for other event sources (such as from syslogs).

7.3.1 Event console

Events can be viewed from the web GUI by selecting the "Events" option.

	09-Jul-2008 09:01 GMT-05:00
Node List Search Outages Pat	h Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Map Admin Help
Home / Events	
Event Queries	Outstanding and acknowledged events
Event ID: Get details All events Advanced Search	Events can be acknowledged, or removed from the view of other users, by selecting the event in the Ack check box and clicking the Acknowledge Selected Events at the bottom of the page. Acknowledging an event gives users the ability to take personal responsibility for addressing a network or systems-related issue. Any event that has not been acknowledged in serior, you can select the View all acknowledged events link, find the event, and unacknowledge it, making it available again to all users' views. If you have a specific event identifier for which you want a detailed event description, type the identifier into the Get details for Event ID box and hit [Enter]. You will then go to the appropriate details page.

Figure 37: OpenNMS Events menu

The "Advanced Search" option provides several ways to filter events. By default "Outstanding" events are displayed (ie. events that have not been Acknowledged).

open NMS [®]		Advanced Event Search User: admin (Notices On) - Log out 09-Jul-2008 09:04 GMT-05:00
	Node List Search Outages Path Outag	es Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Map Admin Help
Home / Events / Advanced Eve	nt Search	
Advanced Event Search		Searching Instructions
Event Text Contains:	TCP/IP Address Like:	The Advanced Event Search page can be used to search the event list on multiple fields. Fill in values for each field that you wish to use to narrow down the search.
	..*	To select events by time, first check the box for the time range that you wish to limit and then fill out the time in the boxes provided
Node Label Contains: Severity:		If you wish to select events within a specific time span, check <i>both</i> boxes and enter the beginning and end of the range in the boxes provided.
Service:		
Events After:	Events Before:	
9 🗾 04 🛛 AM 💻	9 • 04 AM •	
Jul 🔄 9 2008	9 2008	
Sort By:	Number of Events Per Page:	
Event ID (Descending)	10 events 💌	
Search		

Figure 38: OpenNMS Advanced Event Search options

Note that if you wish to search on severity, you have to specify an exact severity; you cannot specify "severity greater than....".

🎯 Li	🥹 List Events OpenNMS Web Console - Mozilla Firefox						
<u>F</u> ile I	File Edit View History Bookmarks Tools Help						
✓ · → · <					Q)		
				D Source Forge pet: Dert	Caarab raquita		in energy (
	st Even	ts Openiv (SourceForge.net. Part L	Search results - O		in opennins 🖬 💌
open NMS® User: admit 09-Jul-				User: admin 09-Jul-20	Event List (Notices On) - Log out 08 09:21 GMT-05:00		
			Node List Search Ou	tages Path Outages Dashboard Events Al	arms Notifications Assets	Reports Charts Surveillance	Map Admin Help
Hon	ne / Even	ts / List					
View	all events	Advanced Search	Severity Legend Acknowledge e	ntire search			
Even	t Text:		Time: Any 💌 Se	arch			
Resu	, lts: (1-10 of	1689)					
Sear	ch constrain	ts: Event(s) outst	anding [-]			1 2	3 4 5 Next Last
_			Terres		Phone and a second s	Legend	
Ack	V ID	<u>Severity</u>	Time	Node	<u>Interface</u>	<u>Service</u>	Ackd
	151463	Normal [+] [-]	09/07/08 09:20:06 [<] [>]				
			uei.opennms.org/internal/authentic	cation/sessionRemoved [+] [-] Edit notifications	for event		
			OpenNMS user 'rtc' has been logge	d out of the WebUI, most likely due to a session	timeout.		
	151455	Normal [+] [-]	09/07/08 09:19:58 [<] [>]				
			uei.opennms.org/internal/authentic	cation/successfulLogin [+] [-] Edit notifications fo	ir event		
_	151202	Minanfilf1	OpenNMS user rtc has logged in tro	bp7410 skills 1st ep uk [1][]	10.0.07.[1][]	CNMD [] []	
	151303	Pinor [+][-]	uei opennms org/podes/dataColles	tionEailed [+][-] Edit notifications for event	10.0.0.37 [4][-]	SIMPE [#][-]	
			SNMP data collection on interface 1	0 0 0 97 failed			
	151278	Major [+][-]	09/07/08 08:59:37 [<] [>]	hp7410.skills-1st.co.uk [+][-]			
	1012/0		uei.opennms.org/nodes/nodeDown	[+][-]Edit notifications for event			
			Node hp7410.skills-1st.co.uk is dow	ND.			
Г	151197	Normal [+] [-]	09/07/08 08:48:27 [<] [>]	group-100-s2.class.example.org [+] [-]	172.31.100.21 [+] [-]	SNMP [+] [-]	
			uei.opennms.org/nodes/dataCollec	tionSucceeded [+] [-] Edit notifications for even	t		
			SNMP data collection on interface 1	72.31.100.21 previously failed and has been res	stored.		
Г	151180	Normal [+] [-]	09/07/08 08:46:17 [<] [>]	deodar.skills-1st.co.uk [+] [-]			
			uei.opennms.org/internal/capsd/re	scanCompleted [+] [-] Edit notifications for ever	ht		
			A services scan has been complete	d on this node.			
	151163	Normal [+] [-]	09/07/08 08:44:59 [<] [>]	switch.skills-1st.co.uk [+] [-]			
			uei.opennms.org/internal/capsd/re	scanCompleted [+] [-] Edit notifications for ever	nt		
			A services scan has been complete	d on this node.			
F	151162	Minor [+][-]	09/07/08 08:44:42 [-1[-]	aroun-100-s2 class example aro [+] [-]	172 31 100 21 [+] [-]	SNMP [+1[-]	

Figure 39: OpenNMS display of All events

The column headers can be clicked on to use as sort keys (ascending / descending). The "Ack" box can be ticked to Acknowledge one or more events – they will then disappear from this display which only shows "Outstanding" events. Click on the "-" symbol beside "Event(s) outstanding" to see "Event(s) Acknowledged", including the name of the user that acknowledged the event.

The various [+] and [-] links can be used to filter in/out on the parameter (such as node, interface, or service). The [<] and [>] beside the Time can be used to filter for events before or after this time.

To see the event detail, click on the ID link.

open	CopenNMS® Event Detail User: admin (Notices On) - Log out 09-Jul-2008 23:15 GMT-05:00						
	Node List Search Outages Pat	th Outages Dashboard	Events Alarms Notifications Asse	ts Reports Charts Surveillance Map Admin Help			
Home / Event	Home / Events / Detail						
Event 139192							
Severity	Normal	Node	group-100-r2.class.example.org	Acknowledged By admin			
Time	7/8/08 8:41:09 AM	Interface		Time Acknowledged 7/8/08 8:41:33 AM			
Service							
UEI	uei.opennms.org/internal/capsd/rescanCompleted						
Log Message							
A services scan l	has been completed on this node.						
Description							
A services scan has been completed. The list of services on this node has been updated.							
Operator Instructions							
No instructions a	vailable						
Unacknowledge							

Figure 40: OpenNMS Event detail for event 139192

7.3.2 Internally generated events

Events (and indeed alarms) are configured in /opt/opennms/etc/eventconf.xml, where the *first match* for an event defines its characteristics. For this reason, the ordering of stanzas in eventconf.xml is very important. Any individual event is identified by a Universal Event Identifier (uei).

Events are bracketed by <event> </event> tags. Within the event definition, the following tags can also be used:

•	• uei		a label to uniquely identify the event		
•	• event-label		a text label for the event – used in the Web GUI		
•	de	escr	description of the event		
•	log	gmsg	summary of the event where the <i>dest</i> parameter is one of		
	\circ logndisplay		log to events database and display in web GUI		
	\circ logonly		log to database but don't display in web GUI		
	\circ suppress		don't log to database or web GUI		
	0	donotpersist	don't log or display but do pass to other daemons (eg. for notification)		
	0	discardtraps	trapd to discard TRAPs – no processing whatsoever		
•	• severity				
•	ala	arm-data	create an alarm for this event with		
	• reduction-key		fields to compare to determine duplicate event		

- alarm-type 1=problem, 2=resolution. alarm-type=2 also takes a clear-key parameter defining the problem event this resolves
- \circ auto-clean true or false
- operinstruct optional instructions for operators using the web GUI
- mouseovertext text to display when mouse positioned over this event
- autoaction absolute pathname to executable program executed every event instance

Many of the tags can use data substituted from the event. These are documented on the OpenNMS wiki:

🥹 Event parameters - OpenNMS - Mozilla Firefox						
<u>F</u> ile <u>E</u> dit <u>V</u> iew High	<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp					
👍 🛪 🚵 🖉 🙆 🧑 http://www.oponpms.org/index.php/Event.parameters 🖸 🛪 🔊 🖓 Secolo						
🛛 🗋 Detail OpenN	. 🖸 📘 Nagios 🛛 🔄 🖸 S	SourceForge 🖾 🛛 🔞 Event param 🖾 📄 'Re: [oper	nms 🖸 💌			
(mombule ®	article discussion view source	Log in / crea	ate account			
(Obanumz	Event parameters					
Enterprise-grade						
Network Management	Event parameters are used in the event tokens delimitted with percent ('%') sig	t-configuration.xml and notifications.xml files. The parameters are parse ns. This is the currrent list of valid paramenters:	d as			
Ū	Someone should better define these ;-)					
get opennms	%eventid%					
Main Page	The Event ID xml tag					
Latest Release	%uei%					
Other Downloads	The UEI xml tag					
SourceForge Project	%source%					
get help	The event source xml tag					
 Official Documentation EAOs 	%time%					
White Papers	The event time					
Discussion Lists	%dpname%					
Commercial Support	%nodeid%					
get involved	The event nodeid					
Development Home	%nodelabel%					
Report a Bug	The nodelabel					
#opennms IRC	%host%					
Browse Source Code	The host					
 API docs 	%interface%					
XSD docs	The interface					
get to know us	%interfaceresolve%					
Order of the Green	Reverse DNS lookup of the interfac	çe				
Polo	%ifalias%	%community%				
OpenNMS Store	SNMP ifAlias	SNMP community string				
search	%id%	%snmphost%				
	SNMP ID	SNMP host				
Go Search	%snmp%	%service%				
	SNMP	OpenNMS service				
toolbox	%idtext% %severity%					
 What links here Related changes 	SNMP ID Text OpenNMS severity					
 Upload file 	Veload file %version% %operinstruct%					
 Special pages 	Special pages SNMP version Event defined operator instructions					
Printable version	Printable version %specific% %mouseovertext%					
Converse)	SININF Specific ID					
DEV-JAM 007	SPONSORS: DEV-JAM 007 SNMP generic ID Categories: Events and Notifications Configuration					
Google	//community //					

Figure 41: OpenNMS event parameters that can be substituted

Here is an example event from the default eventconf.xml:

Figure 42: OpenNMS event definition for nodeLostService

The different severities available can be seen by selecting the "Severity Legend" option from the top of an events list.

Но	me	
	Critical	This event means numerous devices on the network are affected by the event. Everyone who can should stop what they are doing and focus on fixing the problem.
	Major	A device is completely down or in danger of going down. Attention needs to be paid to this problem immediately.
	Minor	A part of a device (a service, and interface, a power supply, etc.) has stopped functioning. The device needs attention.
	Warning	An event has occurred that may require action. This severity can also be used to indicate a condition that should be noted (logged) but does not require direct action.
	Indeterminate	No Severity could be associated with this event.
	Normal	Informational message. No action required.
	Cleared	This event indicates that a prior error condition has been corrected and service is restored

Figure 43: OpenNMS event severity legend

Note that there is no separate file to configure alarms; it is simply done with the <alarm-type> tag in eventconf.xml.

OpenNMS comes with a huge number of events pre-defined. To make eventconf.xml much more manageable, inclusion files can be specified at the end, such as:

<event-file>events/NetSNMP.events.xml</event-file>

The events subdirectory currently has around 100 files in it! For performance reasons, it makes sense to edit eventconf.xml and remove any <event-file> stanzas that are not relevant for your organisation.

Also note that the whole OpenNMS system must be recycled in order for changes to eventconf.xml to take effect!

7.3.3 SNMP TRAP reception and configuration

OpenNMS will automatically monitor the SNMP TRAP part (UDP / 162) with the trapd process. The /opt/opennms/etc/events directory contains around 100 files which specify SNMP TRAP translations into OpenNMS events. If a TRAP is sent to OpenNMS that it has no configuration for, then it will use a default mapping found in default.events.xml.

🥹 List Events OpenNMS Web Console - Mozilla Firefox						
<u>Eile E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp						
💠 • 🧭 🛞 🏠 🗋 http://opennms:8980/opennms/event/list 🔹 🕨 💽 🕞 Google						
🗅 List Event	ts OpenN (Nagios	🔄 🗋 SourceForge.net: Part 🖸	Eventconf.xml - Ope	ənN 🖂 🗍 🗈 'color	css' in opennms 🖸
open NMS [®]					User: a 09	Event List Idmin (Notices On) - Log out -Jul-2008 23:54 GMT-05:00
		Node List Search Ou	itages Path Outages Dashboard Events Ala	irms Notifications Assets R	eports Charts Surve	illance Map Admin Help
View all events Event Text: Results: (1-10 of	Advanced Search	Severity Legend Acknowledge e	entire search			
Search constrain	ts: Event(s) outst	anding [-]				1 2 3 4 5 Next Last
					L	_egend
Ack ⊻ <u>ID</u>	<u>Severity</u>	Time	Node	<u>Interface</u>	<u>Service</u>	Ackd
158730	Normal [+] [-]	09/07/08 23:54:08 [<] [>]		127.0.0.2 [+] [-]		
		uei.opennms.org/generic/traps/EnterpriseDefault [+] [-] Edit notifications for event				
		Received unformatted enterprise e	event (enterprise: .1.3.6.1.4.1.123 generic:6 spec	fic:1234). 1 args: .1.3.6.1.4.1.1	23.1234="bad news 1"	
158729	Normal [+] [-]	09/07/08 23:53:03 [<] [>]				
			and a second sec	A second s		

Figure 44: OpenNMS Unknown trap appears in the Events list

Clicking on the event ID gives the detail of the event which shows all the information that arrived with the TRAP.

open	Event Detail User: admin (Notices On) - Log out 10-Jul-2008 00:06 GMT-05:00					
	Node List Search Outages Path Outages Dashboard Events Alarms	Notifications Assets	Reports Charts	Surveillance Map Admin Help		
Home / Event	; / Detail					
Event 158730						
Severity	Normal	Node		Acknowledged By		
Time	7/9/08 11:54:08 PM	Interface	127.0.0.2	Time Acknowledged		
Service						
UEI	uei.opennms.org/generic/traps/EnterpriseDefault					
Log Message						
Received unform	Received unformatted enterprise event (enterprise: 1.3.6.1.4.1.123 generic: 6 specific: 1234). 1 args: 1.3.6.1.4.1.123.1234="bad news 1"					
Description						
This is the default event format used when an enterprise specific event (trap) is received for which no format has been configured (i.e. no event definition exists). The total number of arguments received with the trap: 1. They were: 1.3.6.1.4.1.123.1234="bad news 1"						
Operator Instructions						
No instructions available						
Acknowledge						

Figure 45: OpenNMS Event detail for an unformatted TRAP

TRAPs are configured in eventconf.xml (or an include file), using the <mask> tag. This tag specifies mask elements with name / value pairs that must match data delivered by the TRAP, in order for this particular event configuration to match.

🦉 jane@opennms.skills-1st.co.uk: /opt/opennms/etc/events - Shell - Konsole	
Session Edit View Bookmarks Settings Help	
<pre></pre>	
<pre>(uei)uei.opennms.org/generic/traps/EnterpriseDefault<event-label>OpenNMS-defined trap event: EnterpriseDefault <descr></descr></event-label></pre>	nfigured
<pre>(lognsg dest='logndisplay'></pre>	

Figure 46: OpenNMS Definition in default.events.xml for an unknown specific trap

This example event will match any TRAP whose "generic" field is equal to 6. Note, as with other configurations in eventconf.xml, that this definition will only match the incoming TRAP if no previous definition higher in the file (or include files) had already matched it.

The mask element name tag must be one (or more) of the following:

- uei
- source
- host
- snmphost
- nodeid
- interface
- service
- id (OID)
- specific
- generic

It is possible to use the "%" symbol to indicate a wildcard in the mask values.

SNMP TRAPs often have additional data with them, known as "varbinds". This data can be accessed using the cparm> element, where:

Each parameter consists of a name and a value.

- %parm[all]%: Will return a space-separated list of all parameter values in the form parmName1="parmValue1" parmName2="parmValue2" etc.
- %parm[values-all]%: Will return a space-separated list of all parameter values associated with the event.
- %parm[names-all]%: Will return a space-separated list of all parameter names associated with the event.

- %parm[<name>]%: Will return the value of the parameter named <name> if it exists.
- %parm[##]%: Will return the total number of parameters.
- %parm[#<num>]%: Will return the value of parameter number <num>.

Any of this data can be used in the message or description fields.

In addition, the varbind data can also be used to filter the event within the <mask> tags, following the <maskelement> tags. It is possible to match more than one varbind, and more than one value per varbind. For example:

```
<varbind>
<vbnumber>3</vbnumber>
<vbvalue>2</vbvalue>
</varbind>
<varbind>
<vbnumber>4</vbnumber>
<vbvalue>2</vbvalue>
<vbvalue>3</vbvalue>
</varbind>
```

The above code snippet will match if the third parameter has a value of "2" or "3" *and* the fourth parameter has a value of "2" or "3". It is also possible to use regular expressions when matching varbind values.

Again, note that the order in which events are listed is very important. Put the most specific events first.

Here is an example definition that includes matching a varbind with a regular expression. Note the <vbvalue> matches any string that contains either Bad or bad .

Extra stanzas have also been added for <operinstruct> help (which provides a web link on one line and plain text on the second), a <mouseovertext> tag (which doesn't appear to work) and a tag to run an automatic action (a shellscript) whenever this event occurs.

```
jane@opennms.skills-1st.co.uk: /opt/opennms/etc - Shell - Konsole
Session Edit View Bookmarks Settings Help
(events)
 !--- Event conversion for Skills 1st TRAPs -->
<!-- Match any specific event from enterprise .1.3.6.1.4.1.123 where varbind 1 contains either Bad or bad -->
(event>
        <mask>
                  <maskelement>
                            <mename>id</mename>
                            <mevalue>.1.3.6.1.4.1.123</mevalue>
                  </maskelement>
                  <maskelement>
                            <mename>generic</mename>
                           <mevalue>6</mevalue>
                  </maskelement>
                  </mask>
         (uei)uei.opennms.org/uendor/skills/traps/trap123_bad</uei>
<event-label>Skills 1st defined trap event: trap123_bad</event-label>
         (descr)
                 &lt:p>Bad news from enterprise xidx, generic xgenericx, specific xspecificx with varbinds: args(xparm[##]x):xparm[all]x.<xp
         </descr>
                  .
<logmsg dest='logndisplay'>
<p&gt;Bad news from enterprise xidx, generic xgenericx, specific xspecificx with varbinds: args(xparm[##]x):xparm[all]x.&lt;/p
                  </logmsg>
         (severity)Ma jor(/severity)
(alarm-data reduction-key="/weix:xdpnamex:xnodeidx" alarm-type="1" auto-clean="false" />
          (operinstruct)
                    ält:pågt:check ålt:a href="http://www.skills-1st.co.uk"ågt;skills-1stålt:/aågt; for assistance ålt:/pågt;
ឱlt:pågt:When all else fails, RTFMIYCFI! ålt:/pågt;
          </operinstruct>
         <mouseovertext>
                    When all else fails, RTFM - if you can find it!
           /mouseovertext>
         <autoaction>
         /tmp/action.sh %uei% %id% %generic% %specific% 
{/autoaction>
 (/event)
```

Figure 47: OpenNMS Configuration of specific TRAP with varbind matching a regular expression

If you have SNMP TRAP definitions in a mib file, the open source utility *mib2opennms* can be obtained to convert SNMP V1 TRAPs and SNMP V2 NOTIFICATIONS into an OpenNMS event configuration xml file. For a source file vcs.mib in /home/jane, use:

mib2opennms -f /opt/opennms/etc/events/vcs.events.xml -m /home/jane vcs.mib

7.3.4 Alarms, notifications and automations

In OpenNMS you can add an <alarm-data> tag to an event configuration to create an alarm. Alarms are defined as "Important Events" and have a separate display. It is similar to the Events display in that you can select All Alarms or you can specify a search to filter for particular alarms.

0	Alarm Lis OpenNMS® User: admin (Notices On) - Log o 10-Jul-2008 07:53 GMT-05:0						
Home View a	Node List Search Outages Path Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Map Admin Help Home / Alarms / List View all alarms Advanced Search Severity Legend Acknowledge entire search						
Alarm Results Search	Alarm Text: Time: Any Search Results: (1-10 of 19) Source constrainty, alarm is subtanding [1]						
					Legend		
Ack	√ <u>ID</u> <u>Severity</u>	<u>Node</u> <u>Interface</u> <u>Service</u>	Count	<u>Last Event Time</u> <u>First Event Time</u>	Log Msg		
Г	1475 UEI [+] [-] Sev. [+] [-]	nagios3.skills-1st.co.uk [+] [-] 10.0.0.134 [+] [-]	3	10/07/08 07:53:25 [<] [>] 10/07/08 07:53:12 [<] [>]	Bad news from enterprise .1.3.6.1.4.1.123, generic 6, specific 1234 with varbinds: args(1):.1.3.6.1.4.1.123.1234="bad news 24".		
Г	1460 UEI [+] [-] Sev. [+] [-]		1	10/07/08 07:08:34 [<] [>] 10/07/08 07:08:34 [<] [>]	OpenNMS user '' (may be blank) has failed to login from 10.0.0.121. The failure event is BadCredentialsException with the message 'Bad credentials'.		
	1395 UEI [+] [-] Sev. [+] [-]	group-100-s2.class.example.org [+][-] 172.31.100.21[+][-] SNMP[+][-]	16	10/07/08 07:24:58 [<] [>] 09/07/08 19:49:28 [<] [>]	SNMP data collection on interface 172.31.100.21 failed.		
Γ	1394 UEI[+][-] Sev.[+][-]	wrt54g.skills-1st.co.uk [+] [-] 10.0.0.3 [+] [-] DNS [+] [-]	1	09/07/08 19:30:56 [<] [>] 09/07/08 19:30:56 [<] [>]	DNS outage identified on interface 10.0.0.3 with reason code: Unknown.		
	1389 UEI[+][-] Sev.[+][-]	group-100-a1.class.example.org [+][-]	1	09/07/08 17:07:04 [<] [>] 09/07/08 17:07:04 [<] [>]	Node group-100-a1.class.example.org is down.		
Γ	1387 UEI [+] [-] Sev. [+] [-]	group-100-a1.class.example.org [+][-] 172.31.100.3[+][-] SNMP[+][-]	16	10/07/08 07:25:00 [<] [>] 09/07/08 17:02:38 [<] [>]	SNMP data collection on interface 172.31.100.3 failed.		
	1384 UEI[+][-] Sev.[+][-]	blue-atlas.skills-1st.co.uk [+] [-]	1	09/07/08 16:02:39 [<] [>] 09/07/08 16:02:39 [<] [>]	Node blue-atlas.skills-1st.co.uk is down.		
	1383 UEI [+] [-]	blue-atlas.skills-1st.co.uk [+] [-] 10.0.0.2 [+] [-]	16	10/07/08 07:25:01 [<] [>]	SNMP data collection on interface 10.0.0.2 failed.		

Figure 48: OpenNMS Alarms display

Alarms are defined as part of an event definition in eventconf.xml and its include files. It uses the <alarm-data> tag where:

- reduction-key fields to compare to determine duplicate event
- alarm-type 1=problem, 2=resolution. alarm-type=2 also takes a clear-key parameter defining the problem event this resolves
- auto-clean true or false. True ensures that all *events* other than the latest one, that match the reduction-key, are removed (very useful for clearing out duplicate events)

One of the key characteristics of an alarm that differentiates it from an event, is the reduction-key field, which should ensure that duplicate events are treated as one event with multiple instances, rather than as multiple events.

Most of the information provided with an event is also available in the Alarm display. The new field is "Count" which shows the number of duplicate events that have been integrated into this alarm. To see the individual events, click on the number in the Count column. At present (July 10th, 2008), acknowledging events has no effect on related alarms, and vice versa. Note that the concepts of "Acknowledging" and "Clearing" are completely different. An operator can acknowledge an event or an alarm, and then owns it. This does not clear the event (ie. remove it entirely from the events database).

Automatic actions can be configured for an *event* using the <autoaction> tag but this can only run an executable and it runs on every occurrence of the event (which may not be what you want!).

OpenNMS's concept of *automation*, however, is triggered from alarms rather than events. Automation is the concept of actions being performed on a scheduled basis, provided the correct triggers exist. An <automation> tag includes:

- name the name of the automation
- interval the frequency in milliseconds at which the automation runs
- trigger-name a string that references a trigger definition
- action-name a string that references an action definition

The triggers and actions are SQL statements that operate on the events database.

Automation is defined in /opt/opennms/etc/vacuumd.xml where there are a number of useful rules, by default:

```
jane@opennms.skills-1st.co.uk: /opt/opennms/etc - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
  </statement>
  <automations>
    <automation name="cosmicClear" interval="30000" active="true"</pre>
                trigger-name="selectResolvers"
                action-name="clearProblems"
    <automation name="cleanUp" interval="30000" active="true"</pre>
                action-name="deletePastClearedAlarms" />
    <automation name="fullCleanUp" interval="300000" active="true"</pre>
                action-name="deleteAllPastClearedAlarms" />
   <automation name="fullGC" interval="300000" active="true"</pre>
                action-name="fullGarbageCollect" />
    <automation name="unclear" interval="30000" active="true"</pre>
                trigger-name="selectClearedAlarms"
                action-name="resetSeverity" />
   <automation name="escalation" interval="30000" active="true"
    trigger-name="selectSuspectAlarms"</pre>
                action-name="escalateAlarm"
                action-event="eventEscalated" />
    <automation name="purgeStatisticsReports" active="true"</pre>
                interval="3600000"
                action-name="deletePurgeableStatisticsReports" />
```

Figure 49: OpenNMS Default definitions for automations in vacuumd.xml

Note that automations always require an action-name but do not necessarily need a trigger-name.

The "cosmicClear" automation is the means by which an <alarm-data> alarm-type=2 tag in eventconf.xml, can clear bad news events when good news events arrive.

Here is the definition of the selectResolvers trigger name:

Figure 50: OpenNMS Definition of selectResolvers trigger in vacuumd.xml

... and the clearProblems action:
```
<action name="clearProblems" >
  <statement>
    UPDATE alarms
       WHERE alarmType=1
       AND severity > 2
      AND lastEventTime < ${lastEventTime}
AND eventUei = ${clearUei}
AND cOALESCE(dpName, '') = COALESCE(${dpName}, '')
AND COALESCE(nodeID, 0) = COALESCE(${nodeID}, 0)
AND COALESCE(ipaddr, '') = COALESCE(${ipaddr}, '')
       AND COALESCE(serviceID, 0) = COALESCE(${serviceID}, 0)
  (/statement)
</action>
<!-- New and optimized version of clearing problems -->
<action name="clearProblems" >
  <statement>
   UPDATE alarms
       SET severity=2, firstautomationtime = COALESCE(firstautomationtime, ${_ts}), lastautomationtime = ${_ts}
     WHERE alarmType=1
       AND severity > 2
       AND lastEventTime < ${lastEventTime}
       AND reductionKey = ${clearKey}
  </statement>
(/action>
```

Figure 51: OpenNMS Definition of clearProblems action in vacuumd.xml

The trigger is keyed on the field alarmType=2 . Note that the first version of the action is commented out – the "clear-uei" element is now deprecated in the <alarm-data> tag and only the "clear-key" element on the good news event is used to match against the "reduction-key" element of the bad news event, setting the severity to 2 (ie. Cleared). Also note from the <automation> tag that cosmicClear will run every 30 seconds.

If users need to be notified of an event then OpenNMS provides email and pager notifications out-of-the-box, run by the notifd daemon. It is also possible to create other notification methods such as SNMP TRAPs or an arbitrary external program. There are several related configuration files in /opt/opennms/etc :

•	destinationPaths.xml	who, when, how to notify / escalate
•	notifd-configuration.xml	global parameters for notifd
•	notificationCommands.xml	notification methods – email, http, page
•	notifications.xml	what events generate notifications, where
•	javamail-configuration.properties	configuration for java emailer (default)

The main files that will need attention are destinationPaths.xml, notifdconfiguration.xml and notifications.xml. Here is part of the examples file provided in /etc/opennms/etc/examples/destinationPaths.xml:

```
💻 jane@opennms.skills-1st.co.uk: /opt/opennms/etc/examples - Shell - Konsole
Session Edit View Bookmarks Settings Help
<?xml version="1.0"?>
<destinationPaths>
   <header>
       (reu)1.2(/reu)
       <created>Wednesday, February 6, 2002 10:10:00 AM EST</created>
       <mstation>localhost</mstation>
   </header>
   Kpath name="Email-Reporting">
       <target>
               <name>Reporting</name>
               <command> javaEma i l</command>
       </target>
   </path>
   <path name="Page-Management">
       <target>
               <name>Management</name>
               <command>textPage</command>
               <command> javaPagerEmail</command>
               <command> javaEma i l</command>
       </target>
   </path>
   <target interval="15m">
               <name>Network/Systems</name>
               <command>textPage</command>
               <command> javaPagerEmail</command>
               <command> javaEma i l</command>
       </target>
       <escalate delay="15m">
           <target>
               <name>Management</name>
               <command>textPage</command>
               <command>javaPagerEmail</command>
               <command> javaEma i l</command>
           </target>
       </escalate>
   </path>
```

Figure 52: OpenNMS Example entries in destinationPaths.xml

The <name> tag specifies a user or group of users defined in OpenNMS. The <command> tag specifies a method that must be defined in notificationCommands.xml. Note that escalations are possible.

When an event is received for which a notification is required, OpenNMS "walks" the destination path. We say that the destination path is "walked" because it is often a series of actions performed over time and not necessarily just a single action (although it can be). The destination path continues to be walked until all notifications and escalations have been sent or the notification is acknowledged (automatically or by manual intervention).

Out-of-the-box, the only destinationPath that is configured is for javaEmail to the Admin group of users.

The notifications.xml file species what events trigger notifications and to whom. Here is an example from the default file:

```
jane@opennms.skills-1st.co.uk: /opt/opennms/etc - Shell - Konsole <2>
 Session Edit View Bookmarks Settings Help
 {?xml version="1.0" encoding="UTF-8"?>
  <reu xmlns="">1.2</reu>
</reu xmlns="">1.2</reu>
</reu xmlns="">1.2</reu>
</reu xmlns="">1.2</reu>
</reu
</pre>

(reu xmlns="">2008 1:33:51 PM GMT<//reated>

(mstation xmlns="">>localhost</mstation>
       </ns1:header>
       <notification name="interfaceDown" status="on" writeable="yes">
            (uei xmlns="">uei.opennms.org/nodes/interfaceDown</uei>
(rule xmlns="">IPADDR != '0.0.0.0'</rule>
(destinationPath xmlns="">Email-Admin</destinationPath>
(text-message xmlns="">All services are down on interface xinterfaceresolvex (xinterfacex)
 on node %nodelabel%. New Outage records have been created
 and service level availability calculations will be impacted
 until this outage is resolved.
            </text-message>
<subject xmlns="">Notice #%noticeid%: %interfaceresolve% (%interface%) on node %nodelabel% down.</subject>
<numeric-message xmlns="">111-%noticeid%: %interfaceresolve% (%interface%) on node %nodelabel% down.</subject>
<numeric-message xmlns="">111-%noticeid%: %interfaceresolve% (%interface%) on node %nodelabel% down.</subject>
</numeric-message</pre>
       </notification>
       <notification name="nodeDown" status="on" writeable="yes">
            <uei xmlns=""
            <uei xmlns="">uei.opennms.org/nodes/nodeDown</uei>
<rule xmlns="">IPADDR != '0.0.0.0'</rule>
            <destinationPath xmlns="">Email-Admin</destinationPath>
            <text-message xmlns="">All services are down on node %nodelabel%. New Outage records have
 been created and service level availability calculations will
 be impacted until this outage is resolved.
            </text-message>
            <subject xmlns="">Notice #znoticeidz: node znodelabelz down.</subject>
            <numeric-message xmlns="">111-xnoticeidx</numeric-message>
       </notification>
Figure 53: OpenNMS Extract of notifications from notifications.xml
```

The notification called "interfaceDown" is turned on; it applies to all interfaces other than 0.0.0.0; the notification is sent to the destination "Email-Admin" (defined in destinationPaths.xml) and the text message of the email includes 3 parameters from the event – 4 parameters are included on the email subject. The default notifications.xml generates email to the Admin group for the following events:

- interface Down
- nodeDown
- nodeLostService
- nodeAdded
- interfaceDeleted
- High Threshold
- Low Threshold
- High Threshold Rearmed
- Low Threshold Rearmed

Nothing, so far, has handled acknowledging notifications. This can either be done manually by a user or can be performed automatically. Either way, when a notification is acknowledged, it stops the destination path being walked for the original notification. It will also create a new notification to tell users that the original issue is resolved. Automatic acknowledgements are configured in /opt/opennms/etc/notifd-configuration.xml where <auto-acknowledge> tags specify the uei resolution / problem events, along with the parameters on the event which must also match for the notification to be automatically acknowledged.



Figure 54: OpenNMS notifd-configuration.xml with auto-acknowledgements for notifications

Note that at present (July 2008) notifications are driven by events not alarms. Also note that acknowledging notices has no effect on their associated events or alarms.

It would appear that there has been a discussion of a change in architecture around events, alarms and notifications, at least throughout 2008. In the future, it is suggested that alarms will be where most automation is driven from, including notifications, and that events will become more of a background log.

7.4 Performance management

7.4.1 Defining data collections

There are several parallels between the capability discovery subsystem and the performance data collection subsystem. Each uses the snmp-config.xml file, described in section 7.1.2, to get SNMP parameters for each device - such as SNMP version, port number, community names.

The capability discovery process, capsd, uses the protocol definitions in capsdconfiguration.xml to determine what services (capabilities) to discover – these are things like SNMP, DNS, ICMP, SSH. The performance data collection process, collectd, uses 2 files to define what data to collect:

- datacollection-config.xml specifies collection names (just the snmp-collection called *default* out-of-the-box), which defines (typically MIB) values to collect
- collectd-configuration.xml specifies packages for collection. A package combines filters and ranges to determine which interfaces collections should be applied to, with services which reference collections in datacollection-config.xml. collectd-configuration.xml can also specify data collection intervals and whether the collection is active.

Note that if a device has several interfaces that:

- Support SNMP
- Have a valid ifIndex
- Is included in a collection package in collectd-configuration.xml

then the lowest IP address is marked as primary and will be used by default for all performance data collection.

collectd is triggered when capsd generates a NodeGainedService event. The discovered protocol name (eg. SNMP, SSH) is passed from capsd to collectd, along with the primary interface from the event. These are checked against the configuration in collectd-configuration.xml to see whether any collection packages are valid (there should be at least one, by definition!) and data collection is started.

```
Session Edit View Bookmarks Settings Help
K?xml version="1.0"?>
                                                                                           *
<?castor class-name="org.opennms.netmgt.collectd.CollectdConfiguration"?>
<collectd-configuration
       threads="50">
        charge name="example1">
                <filter>IPADDR != '0.0.0.0'</filter>
                <include-range begin="1.1.1.1" end="254.254.254.254"/>
                <service name="SNMP" interval="300000" user-defined="false" status="on">
                        <parameter key="collection" value="default"/>
                </service>
        </package>
                                          class-name="org.opennms.netmgt.collectd.SnmpColl
        <collector service="SNMP"
ector"/>
</collectd-configuration>
```

Figure 55: OpenNMS collectd-configuration.xml as shipped

There is only one package specified in collectd-configuration.xml, as shipped, which applies to all interfaces other than 0.0.0.0 and in the range 1.1.1.1 through 254.254.254.254. As with poller-configuration.xml, you must have one filter

statement per package and can then use multiple <specific> , <include-range> and <exclude range> statements to define which interfaces this package applies to. You can also use the <include url> tag to specify a file with a list of interfaces.

There is only one data collection service defined for OpenNMS out-of-the-box, in collectd-configuration.xml – the SNMP service. It will run every 5 minutes (300,000 ms) and will collect the MIB variables specified in the collection called *default*, specified in datacollection-config.xml. The <service> stanza can also specify values for SNMP timeouts, retries and port number which would override the default values in snmp-config.xml.

The package definition can also use the <outage-calendar> tag to specify scheduled downtime for devices, during which data collection will be suspended. This should be used to prevent lots of failed SNMP collection events. Outage periods are defined in the poll-outages.xml file.

Obviously you can specify different packages with different address ranges, collection intervals and with different collection keys. You can also specify data collectors other than SNMP, such as NSClient, JMX and HTTP. See <u>http://blogs.opennms.org/?p=242</u> for a note on using an HTTP data collector.

The datacollection-config.xml file defines one or more SNMP data collections that Tarus Balog (the prime developer behind OpenNMS) calls a "scheme", to differentiate it from the "package" defined in the collectd configuration file. These schemes bring together OIDs for collection, into *groups* and the groups are mapped to *systems*. The systems are mapped to interfaces by a device's systemOID. In addition, each "scheme" controls how the data will be collected and stored.

Fundamentally, OpenNMS uses RRD Tool (Round Robin Database Tool) to store performance data. This paper is not a tutorial on RRD Tool so please follow the reference to RRD at the end of this paper for more information.

The basis of RRD is that a fixed amount of space is allocated for a given database when it is created. It holds data for a given period of time, say 1 month, 1 year, etc. The sampling interval is known so you know how many datapoints will go into the database and hence how much space is required. Once the database is full, newer datapoints will replace the oldest ones, cycling around.

Figure 56: OpenNMS datacollection-config.xml collection and RRD parameters

The <rrd> stanza specifies how data will be stored in a Round Robin Archive (RRA). The snapshot shown in the figure above specifies:

- <rrd step="300">
 - $\circ~$ data to be saved every 5 minutes, per step
- RRA:AVERAGE:0.5:1:2016
 - create an RRA with values AVERAGE'd over 1 step (ie. this data is "raw", not consolidated). The RRA will have 2016 rows representing 7 days of data (5 minute steps = 12 / hour * 24 hours * 7 days = 2016). Consolidate the samples provided 0.5 (half) of them are not UNKNOWN (otherwise the consolidated value will be UNKNOWN)
- RRA:AVERAGE:0.5:12:1488
 - create an RRA with values AVERAGE'd over 12 steps (ie. this data is consolidated over 1 hour). The RRA will have 1488 rows representing 2 months of data (1 hour consolidations * 24 hours * 62 days = 1488). Consolidate the samples provided 0.5 (half) of them are not UNKNOWN (otherwise the consolidated value will be UNKNOWN)
- RRA:AVERAGE:0.5:288:366
 - create an RRA with values AVERAGE'd over 288 steps (ie. this data is consolidated over 288 * 5 min steps = 1 day). The RRA will have 366 rows representing 1 year of data (1 day consolidations * 366 days = 366). Consolidate the samples provided 0.5 (half) of them are not UNKNOWN (otherwise the consolidated value will be UNKNOWN)
- RRA:MAX:0.5:288:366
 - $\circ~$ create an RRA with MAX values averaged daily and keep 1 year of data
- RRA:MIN:0.5:288:366
 - $\circ~$ create an RRA with MIN values averaged daily and keep 1 year of data

The top of datacollection-config.xml defines where the RRD repositories are kept and how many variables can be retrieved by an SNMP V2 GET-BULK command (10 is the default). Within the repository directory, for each node, there will exist a directory that consists of the node number. Thus, if the system was collecting data on node 21, there would be a directory called /opt/opennms/share/rrd/snmp/21 containing a datafile for each MIB OID being collected. File names will match the *alias* parameter for a MIB OID, in datacollection-config.xml.

The node number can be found by going to the detailed node information for a device and choosing the *Asset Info* link:

🎯 bino.skills-1st.co.uk N	🧃 bino.skills-1st.co.uk Node OpenNMS Web Console - Mozilla Firefox										
<u>File Edit View History B</u>	ookmarks <u>T</u> oo	ols <u>H</u> elp									
🦛 • 🔿 • 🥑 🔕 🏠 🖸) http://opennr	ms:8980/opennm	s/element/no	ode.jsp	?node=4		•	G Google			
Nagios	🗋 bino.skills	s-1st.co 🚨 🛛] Nagios Ad	Idons	s	Source	Forge.net:	. 🖂 🗋 🕒 'snm	pstorageflag s 🞑		
open NMS [®]	,							User: admi 05-Aug-:	Node n (Notices On) - Log out 2008 04:27 GMT-05:00		
Node List Search Outages Path Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Map Admin Help											
Node: bino.skills-1st View Events View Alarms Asse	t Info	urce Graphs Rescan	Admin								
General (Status: Active) Notification View Node Link Detailed Info You: Outstanding: (Check)											
Ausilability			You: Ackno	wledge	ed: (Check)						
Availability (last 24 hours)	81.250%		Recent Eve	nts							
Producer (rase 24 riodres)	Overall	80.000%	1 94387	04/08	/08 01:03:45	Normal	A services sca	an has been com	pleted on this node.		
	DNS	100.000%	□ 187237	30/07	/08 23:10:13	Normal	A services sca	an has been com	pleted on this node.		
	FTP	0.000%	□ 180154	30/07	/08 09:03:46	Normal	A services scan has been completed on this node.				
	ICMP	100.000%	□ 180152	30/07	/08 09:02:50	Warning	A services sca	an has been force	ed on this node.		
10.0.0.121	Router	Not Monitored	□ 175101	29/07	/08 23:07:42	Normal	A services sca	an has been com	pleted on this node.		
	SNMP	100.000%	Acknowled	qe F	leset	More					
	SSH	100.000%									
	StrafePing	Not Monitored	Recent Out	ages							
	Overall	100.000%	Interface		Service	Lost		Regained	Outage ID		
	DNS	Not Monitored	10.0.0.121		FTP	08/07/08 0	8:37:43	DOWN	317		
	FTP	Not Monitored	172.16.222.1		FTP	08/07/08 0	8:37:41	DOWN	315		
10 191 0 1	ICMP	100.000%	172.16.223.1		FTP	08/07/08 0	8:37:28	DOWN	314		
1011911011	Router	Not Monitored									
	SNMP	Not Monitored									
	COLL	No. Manufacture of									

Figure 57: OpenNMS Asset Info link for a device

The resulting page includes the Node ID at the top.

<u>E</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory	<u>B</u> ookmarks <u>T</u> ools	<u>H</u> elp					
🌾 - 🔶 - 🥑 🙆 🏠	http://opennms:	8980/opennms/asset/mo	dify.jsp?node=4		G Google	Q	
Nagios	Modify Ass	et O 🐼 🗋 Nagios A th Outages Dashboard Ever	ddons 💽 🖬 So its Alarms Notifications	ourceForge.ne	t: 🕢 🗋 🕒 'snmp User: admir 05-Aug-2 Charts Surveillance	Ostorageflag s Modify Asset (Notices On) - Log out 008 04:31 GMT-05:00 e Map Admin Help	
Home / Assets / Modified bino.skills-1st.co.uk General Information	ode ID 4)						
System Id	.1.3.6.1.4.1.8072.3.2.10				System Name	bino	
System Location	Cedar Chase				System Contact	Jane Curry	
Configuration Categories							
Display Category		Notification Category					
Poller Category		Threshold Category					
Identification							
Description				Cate	gory Unspecified	I	
Manufacturer		Model Number		Seria Numl	ber		
Asset Number		Date Installed		Oper Syste	ystem		
Location							
Region		Division		Depa	artment		
Address 1							
Address 2							
City		State		ZIP			
Building		Floor		Roon	n		
Rack		Slot		Port			
Circuit ID							
Vendor							

Figure 58: OpenNMS Asset information page, including Node ID

The snmpStorageFlag parameter in the snmp-collection stanza of datacollectionconfig.xml defines for which interfaces of a device, data will be stored. Possible values are:

- all (the old default)
- primary the primary SNMP interface
- select collect from all IP interfaces *and* can use Admin GUI to select additional non-IP interfaces to collect data from (new default since OpenNMS 1.1.0)

<u>F</u> ile <u>E</u> dit <u>\</u>	/iew Hi <u>s</u> tory	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp							0			
🧼 • 🧼 •	╞ • 🗼 - 🥃 🐼 🏠 🗋 http://opennms:8980/opennms/admin/snmpGetInterfaces?node=22&nodek 🔹 🕨 💽 - Google 🔍											
Nagios	C	📔 🕒 Select SNMP Inte 🞑	B Nagios	s Addons	🗵 📴 Sou	rceForge.net	🗵	🕒 'snmpstoragef	lag s 🖸 🔽			
оре	Select SNMP Interfaces User: admin (Notices On) - Log out 05-Aug-2008 02:08 GMT-05:00											
	Node L	st Search Outages PathOutages	Dashboard	Events Alarms	Notifications	Assets Report	s Charts	s Surveillance Map	Admin Help			
Home / A	dmin / Select S	NMP Interfaces										
Choose SN	MP Interfaces fo	or Data Collection										
Listed below	are all the interfac	es discovered for the selected node. If s	snmpStorag	eFlag is set to "sel	ect" for a collec	tion scheme that	includes t	the interface marked a	s "Primary",			
only the inte	rfaces checked bel	ow will have their collected SNMP data s	tored. This I	has no effect if snr	npStorageFlag	is set to "primary	" or "all".					
In order to c	hange what interfa	ces are scheduled for collection, simple	check or un	icheck the box bes	ide the interfac	e(s) you wish to	change, a	nd then select "Update	Collection",			
Note: Intern	aces marked as Pr	imary or Secondary will always be selec	ted for data	collection, to rem	ove them, eait	the IP address ra	inge in th	e collecto configuration	me.			
Node La	r: 22 bel : aroun-1 (00-linux class example ord										
Nouc La	BCI. group IV	of midx.class.example.org										
ifIndex	IP Address	IP Hostname	ifType	ifDescription	ifNar	ne	ifAlias	SNMP Status	Collect?			
	10.191.100.3	group-100-linux.class.example.org	0	null	nul	1	null	Primary	~			
3	0.0.0	null	131	sit0	nul			Not Collected				
Undate Co	lection Cancel		+									

Figure 59: OpenNMS GUI Admin page for specifying interfaces to collect data from

Most of the contents of datacollection-config.xml is defining groups and systems:

- groups define groups of SNMP MIB OIDs to collect
- systems use a device's System OID as a mask to determine which groups of OIDs should be collected

```
(groups)
                                                                                                                                                                                                                                                                                                                                                                                       type="counter"
                        (/group)
                             group name="mib2-icmp" ifType="ignore">
(mib0bj oid=".1.3.6.1.2.1.5.2" instance="0"
(mib0bj oid=".1.3.6.1.2.1.5.3" instance="0"
(mib0bj oid=".1.3.6.1.2.1.5.4" instance="0"
alias="icmpInImeExtCosts" type="counter" />
alias="icmpInImeExtCosts" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.4" instance="0"
alias="icmpInImeExtCosts" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.6" instance="0"
alias="icmpInImeExtCosts" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.6" instance="0"
alias="icmpInImeCosts" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.6" instance="0"
alias="icmpInEchos" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.16" instance="0"
alias="icmpOutErors" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.16" instance="0"
alias="icmpOutErors" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.17" instance="0"
alias="icmpOutErors" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.17" instance="0"
alias="icmpOutErors" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.21" instance="0"
alias="icmpOutEchos" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.21" instance="0"
alias="icmpOutEchos" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.21" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.5" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.9" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.9" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.9" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.11" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.11" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.11" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.12" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.13" instance="0"
alias="icmpInEchoReps" type="counter" />
(mib0bj oid=".1.3.6.1.2.1.5.14" instance="0"
alias="icmpInEchoReps" type="coun
                        </group>
                        </group)
"datacollection-config.xml" line 178 of 1966 --9%-- col 5
```

Figure 60: OpenNMS group definitions in datacollection-config.xml

Unfortunately OpenNMS does not have a MIB compiler so all MIB OIDs need to be manually specified in this file (the good news is that there are lots there out-of-thebox). Once groups of MIB variables are declared, system stanzas say which group(s) are to be collected for any device whose system OID matches a particular pattern.

Each SNMP MIB variable consists of an OID plus an instance. Usually, that instance is either zero (0) or an index to a table. At the moment, OpenNMS only understands a small number of table indices (for example, the ifIndex index to the ifTable and the hrStorageIndex to the hrStorageTable). All other instances have to be explicitly configured.

The ifType parameter can be used to specify the sort of interfaces to collect from. Legal values are:

• all collect from all interface types

 ignore used when the value would be the same for all interfaces eg. CPU utilisation for a Cisco router
 <i/f type number> used to denote one or more specific interface types. For example ifType=6 for ethernetCsmacd. See

h<u>ttp://www.iana.org/assignments/ianaiftype-mib</u> for a comprehensive list.

OpenNMS understands four types of variables to collect on - gauge, timeticks, integer, octetstring. Note that RRD only understands numeric data.

```
<systems>
  <systemDef name="Enterprise">
    <sysoidMask>.1.3.6.1.4.1.</sysoidMask>
    (collect)
      <includeGroup>mib2-interfaces</includeGroup>
      <includeGroup>mib2-tcp</includeGroup>
      <includeGroup>mib2-icmp</includeGroup>
    </collect>
  </systemDef>
  <systemDef name="Alvarion BreezeAccess base">
    <sysoidMask>.1.3.6.1.4.1.12394.4.1</sysoidMask>
    <collect>
      <includeGroup>alvarion-bad-all-frames</includeGroup>
      <includeGroup>alvarion-interfacesRB<//includeGroup>
    </collect>
  </systemDef>
  <systemDef name="Alvarion BreezeAccess SU">
    <sysoidMask>.1.3.6.1.4.1.12394.4.1.2</sysoidMask>
    <collect>
      <includeGroup>alvarion-snr-lqi</includeGroup>
    </collect>
  </systemDef>
```

Figure 61: OpenNMS systems definitions in datacollection-config.xml

In the figure above, any device which has satisfied the filtering in collectdconfiguration.xml **and** has a system OID starting with .1.3.6.1.4.1 (the start of the Enterprise MIB tree), will collect performance data for MIB-2 interfaces, tcp and icmp, as specified in the earlier <group> stanzas.

Note that the defaults in collectd-configuration.xml and datacollection-config.xml mean that a large number of SNMP data collections will be activated out-of-the-box. This is good in providing lots of samples in small environments but it could be a serious performance and disk usage factor if these defaults are left unchanged, where a large number of interfaces are monitored by OpenNMS.

7.4.2 Displaying performance data

OpenNMS provides a large number of reports out-of-the-box, based on the default data collection parameters. Use the Reports main menu to see the options.



Figure 62: OpenNMS Copyright © 2002-2008 The OpenNMS Group Inc. OpenNMS® is a registered trademark of The OpenNMS Group Inc Figure 62: OpenNMS Report categories available out-of-the-box

- Resource Graphs provide lots of standard reports
- KSC Performance, Nodes, Domains allows users to customise own reports
- Availability availability reports for interfaces & services
- Statistics Reports shows Top-20 ifInOctets across all nodes

Following the *Resource Graphs* link provides access to many standard reports.



Figure 63: OpenNMS Standard performance reports

The standard performance reports display various collected values for one particular node which you choose from the menu provided. The different categories provide:

- Node-level performance data such as TCP connections, CPU, memory
- Interface data for each interface such as bits in/out
- Response time data for services such as ICMP, DNS, SSH
- Disk space information from the ucd-snmp MIB



 $\label{eq:Figure 64: OpenNMS Standard Resource graphs available for a selected node$

Here is part of the node-level performance data set of graphs.



Figure 65: OpenNMS partial display of the node-level performance data graphs

If you wish to create more selective sets of graphs for other people to use, the Key SNMP Customized (KSC) Reports menu to create your own reports which can include graphs of selected MIB variables from one device or can select MIB variables from different devices. Using the "Create New" button will prompt for nodes that have data collections configured as "Child Resources".



Figure 66: OpenNMS KSC Reports menu

Selecting a node and clicking "View child resources" results in a menu of report categories.

Choose Reso	ource KSC Reports OpenNMS Web (Console - Mozilla Firefox
ile <u>E</u> dit <u>V</u> iew	Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	
 	🐼 🏠 🗋 http://opennms:8980/opennr	ns/KSC/customGraphChooseResource.htm?s: 🔹 🕨 💽 Google
Nagios	🛛 🗋 Choose Resourc 🗳	🗋 Nagios Addons 🛛 🔄 📴 SourceForge.net: 🕞 🔞 FAQ-Configuration
open	NMS®	Key SNMP Customized Performance Repo User: admin (Notices On) - Log 05-Aug-2008 09:57 GMT-09
Home / Reports	Node List Search Outages Path Outages	Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Map Admin H
Node: bino.skill	s-1st.co.uk ent resource	Descriptions
This resource has resource or the pa	no available prefabricated graphs. Select a child arent resource (if any).	The menu on the left lets you choose a specific resource that you want to use in a graph. A resource can be any graphable resource such as SNMP data (node-level, interface-level or generic indexed data), response time data, or distributed response time data.
View child resou SNMP Interface D SNMP interfa	Inces Inces	These resources are organized first by top-level resources, such as nodes or domains (if enabled), and then by child resources under the top-level resources, like SNMP node-level data, response time data, etc The resource you are currently looking at (if any) is shown just below the menu-bar on the left side of the page. If the resource has any available prefabricated graphs, they will be listed in the Choose the current resource box along with a "Choose this resource" button which will take you to the graph customization page. If the current resource has child resources (or if you are at the top-level) a list of available child resources will be shown in the View child resources box. You can select a child resource and click the "View child resource" button to view the details of the selected child resource, including any available graphs and any sub-children. If you know the resource you are selecting has graphs, you can go straight to the graph customization page by clicking "Choose of the current resource (or see all top-level resource). For example, if you are looking at an SNMP interface resource, its parent resource would be the node which owns that SNMP interface. If you are looking at a node, you would have the option to see all top-level resources.
resources" button View top-level re	to see all top-level resources. esources	

Figure 67: OpenNMS Report categories available for customised reports

If you select the Node-level Performance Data option and the "Choose child resource" button then each of the MIB variables collected can be displayed and selected.

<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> t	ory <u>B</u> ookmarks <u>T</u> oo	ls <u>H</u> elp						4
- 🔶 - 🕑 📀	🏠 🗋 http://opennm	ns:8980/opennms/KSC/c	ustomGraphEc	litDetails.htm	n?resource 🔻 🖡	G Google		Q
Nagios	🖾 🗋 Performar	nce Re 📴 🗋 Nagios	s Addons	🕒 📴 Sou	rceForge.net:	🔄 🔞 FAQ-C	onfiguration	
open NN	∕IS®				Key SNM	P Customized Pe User: admin 05-Aug-2	rformance Rep n (Notices On) - Lo 2008 10:03 GMT-0	orts g out 05:00
Ч	Iode List Search Outage	s Path Outages Dashboard	Events Alarms	Notifications	Assets Reports	Charts Surveilland	e Map Admin	Help
Home / Reports / K Customized Report Sample graph	SC Reports / Custom Graph Definition	Graph						l
N SNMP Node Data: Nod From Tue Jul 29 1 To Tue Aug 05 :	lode: bino.skills-1st.co.uk e-level Performance Data 0:03:10 GMT-05:00 2008 10:03:10 GMT-05:00 2008	by 1.0 v v v v v v v v v v v v v	TCP Open Connect Thu Fri 17.11 m Hin 30.44 m Hin	tions Sat Su 694.32 m Max 694.28 m Max	n Mon : 850.36 m : 1.12	OpenNING / Dirachin		
Choose graph option Title Timespan Prefabricated Report Graph Index Cancel edits to this gr	s 7_day ▼ (This seld netsnmp.cpuUsage 1 ▼ (This selects the des aph <u>Refresh sample vi</u>	ects the relative start and stop	times for the repor ricated graph repo he graph to be inse rce Done with a	t) rt to use) erted) edits to this gra	ph_			

Figure 68: OpenNMS Selecting prefabricated reports to include in a customised report

The dropdown alongside the "Prefabricated Report" field allows you to select any of the default reports to include in your own customised reports. You can include several different graphs, from the same or different nodes, in your KSC report.

7.4.3 Thresholding

The thresholding capability in OpenNMS has changed fairly significantly over time – see <u>http://www.opennms.org/index.php/Thresholding#Merge_into_collectd</u>. for a good explanation.

Pre OpenNMS 1.3.10, collectd collected data and threshd performed thresholding – two separate processes. This design used a "range" parameter in threshdconfiguration.xml to get around problems caused by the asynchronous manner nature of collectd and threshd.

OpenNMS 1.3.10 merged the thresholding functionality into collectd and introduced a new parameter into collectd-configuration.xml:

• <parameter key="thresholding-group" value="default-snmp"/>

where the value of the thresholding group matched a definition in threshdconfiguration.xml. The need for the "range" parameter disappeared. However, to define different filters for thresholding, different packages had to be defined in collectd-configuration.xml. From OpenNMS 1.5.91, (this paper is based on version 1.5.93), filters can be defined in threshd-configuration.xml so that packages in collectd-configuration.xml can be kept simple. The parameter in threshd-configuration.xml changes; the thresholdinggroup key disappears and is replaced by:

• <parameter key="thresholding-enabled" value="true"/>

Here is the default collectd-configuration.xml:

```
Session Edit View Bookmarks Settings Help
K?xml version="1.0"?>
<?castor class-name="org.opennms.netmgt.collectd.CollectdConfiguration"?>
<collectd-configuration
        threads="50">
        <package name="example1">
                <filter>IPADDR != '0.0.0.0'</filter>
                <include-range begin="1.1.1.1" end="254.254.254.254"/>
                <service name="SNMP" interval="300000" user-defined="false" status="on">
                        <parameter key="collection" value="default"/>
                </service>
        </package>
        <collector service="SNMP"
                                         class-name="org.opennms.netmgt.collectd.SnmpColl
ector"/>
</collectd-configuration>
```

Figure 69: OpenNMS Default collectd-configuration.xml

The lack of any thresholding parameter implies that thresholding is disabled.

... and the default threshd-configuration.xml:

```
Session Edit View Bookmarks Settings Help
K?xml version="1.0"?>
<?castor class-name="org.opennms.netmgt.threshd.ThreshdConfiguration"?>
<threshd-configuration
        threads="5">
        <package name="example1">
                <filter>IPADDR != '0.0.0.0'</filter>
                <include-range begin="192.168.0.1" end="192.168.0.254"/>
                <service name="SNMP" interval="300000" user-defined="false" status="on">
                        <parameter key="thresholding-group" value="default-snmp"/>
                        <parameter key="range" value="600000"/>
                </service>
        </package>
       <thresholder service="SNMP"
                                       class-name="org.opennms.netmgt.threshd.SnmpThresholder"/>
</threshd-configuration>
```

Figure 70: OpenNMS Default threshd-configuration.xml

The default threshd-configuration.xml is setup for the interim design between versions 1.3.10 and 1.5.90. For OpenNMS 1.5.93, collectd-configuration.xml should be changed as shown below:

```
Session Edit View Bookmarks Settings Help

{?xml version="1.0"?>

<?castor class-name="org.opennms.netmgt.collectd.CollectdConfiguration"?>
<collectd-configuration
        threads="50">
        <package name="example1">
                <filter>IPADDR != '0.0.0.0'</filter>
                <include-range begin="1.1.1.1" end="254.254.254.254"/>
                <service name="SNMP" interval="300000" user-defined="false" status="on">
                        <parameter key="collection" value="default"/</pre>
                        <parameter key="thresholding-enabled" value="true"/>
                (/service)
        </package>
        <collector service="SNMP"
                                          class-name="org.opennms.netmgt.collectd.SnmpCollector"/>
</collectd-configuration>
```

Figure 71: OpenNMS Modified collectd-configuration.xml to enable thresholds

threshd-configuration.xml can be modified with different packages of thresholding to apply to different ranges of nodes.

```
Session Edit View Bookmarks Settings Help

{?xml version="1.0"?>

<?castor class-name="org.opennms.netmgt.threshd.ThreshdConfiguration"?>
<threshd-configuration
        threads="5">
        <package name="CC">
                 <filter>IPADDR != '0.0.0.0'</filter>
                 <include-range begin="10.0.0.0" end="10.0.0.254"/>
<include-range begin="172.16.0.0" end="172.16.254.254"/>
                 </service>
        </package>
        <package name="raddle">
                 <filter>IPADDR != '0.0.0.0'</filter>
<include-range begin="10.191.0.0" end="10.191.101.254"/>
<include-range begin="172.30.0.0" end="172.31.254.254"/>
                 <exclude-range begin="172.31.100.3" end="172.31.100.3"/>
                 <service name="SNMP" interval="600000" user-defined="false" status="on">
                          <parameter key="thresholding-group" value="raddle-snmp"/>
                 </service>
        </package>
        <thresholder service="SNMP"
                                            class-name="org.opennms.netmgt.threshd.SnmpThresholder"/>
</threshd-configuration>
```

Figure 72: OpenNMS Modified threshd-configuration.xml

Different filters are applied to each package. The "thresholding-group" parameter is required here and the value points to a matching definition in thresholds.xml, where the MIBs to threshold and the threshold values, are specified.



Figure 73: OpenNMS Modified thresholds.xml for CC-snmp group and raddle-snmp group

The attributes of a threshold are:

- **type:** A "high" threshold triggers when the value of the data source exceeds the "value", and is re-armed when it drops below the "re-arm" value. Conversely, a "low" threshold triggers when the value of the data source drops below the "value", and is re-armed when it exceeds the "re-arm" value. "relativeChange" is for thresholds that trigger when the change in data source value from one collection to the next is greater than "value" percent.
- **expression:** A mathematical expression involving datasource names which will be evaluated and compared to the threshold values. This is used in "expression" thresholding (supported from 1.3.3).
- **ds-name:** The name of the variable to be monitored. This matches the name in the "alias" parameter of the MIB statement in datacollection-config.xml .
- **ds-type:** Data source type. "node" for node-level data items, and "if' for interface-level items.
- **ds-label:** Data source label. The name of the collected "string" type data item to use as a label when reporting this threshold. *Note: this is a data item whose value is used as the label, not the label itself.*
- **value:** The value that must be exceeded (either above or below, depending on whether this is a high or low threshold) in order to trigger. In the case of relativeChange thresholds, this is the percent that things need to change in order to trigger (e.g. 'value="1.5" means a 50% increase).
- **rearm:** The value at which the threshold will reset itself. Not used for relativeChange thresholds.

- **trigger:** The number of times the threshold must be "exceeded" in a row before the threshold will be triggered. Not used for relativeChange thresholds.
- **triggeredUEI:** A custom UEI to send into the events system when this threshold is triggered. If left blank, it defaults to the standard thresholds UEIs.
- **rearmedUEI:** A custom UEI to send into the events system when this threshold is re-armed. If left blank, it defaults to the standard thresholds UEIs.

By default, standard threshold and rearm events will be generated but it is also possible to create customised events with the threshold attributes. This would then make it easier to generate notifications for specific thresholding / rearm events.

Here is a screenshot with standard events generated by thresholds on the raddle network:

w	all events	Advanced Se	arch Severity Legend Acknov	wledge entire search							
ent	Text:		Time: Any	▼ Search							
sul	ts: (1-10 of	f 2980)					and a support of				
arc	h constrair	nts: Event(s) o	outstanding [-]			1 2	3 4 5 Next Las				
						Leger	nd and a second se				
k	∨ <u>ID</u>	<u>Severity</u>	Time	Node	Interface	Service	Ackd				
1	217583	Normal	05/08/08 23:59:20 [<] [>]								
		[+][-]	uei.opennms.org/internal/aut	hentication/successfulLogin [+] [-] Edit n	otifications for event						
			OpenNMS user admin has log	ged in from 10.0.0.121.							
1	217582	Normal [+][-]	05/08/08 23:58:30 [<] [>]								
			uei.opennms.org/internal/authentication/successfulLogin [+] [-] Edit notifications for event								
			OpenNMS user rtc has logged	l in from 127.0.0.1.							
	217566	Warning [+][-]	05/08/08 23:54:54 [<] [>]	server.class.example.org [+] [-]	10.191.101.1 [+] [-]	SNMP [+] [-]					
			uei.opennms.org/threshold/re	elativeChangeExceeded [+] [-] Edit notifi	cations for event						
			Relative change exceeded for previousValue="38540.0" mu	- SNMP datasource ifInOctets on interface Itiplier="1.05" label="Unknown" ifLabel=	e 10.191.101.1, parms: ds= "eth0-000c29aea14f" ifInde	="ifInOctets" value="82 ex="2"	948.0"				
2	217565	Warning [+][-]	05/08/08 23:54:54 [<] [>]	server.class.example.org [+] [-]	10.191.101.1 [+] [-]	SNMP [+] [-]					
			uei.opennms.org/threshold/re	elativeChangeExceeded [+] [-] Edit notifi	cations for event						
			Relative change exceeded for SNMP datasource ifOutOctets on interface 10.191.101.1, parms: ds="ifOutOctets" value="80593.0" previousValue="37973.0" multiplier="1.05" label="Unknown" ifLabel="eth0-000c29aea14f" ifIndex="2"								
	217564	Warning [+][-]	05/08/08 23:54:51 [<] [>]	group-100-linux.class.example.o [+] [-]	10.191.100.3 [+] [-]	SNMP [+] [-]					
			uei.opennms.org/threshold/re	elativeChangeExceeded [+] [-] Edit notifi	cations for event						
			Relative change exceeded for previousValue="19591.0" mu	r SNMP datasource ifInOctets on interface tiplier="1.05" label="Unknown" ifLabel=	e 10.191.100.3, parms: ds= "eth0-000c29fb7555" ifInde	="ifInOctets" value="70 ex="2"	624.0"				
	217563	Warning [+][-]	05/08/08 23:54:51 [<] [>]	group-100-linux.class.example.o [+] [-]	10.191.100.3 [+] [-]	SNMP [+] [-]					
			uei.opennms.org/threshold/relativeChangeExceeded [+] [-] Edit notifications for event								
			Relative change exceeded for previousValue="14119.0" mu	- SNMP datasource ifOutOctets on interfa Itiplier="1.05" label="Unknown" ifLabel=	ce 10.191.100.3, parms: d: "eth0-000c29fb7555" ifInde	s="ifOutOctets" value=" ex="2"	15337.0"				
1	217538	Warning	05/08/08 23:49:41 [<] [>]	server.class.example.org [+] [-]	10.191.101.1 [+] [-]	SNMP [+] [-]					
	2012/2012/20	[+][-]	·····	lation of the sector and add to 1.0.0 million and	antiona fau avant						

Figure 74: OpenNMS Threshold events from various devices in the raddle network

For those who prefer not to edit XML configuration files, the OpenNMS Admin menu provides a GUI way to create and modify thresholds.

🥹 Admin OpenNMS Web Console - Mozilla Firefox 🎱 📃 🗖 🗙										
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	0									
👍 • 🔿 • 🧭 💿 🏠 🗋 http://opennms:8980/opennms	/admin/index.jsp									
	adons 🖕 🔤 Sourcerorge 🔄 KorrAc-Coningal 🔄 Korritesholding									
OPENNMS [®] User: admin (Notices On) - Log out 06-Aug-2008 00:21 GMT-05:00 Node List Search Octave Dath Octave Dathbard Events Alarme Notifications Acats Departs Chats Surgillance Mar. Advise Hole										
Node List Search Outages Path Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Map Admin Help										
Online	Outline Descriptions									
Configure Discovery Configure Users, Groups and Roles	range to discovery allows you, the Administrator, to add or delete ip address specific and range to discover.									
Configure Notifications Manage and Unmanage Interfaces and Services Configure SNMP Data Collection per Interface Configure SNMP Community Names by IP	Configure Users and Groups allows you, the Administrator, to add, modify or delete existing users. If adding or modifying users, be prepared with user IDs, passwords, notification contact information (pager numbers and/or email addresses), and duty schedule information. You can then Add users to <i>Groups</i> .									
Add Interface Delete Nodes	Configure Notifications allows you to create new notification escalation plans, called									
Import and Export Asset Information	have any arbitrary number of escalations or targets (users or groups) and can send notices									
Scheduled Outages Manage Surveillance Categories	through email, pagers, et cetera. Each notification path can be triggered by any number of									
Manage Applications	When OpenNMS was first started, the nodes, interfaces, and services in the network were									
Manage Provisioning Groups <u>Manage Thresholds</u> Manage Location Monitors	discovered. As your network grows and changes, the TCP/IP ranges you want to manage, as well as the interfaces and services within those ranges, may change. Manage and Unmanage Interfaces and Services allows you to change your OpenNMS configuration along with your network.									
Notification Status: (* On (Off Update	Manage SNNP Data Collection per Interface: This interface will allow you to configure which non-IP interfaces are used in SNMP Data Collection.									
	Configure SNMP Community Names by IP: This interface will allow you to configure the Community String used in SNMP Data Collection.									
	Add Interface is an interface to add an interface to the database. If the IP address of the interface is contained in the ipAddrTable of an existing node, the interface will be added into the node. Otherwise, a new node will be created.									
	Delete Nodes is an interface to permanently delete nodes from the database.									
	Import and Export Asset Information provides an easy-to-use interface for adding data to OpenNMS's asset inventory from your database or spreadsheet application, as well as extracting data from the asset inventory for use in your favorite spreadsheet or database. Our comma-delimited file format is supported by most spreadsheet and database applications, and details for using the Import and Export functionalities can be found through this link as well.									
	Scheduled Outages provides an interface for adding and editing scheduled outages. You can pause notifications, polling, thresholding and data collection (or any combination of the four) for any interface/node for any time.									
	Manage Surveillance Categories allows you to add and delete surveillance categories and edit the list of nodes belonging to each category.									
	Manage applications allows you to manage applications (groups of services on interfaces).									
	Manually Provisioned Nodes allows you to manually add nodes interfaces and services to									

Figure 75: OpenNMS Admin menu

Selecting the "Manage Thresholds" option displays all thresholds currently configured in thresholds.xml.

ile Edit View History Bookmarks Tools Help										
<										
Nagios 🛛 🗋 List Thres	h 📧 🗋 🗅 Nagios Addons 💿 🛛 🚾 SourceForge 🖾 🗍 🌀 FAQ-Configur 🖾 🗋 🌀 Thre	sholding 🖾 🔽								
OPEN NMS [®] Node List Search OL	Threshol User: admin (1 06-Aug-200 ages Path Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance	ds Configuration Notices On) - Log out 8 00:16 GMT-05:00 Map Admin Help								
Home / Admin / Threshold Groups										
Threshold Configuration										
Name	RRD Repository									
CC-snmp	/opt/opennms/share/rrd/snmp/	Edit								
default-snmp	/opt/opennms/share/rrd/snmp/	Edit								
raddle-snmp	/opt/opennms/share/rrd/snmp/	Edit								

Figure 76: OpenNMS Configuring thresholds through the Admin menu

Usin	g the	East butto	on permits	s mo	amca	tion of	an exist	ing t	nres	nold	l.		
<u>F</u> ile <u>E</u>	dit <u>V</u> iew H	Hi <u>s</u> tory <u>B</u> ookmarl	ks <u>T</u> ools <u>H</u> elp										$\langle \rangle$
- 🧼	- C	🕑 🚮 🗋 http://	opennms:8980/op	pennm	s/admin/tł	nresholds/ir	idex.htm?grou	pName=	C 🔻 🕨	- G-	Google		Q)
Nag	gios	🕒 🕒 Edit Gr	oup 🞑 🗋 N	lagios	Addons	🖸 📴 Sou	ceForge	6 FA	.Q-Conf	igur	🖸 🔞 Thre	sholding -	
0	penN	IMS®									User: admin (06-Aug-200	Threshold Notices On) 18 00:25 GI	i Group - Log out MT-05:00
		Node List Search	Outages Path Out	ages D	Dashboard	Events Alarr	ns Notifications	Assets F	Reports	Charts	Surveillance	Map Adm	in Help
Home	e / Admin /	Threshold Group	s / Edit Group										
Edit	group CC-sn	mp											
Basic Type	Datasource	s e Datasource type	Datasource label	Value	Re-arm	Trigger Tr	iggered UEI Re	e-armed U	EI		1		
high	avgBusy5	node		5.0	4.0	2			Edit	Delete			
low	freeMem	node		1024.0	1000000.0	3			Edit	Delete			
Crea	te New Th	nreshold											
Expre	ession-base	ed Thresholds											
Туре	Expression	Datasource type	Datasource label	Value	Re-arm T	rigger Trig	jered UEI Re-a	armed UEI					
Crea	te New Ex	pression-based	Threshold										
Help													
The up thresh To cre	oper section is old line. To de ate a new thre	Basic Thresholds (thre lete the threshold, clic shold, click on the "Cr	sholds on a single dat k on "Delete" on the s reate New Threshold" ¹	tasource ame line link	e). The thres e as the thre	hold details ar shold you war	e displayed to edi t to delete.	t the thresh	nold, click	on the '	"Edit" link on sa	ame line as t	.he
to that	for the Basic	Thresholds section	inresnoids, where the	value b		u is a mathem		including of	ne or moi	re uata s	sources. Function	mancy is ide	nucai
to see	existing notifi	n UEI for triggering or cations for that UEI, ar	nd possibly create a ne	old, then ew notifi	ication for th	nyperlink. Clic at UEI.	king on that link ta	akes you to	the notif	ications	wizard for that	UEI, allowin	g you

Figure 77: OpenNMS Modifying thresholds through the Admin GUI

7.5 Managing OpenNMS

So far, this description of OpenNMS has focused very much on configuration by editing xml files. It is well worth mentioning that there is now an Admin menu (touched on in the Thresholding section previously), which means many of the configuration tasks can be driven by a menu-based, fill-in-the-blanks GUI. Refer back to Figure 75: OpenNMS Admin menu for a list of the areas which can be configured this way.

7.6 OpenNMS summary

OpenNMS is a mature and very capable systems and network management product. It satisfies most requirements for discovery, availability monitoring, problem management and performance management.

It has a clean architecture for configuration with everything being defined in XML files. It has an excellent mechanism for collecting and configuring SNMP TRAPs.

For those who prefer to customise through a GUI, the Admin menu provides access to configure some of these files without needing to know an editor or XML.

It feels like a solid, reliable product and is designed (say the developers) to scale to truly large enterprises. There are lots of good samples provided and the default configurations provide rich functionality.

Areas where it is weak are around formal documentation and the lack of a usable topology map. That said, the help that is provided with OpenNMS panels is very good. Data collection and thresholding is strong. The addition of a MIB compiler and browser would improve matters enormously. It is also short of a way to discover applications that do not support port-sniffing or SNMP.

There are two large problems with OpenNMS that give me great concern. You have to bounce the whole OpenNMS system if you change any configuration files!

The second big issue – known to be under review – is the association between events, alarms and notifications. Currently, notifications are driven from events whereas driving them from alarms would seem preferable. There is also no link between acknowledging events, alarms and notifications.

I have two personal negative feelings with OpenNMS. The first is that it is written in Java. Sorry, but I hate Java applications! To be fair, OpenNMS does not suffer from performance issues that affect so many other Java applications but its logfiles are Java logfiles and life is just too short to find anything useful in them! My second personal non-preference is that OpenNMS is very wordy. The important information never seems to hit the eye on most screens.

8 Zenoss

Zenoss is a third Open Source, multi-function systems and network management tool. Unlike Nagios and OpenNMS, there is a free, core offering (which does seem to have most things you need), and Zenoss Enterprise that has extra add-on goodies, high availability configurations, distributed management server configurations and various support contract offerings which includes some education. For a comparison of the "free" and "fee" alternatives, try <u>http://www.zenoss.com/product/#subscriptions</u>.

Zenoss offers configuration discovery, including layer 3 topology maps, availability monitoring, problem management and performance management. It is based around the ITIL concept of a Configuration Management Database (CMDB), "the Zenoss Standard Model". Zope Enterprise Objects (ZEO) is the back-end object database that stores the configuration model, and Zope is the web application development environment used to display the console. The relational MySQL database is used to hold current and historical events.

Zenoss 2.2 has recently been released which provides "stack" builds – complete bundles including Zenoss and all its prerequisites. These stack installers are available for a wide variety of Linux platforms; standard RPM and source formats are also available. For easy evaluation, a VMware appliance can be downloaded, ready to go.

I tried both the VMware build and the 2.2 stack install for SuSE 10.3; both were relatively painless. The rest of this section is based on the 2.2 stack installation on a machine whose hostname is zenoss.

To access the Web console, point your browser at <u>http://zenoss:8080</u>. The default user is admin with a password of zenoss. The default dashboard is completely configurable but this screenshot is close to the default.

🥹 Zenoss: Dash	board - Mozilla Firefox 🍥			
<u>F</u> ile <u>E</u> dit ⊻iew	Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp			0
🦛 • 🧼 • 🧭	💿 🏠 🖸 http://zenoss:8080/zport/dmo	d/Dashboard	▼ ▶ Google	Q)
🗀 openSUSE 🍕	Getting Started 🔯 Latest Headlines			
700			Device/IP Search	-
zen	USS I CORE		admin Preferences	Logout Help
			Zenoss s	erver time: 17:49:21
Main Viewe	Last updated 2008-07-01 17:50:00.		Configure layout Add portlet	Stop Refresh
Dashboard	Production States	*	Device Issues	
Event Console	Device	Prod State	Device	Events
Network Map	No records found.		wsvr2k1.class.example.org	2
Classes			blue-atlas.skills-1st.co.uk	
Events			bino.skills-1st.co.uk	
Devices Services			group-100-a1.class.example.org	
Processes			Zenoss.skills-1 st.co.uk	
Products			deodar-mgt. skills-1 st. co. uk	
Browse By	Object Watch List	*	wrt54g.skills-1st.co.uk	1
Systems Groups	Object	Events	group-100-c3.class.example.org	1
Locations	X 🛅 /Devices/Discovered	7	group-100-c2.class.example.org	
Reports			group-100-c1.class.example.org	
Management			group-100-b2.class.example.org	
Add Device			group-100-b1.class.example.org	
Mibs Collectors				
Settings				
Event Manager				
				_
Done				0

Figure 78: Zenoss default dashboard

8.1 Configuration – Discovery and topology

There is a good Zenoss Quickstart document available from http://www.zenoss.com/community/docs . Similar to OpenNMS, the architecture is based on object-oriented techniques.

8.1.1 Zenoss discovery

zProperties can be defined for devices, services, processes, products and events. Objects can be grouped and sub-grouped with zProperties being refined and changed throughout the hierarchy. So, for example, the Device object class has default subclasses for different device types, as shown below.

🥹 Zenoss: Devi	ces - Mozilla Firefox	9						
<u>F</u> ile <u>E</u> dit ⊻iew	Hi <u>s</u> tory <u>B</u> ookmarks	<u>T</u> ools <u>H</u> e	elp					0
🦛 • 🧼 • 🥑	💿 🏠 🖸 http://ze	noss:8080/	zport/dmd/[Devices			- ▶ G- Google	Q
CopenSUSE	Getting Started	atest Head	lines					
		atooti iouu		_	_	_	Device/IP Search	9
∠en	OSSIC	ORE					admin Prefer	ences Logout Help
	/Devices						Z	enoss server time: 18:12:09
					_			
Main Views	Classes	Events	zProperties	Templates				
Dashboard Event Console	Summary				-	_	-	
Device List	Events 5		5 26		Sub Count	25	Device Count	21
	Sub-Device	s	9			Devices	9	
Events	Select: <u>All None</u>				Name		<u>Events</u>	
Devices		Subs	Devices	Events				
Services Processes	Discovered	ů	•					
Products		0	-					
Browse By	Network	0	-					
Systems Groups	Ping	U	5					
Locations	Power	2	0					
Networks Reports	Printer	2	0					
Management	Server	7	4	4				
Add Device	no ping	0	1					
Mibs Collectors	1 of 8 k Discover	ed <u>▼ > > </u>	show all	Page Size 40 ok				
Settings								
Event Manager								
Done								0

Figure 79: Zenoss device classes

The class of Devices has a zProperties page as do the classes Network, Server, Printer, etc. Devices will initially be added to the Discovered class and can then be moved to a more appropriate class.



Figure 80: Zenoss Server Device classes

Discovery and monitoring is largely controlled by the combination of zProperties applied to a device, of which there are a large number (most with sensible defaults). Initially, basic SNMP and ping-polling parameters should be configured in the zProperties page for Devices.

🔮 Zenoss: Dev	vices - Mozilla Firefox 🎱					
<u>F</u> ile <u>E</u> dit ⊻iev	w Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> e	lp		<		
700			Device/IP Search			
zen			admin Preferences	Logout Help		
	Devices		Zenoss ser	ver time: 18:23:48		
Main Views	Classes Events Z	Properties Templates				
Dashboard	Proportion Configuration					
Event Console	Property	Value	Туре	Path		
Device List	z Collector Client Timeout	180	int	1		
Network Map	zCollectorDecoding	latin-1	string	1		
Classes	z Collector Log Changes	True 🔻	boolean	1		
Events	zCollectorPlugins	Edit	lines	1		
Devices	z Command Command Timeout	15.0	float	1		
Services	z Command Cycle Time	60	int	1		
Processes	z Command Existance Test	test-f%s	string	1		
Floudets	z Command Login Timeout	10.0	float	1		
Browse By	z Command Login Tries	1	int	1		
Systems	zCommandPassword		string	1		
Groups	z Command Path	/opt/zeposs/libexec	string	1		
Locations Networks Deports	z Command Port	22	int			
	z CommandProtocol	ech	string			
Reports		331	Stilly			
Management	Z Command Search Bath		lines			
Add Device	2 command search rath		iii les	·		
Mibs	- Common d'Une recent		at the second			
Collectors	Command Username	During	sung	·		
Event Manager	- Device Templeter	Device	lin an	1.00		
	2 Device remplates		ines	/		
	z File System MapIgnore Names		string	1		
	z File System MapIgnore Types		lines	1		
	Theor	Inotidmeliconsingion pro	adain a	,		
Dana		reportation and a second strategy and a second strategy and a second strategy and seco	sung			

Figure 82: Zenoss zProperties for the Device class (part 1)

🥘 Zenoss: Devic	es - Mozilla Firefox 🍥			_
<u>F</u> ile <u>E</u> dit <u>∨</u> iew	Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp			0
	zicon	/zport/dmd/img/icons/noicon.png	string	/
	zlfDescription	False 💌	boolean	1
	zInterfaceMapIgnoreNames		string	/
	zInterfaceMapIgnoreTypes		string	/
	zlp Service Map Max Port	1024	int	/
	zKeyPath	~/.ssh/id_dsa	string	/
	zLinks		string	/
	zLocalinterfaceNames	/lo/vmnet	string	/
	zLocallpAddresses	^127/Y0\.0 ^169\.254 ^224	string	/
	z Max OID Per Request	40	int	1
	zPingInterfaceDescription		string	/
	zPingInterfaceName		string	/
	zPingMonitorIgnore	False 💌	boolean	/
	z Prod State Threshold	300	int	1
	z Python Class		string	/
	z Route Map Collect OnlyIndirect	False 💌	boolean	1
	z Route Map Collect Only Local	False 🔽	boolean	1
	zSnmpAuthPassword		string	/
	z SnmpAuth Type		string	/
	z Snmp Communities	public private	lines	,
	z Snmp Community	public	string	/
	z Snmp MonitorIgnore	False 🗾	boolean	/
	z Snmp Port	161	int	,
	z Snmp Priv Password		string	1
	z SnmpPriv Type		string	/
	z Snmp Security Name		string	1
	z Snmp Timeout	2.5	float	/
	z Snmp Tries	2	int	/
	z SnmpVer	v1 <u>•</u>	string	1
	z Status Connect Timeout	15.0	float	1
	z Sysedge Disk MapIgnore Names		string	1
	z TelnetEnable	False 💌	boolean	/

Figure 83: Zenoss zProperties for the Device class (part 2)

zWinEventlog	False 💌	boolean	1			
zWinEventlogMinSeverity	2	int	1			
zWinPassword		string	/			
zWinUser		string	1			
zWmiMonitorIgnore	True 💌	boolean	1			
z×mlRpcMonitorIgnore	True	boolean	1			
Save						
Delete Local Property						
Delete						

Figure 84: Zenoss zProperties for the Device class (part 3)

The left-hand menus of the web console provide an "Add Device" option (nothing is discovered automatically, out-of-the-box).

🥹 Zenoss: dmd -	- Mozilla Firefox 🅘					
<u>F</u> ile <u>E</u> dit ⊻iew	Hi <u>s</u> tory <u>B</u> ookmarks	s <u>T</u> ools <u>H</u> elp				
700		2005			Device/IP Search	
Zen		JORE			admin Preferences	Logout He
					Zenoss s	erver time: 18:52
Main Views	Add Device	2				
Dashboard	Device Name		Device Class Path	[<u>•</u>	
Event Console	Discovery Protocol	snmp 💌				
Device List	Attributes					
Network Map	Snmp Community		Snmp Port	161		
Classes	Tag Number		Serial Number			
Events	Production State	Production	Priority	Normal 💌		
Devices	Rack Slot	0				
Processes		<i>93</i>				
Products	Comments					
Browse By	Relations	1				
Systems	HW Manufacturer		Add	1		
Groups	HW Product		Add	i		
Networks	OS Manufacturer		Add	1		
Reports	OS Product		Add	1		
Management	Location Path			-		
Add Device	New Location		Add			
Mibs	Systems	T.				
Collectors	New System		bbA			
Settings						
Event Manager	Groups	/				
	New DeviceGroup		Add			
	Collector	localhost 💌				
	New Collector		Add			
		Add Device				

Figure 85: Zenoss Add Devices dialogue

Once a device has been discovered (which by default uses ping), if the discovery protocol is set to SNMP then the device will be queried for its SNMP routing table. Any networks that the device has routes to will then be added to the object class of networks.

🥹 Zenoss: Networks - Mozilla Firefox 🎱 📃 🛛 🗙					
Eile Edit ⊻iew History Bookmarks Tools Help ♦					
700				Device/IP	Search
Zen				admin	Preferences Logout Help
	Notworks				Zanoss server time: 18:58:18
<u></u>	Metworks				201033 301 Ver time. 10.30.10
Main Views	Overview zProper	rties Modifications			
Dashhoard					
Event Console	Subnetworks				
Device List					
Network Map	Add Network	Description	Subnets	Number of IPs	Free IPs
Classes	Delete Networke		0	0	254
Events	Delete Networks		1	12	242
Devices	Discover Devices		0	0	254
Services			0	0	65534
Processes	Г <u>10.191.100.0/24</u>		0	1	253
Products	<u>10.191.101.0/24</u>		0	1	253
Browse By	E 88.97.25.0/24		1	1	253
Systems	T <u>172.16.8.0/24</u>		0	0	254
Groups	T <u>172.16.91.0/24</u>		0	0	254
Locations	<u>172.16.222.0/24</u>		0	0	254
Networks	<u>172.16.223.0/24</u>		1	2	252
Reports	<u>172.16.224.0/24</u>		0	0	254
Management	<u>172.16.225.0/24</u>		0	0	254
Add Device	<u>172.30.0.0/16</u>		0	0	65534
Mibs	<u>172.30.5.0/24</u>		0	0	254
Collectors	<u>172.30.100.0/24</u>		1	2	252
Settings Event Manager	T <u>172.31.0.0/16</u>		0	0	65534
Event Manager	<u>172.31.5.0/24</u>		0	0	254
	<u>172.31.100.0/24</u>		5	13	241
	<u>192.168.0.0/24</u>		0	0	254
	<u>192.168.1.0/24</u>		0	0	254
	<u>192.168.10.0/24</u>		0	0	254
	217.206.98.0/24		1	1	253
	1 of 23 💽 162818816 💌	> > show all			Page Size 40 ok
Done					0

Figure 86: Zenoss Networks class with drop-down menu

Once the presence of a network has been discovered, devices can automatically be discovered on that network – this uses a spray ping mechanism. There is a drop-down menu from the top-left corner of the Networks page (which works fine for simple Class C networks). Although the GUI does manage to display subnetworks accurately, even if the subnetmask is not on a byte boundary, the "Discover Devices" menu does not honour the subnetmask. However, a good feature of Zenoss is that there is a command line (CLI) for virtually everything and the CLI for device discovery on a network *does* honour supplied netmasks. For example:

zendisc run --net 10.0.0/24

Note that the Zenoss discovery algorithm is very dependent on getting routing tables using SNMP and the Zenoss server *must* support SNMP itself.

For devices that do not support ping but do support SNMP, they can be added manually with the "Add Device" menu. The zProperties of the device (or class of

devices if you create a subclass) should have zPingMonitorIgnore=True and zSsnmpMonitorIgnore=False.

There are three Zenoss processes that implement discovery:

- zenmodeler can use SNMP, ssh and telnet to discover detailed information about devices. zenmodeler will only be run against devices that have already been discovered by zendisc . By default, zenmodeler runs every 6 hours.
- zenwin detects Windows (WMI) services
- zendisc is a subclass of zenmodeler. It traverses routing tables using SNMP and then uses ping to detect devices on discovered networks.

8.1.2 Zenoss topology maps

Zenoss has an automatic topology mapping option which can display upto 4 hops from a selected device. It even seems to be able to understand networks served by several routers!



Figure 87: Zenoss Network Map showing 4 hops from group-100-r1

8.2 Availability monitoring

Availability monitoring in Zenoss can use 3 different methods:

- ping tests
 - implemented via zenping
 - detects device availability
- service tests
 - \circ implemented via zenstatus
 - $\circ~$ detects services as defined by TCP / UDP ports
- process tests and Windows Services tests
 - implemented via zenprocess
 - detects processes using the SNMP Host Resources MIB using the snmp.IpServiceMap zCollectorPlugin driven by zenmodeler
 - $\circ~$ detects Windows services using WMI using the WinServiceMap driven by zenwin

8.2.1 Basic reachability availability

Basic availability monitoring is controlled by "Collectors". These are also known as "Monitors" (and the documentation can be confusing!), The Collectors menu can be found on the left-hand side.
😻 Zenoss: locali	nost - Mozilla Firefox 🥘		_ 🗆 🗙
<u>F</u> ile <u>E</u> dit <u>∨</u> iew	Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		$\langle \rangle$
🧼 • 🧼 • 🧭	🛞 🏠 🖸 http://zenoss:8080/zport/dmd/Monitors/Performance/localhost	🔹 🕨 💽 Google	9
Ō Zenoss: loca	alhost 🛛 🔄 SpeedTouch 546: 0514C 🔄		•
Zon		Device/IP Search	-
Zer		admin Preferences Log	out Help
	Monitors calhost	Zenoss server t	ime: 17:51:25
	Overview Edit Performance Modifications		
Main Views			
Dashboard	Performance Collector Configuration		
Event Console	Event Log Cycle Interval (secs)	60	
Device List	SNMP Performance Cycle Interval (secs)	300	
Network Map	Process Cycle Interval (secs)	180	
Classes	Process Parallel Jobs	60	
	Windows Service Cycle Interval (secs)	60	
Events	Windows Modeler Cycle Interval (secs)	60	
Devices	Config Cycle Interval (mins)	360	
Services	Ping Time Out (secs)	1.5	
Processes	Ping Tries	2	
Products	Maximum Ping Packets in Flight	75	
Drource Dr	Ping Cycle Time (secs) Maximum Ping Esilures	1440	
browse by	Modeler Cycle Interval (mins)	720	
Systems	Default Discovery Networks	None	
Groups	Render URL	/zport/Render Server	
Locations	Render User		
Networks			
Reports	Devices	Q	
Management	Select: All None		
Add Device	Name	Events	
Mibs	adsl2.skills-1st.co.uk	2	
Collectors	bino.skills-1st.co.uk		_
Event Manager	blue-atlas_skills-1st.co.uk	10	
	deodar.skills-1st.co.uk		
	group-100-a1_class.example.org		
	aroup-100-b1.class.example.org	1	

Figure 88: Zenoss Collectors (Monitors) overview

The devices being monitored are shown at the bottom of the screen. To change any of these parameters, use the "Edit" tab. The defaults for availability monitoring are:

•	Ping cycle time polling	60 sec
•	Ping timeout	$1.5 \sec$
•	Ping retries	2
•	Status (TCP/UDP service) polling interval	60 sec
•	Process (SNMP Host Resources) polling interval	180 sec
•	SNMP performance cycle interval	300 sec

What availability checks are carried out on a device is controlled by the zProperties of that device, remembering that zProperties can be set at any level of the object hierarchy. By default the /Devices class has zPingMonitorIgnore=False and zSnmpMonitorIgnore=False so every device will get ping polling at 1 minute intervals and SNMP polling at 5 minute intervals.

8.2.2 Availability monitoring of services - TCP / UDP ports and windows services

Service monitoring for ${\rm TCP}\,/\,{\rm UDP}$ ports and Windows services, is configured through the "Services" menu.

Zon	~~~				_	Device/IP Search		
	U 33	JUKE				admin Preference	s Logout	Help
<u> </u>	/Services					Zenos	s server time:	18:21:52
Main Views	Classes	Administra	tion zProperties Mod	ifications				
Dashboard	Sub-Folde	rs				<u>a</u>		
Event Console Device List	Select: <u>All</u> <u>None</u>							
Network Man	Name			Sub-Folders		Services		
	In In Service				2	31	758	
Classes	WinService				0	1	19	
Events								
Devices	Services					9		
Services	Name	Port	Description		Monitor	Count		
Processes			(Contraction of the second se		() 			
Products								
Browse By								
Systems								

Figure 89: Zenoss Services menu

A very large number of Windows services are preconfigured out-of-the-box. These services are actually monitored by the zenwin daemon which uses (and requires) WMI on the Windows target machine. Note the "Count" column showing on how many devices these services have been detected

Zon		Device/IP Sear	ch 🔍
		admin Pre	ferences Logout Help
A	/Services /WinService		Zenoss server time: 18:26:28
Main Views	Classes Administration zProperties Modifications		
Dashboard	Sub-Folders	(4	
Event Console	Name Sub-Folders	Services	
Device List Network Man			
	Services	6	
lasses	Select: All None		
vents	Name	Description	Monitor Count
evices		Application Layer Gateway Service	False 0
ervices	AeLookupSvc	Application Experience Lookup Service	False 0
roducts	Alerter	Alerter	False 1
		Application Management	False 1
rowse By		Windows Audio	False 0
ystems	E BITS	Background Intelligent Transfer Service	False 1
roups	Browser	Computer Browser	False 1
etworks	COMSysApp	COM+ System Application	False 0
eports		Indexing Service	False 0
	ClipSrv	ClipBook	False 1
anagement	CryptSvc	Cryptographic Services	False 0
dd Device		DHCP Server	False 1
Ibs		DNS Server	False 1
ettinas	<u>DcomLaunch</u>	DCOM Server Process Launcher	False 0
vent Manager		Distributed File System	False 1
		DHCP Client	False 1
	Discache	DNS Client	False 1
	ERSvc	Error Reporting Service	False 0
	Event System	COM+ Event System	False 1

Figure 90: Zenoss Windows services

 $\label{eq:expectation} Even more IP services come configured out-of-the-box. There are two subclasses of IP services – Privileged and Registered; either can monitor either TCP or UDP ports.$

	5	URE				admin Prefe	rences Lo	gout He
/Services /Ip	Service /Privile	ged					Zenoss server	time: 10:05
	Classes	Administration	zProperties	Modifications				
	Sub-Folders					G		
Name		Sub-Folders				Services		
	Services		_		_	9		
Select: All	None				Dert	Description	Manitar	Count
					108	Description	Ealee	Count
dis-mon					195	DNSIX Network Level Module Audit	False	0
dn6-nim	<u>-aud</u>				196	DNSIX Session Mat Module Audit Redir	False	0
	<u>n-rea</u>				436	DNA-CMI	False	0
					90	DNSIX Securit Attribute Token Map	False	0
					53	Domain Name Server	False	8
					666	doom ld Software	False	0
dpsi					315	DPSI	False	0
					378	NEC Corporation	False	0
☐ dsf					555		False	0
☐ dsfqw					438	dsfgw	False	0
□ dsp					33	Display Support Protocol	False	0
□ dsp3270	<u>0</u>				246	Display Systems Protocol	False	0
dtaq-ste	:-sb				352	DTAG (assigned long ago)	False	0
□ <u>cttk</u>					365	DTK	False	0
□ <u>dwr</u>					644	dwr	False	0
C echo					7	Echo	False	2
E ets					520	extended file name server	False	0
Elcsd					704	errlog copy/server daemon	False	0
embl-nd	t				394	EMBL Nucleic Data Transfer	False	0
emfis-cr	<u>ntl</u>				141	EMFIS Control Service	False	0

Figure 91: Zenoss Privileged IP services

Again, note the "Count" column. Clicking on the service name shows where the service has been detected:

7 on		F			Device/IP Search	
					admin Preference	s Logout H
	/Services /IpService /Privileged	/domain			Zenos	s server time: 10:0
in Views	Status Edit	Administration	zProperties Modificatio	ons		
shboard	Service Class					
nt Console	Name	domain	Monitor	False		
ce List	Port	53	Description	Domain Name S	erver	
ork Map	Send String		Expect Regex			
	Service Keys	domain, tcp_0	0053, udp_00053			
ses	-					
ts	Sonvice Instance	K.				
ces	Service instance	2				
ces	Device		<u>Name</u>	Monite	or Status	5
esses	bino.skills-1st.co.uk		t <u>cp_00053</u>	<u>3</u> True	Up	
cts	wsvr2k1.class.example.org		tcp 00053	<u>3</u> False	None	
	deodar.skills-1st.co.uk		tcp 00053	<u>3</u> False	None	
se By	blue-atlas.skills-1st.co.uk		t <u>cp_00053</u>	<u>3</u> False	None	
ms	bino.skills-1st.co.uk		udp 0005	3 False	None	
	wsvr2k1.class.example.org		udp 0005	3 Faise	None	
5	blue attac ckille 1 at co.uk		udp 0005	3 False	None	
ns	Dide-alias.skiis-Tst.co.dk		<u>uup 0005</u>	<u>s</u> Faise	NUIC	
rks	1 of 8 🛛 🖉 tcp-00053 💌	> > show all			Page	e Size 40 ok
ts						
	-					
agement						
Device						

Figure 92: Zenoss devices running the domain (DNS) service on TCP 53 or UDP 53

The fact that a service has been *detected* does not imply that it is being *monitored* for availability (the default, out-of-the-box, is that nothing is monitored). The "Monitor" column for devices shows whether active monitoring is taking place (and hence events potentially being generated). The "Monitor" field in the top part of the window shows the global default for this service.

To turn on service monitoring globally for a particular service, use the Services menu to find the service in question. You can then use either the "zProperties" tab or the "Edit" tab to change the Monitor global default to True (the default, as shipped, is False).

To turn on service monitoring for a specific device, access the main page for a device and open the "OS" tab. Under the "IP Services" section, click on the "Name" column header to see services detected. Click on the service name which brings up the service status window for the device where the "Monitor" field can be changed – don't forget to click the "Save" button. Note that the "Monitored" box in the IP Services heading bar can be used to toggle the display between *detected* services and *monitored* services.

Note that the drop-down menu to "Add IpService" is driven by typing in a partial match of the service name you want – the subsequent dropdown then shows configured services that match your selection.

8.2.3 Process availability monitoring

Unix / Linux process monitoring relies on the SNMP Host Resources MIB on the target device. Processes to be monitored can be flexibly defined using regular expressions. Start from the "Processes" menu to see processes defined (there are none out-of-the box). Use the drop-down menu to "Add process".

Zon		Device/IP Search
		admin Preferences Logout Help
	/Processes	Zenoss server time: 15:28:19
Main Views Dashboard Event Console Device List Network Map Classes Events Devices Services Processes Products Browse By Systems Groups Locations Networks	Processes	Zenoss server time: 15:28:19
Management Add Device Mibs Collectors Settings Event Manager		

Figure 93: Zenoss Processes with drop-down menu

Supply a process name and it will be added to the list. To modify the *definition* of the process, click on the process name and select the "Edit" tab.

Zen		E				Device/IP	Search	Legent	
A	Processes /firefox					admin	Zenoss s	erver time: "	15:38:20
Main Views	Status Edit	Administration	zProperties	Modifications					
Dashboard Event Console	State at time: 200	8/07/04 15:37:49						_	
Device List	Name	firefox			-				
Network Map	Regex Ignore Parameters	False T							
Classes	Description	,							-18
Events Devices									
Services									
Processes Products	Save								
Browse By									
Systems									
Groups									

Figure 94: Zenoss dialogue for modifying process definition

To modify the zProperties of a process, use the "zProperties" tab.

7en			Device/	1P Search 🧕	
			adm	in Preferences Log	gout Help
^	/Processes /firefox			Zenoss server	time: 15:41:25
Main Views	▼ Status Edit Administration	zProperties Modifications			
Dashboard	zProperties Configuration				
Event Console	Property	Value	Туре	Path	
Network Man	zAlertOnRestart	False 💌	boolean	1	
	zCountProcs	False 💌	boolean	1	
Classes	zFailSeverity	Error	int	1	
Events	z Monitor	True	boolean	1	
Devices	Save				
Processes	Delete Local Property				
Products					
Browse By	-				
Systems					
Groups					
Locations					
Networks					

Figure 95: Zenoss zProperties for the firefox process

To apply process monitoring to a device, from the OS tab of the device page, select the drop-down menu and use the "Add OSProcess" menu. Defined processes are selectable from the drop-down window.

Ien	©ss™	Core							rences Logout	Hel
	/Devices /Server /Linux /	zenoss.skills-1	st.co.uk							
	▼ Status	os _{Ha}								
	▼ Interfaces							6		
	Select: All None									
	Name IF	^o Address		Net	work	MAC			A Lock	
	T eth0 10	0.0.0.131/24		10.0	0.0	00:0C:29:77:2E	:0E	0		1
	T 🗠 13	27.0.0.1/8						0	0	
	Win Servi						Monitored 🔽	6		1
	Caption	StartMode					Name	Status	Lock	1
	1 of 0 10 12 1	show all	Ad	d OSProv	-				Page Size 40 Jak	l
		Site of	Ad	u 00110				6	inge oile in	5
so By	V OS Proces	ses	-					6		4
	LIASS			F	rocess Class: firefo	ox ▼		Status	LOCK	
	IP Service				firefo	x				
	Select: <u>All</u> <u>None</u>				ftp					
	Name	Proto			Ok mahj	ongg			<u>Status</u> Lock	l
	http-alt	tcp		_		, e	e Port 80)			
	agi T	tcp	631	127.0.0.1	IPP (Internet Printing	g Protocol)			0	
	gqi T	udp	631	0.0.0.0	IPP (Internet Printing	g Protocol)				
	mdns.	udp	5353	0.0.0.0	Multicast DNS				0	
	opsession-prxy	tcp	3307	0.0.0.0	OP Session Proxy					
	<u>smtp</u>	tcp	25	127.0.0.1	Simple Mail Transfe	r			0	
	<u>smux</u>	tcp	199	127.0.0.1	SMUX				0	
	snmp	udp	161	0.0.0.0	SNMP				0	
	snmptrap	udp	162	0.0.0.0	SNMPTRAP				0	
	Sunrpc	tcp	111	0.0.0	SUN Remote Proce	dure Call			0	
	sunrpc	udp	111	0.0.0.0	SUN Remote Proce	dure Call				

Figure 96: Zenoss Add OSProcess monitoring to a specific device

Note that there are currently (July 4th, 2008) a couple of bugs to do with process monitoring whereby processes "disappear" from the OS tab of a device and/or show the wrong status (tickets #3408, #3399, #3270). To mitigate against these, the zenprocess daemon should be stopped and restarted whenever modifications have been made to do with processes. You can use the GUI by choosing Settings and selecting the Daemons tab.

Temporarily, it would also be wise to use the menu for the process and select to Lock the process from Deletion.

More sophisticated availability monitoring can be implemented using standard zCollectorPlugins – note that these are *modelling* plugins as distinct from *performance* plugins. zCollector plugins are applied to device classes or devices through the zProperties tab – use the "Edit" link alongside "zCollectorPlugins" to show or modify the plugins applied and available.

Zen					Device/IP S admin	Preferences	Logout
A	/Devices /Discovered /deodar.skills-1st	.co.uk				Zenoss s	erver time:
Main Views	▼ Status OS Hardwar	re Softw	vare Events	Perf Edit			
Dashboard	Sortable Selection		26				
Event Console	Name: zCollectorPlugins						
Network Map	Path: /						
Classes Events Devices Services Processes Products Browse By Systems Groups Locations Networks Booset	zenoss.snmp.NewDeviceMap zenoss.snmp.DeviceMap zenoss.snmp.InterfaceMap zenoss.snmp.RouteMap	x x x x	Hide Fields	zenoss.cmd.darwin.cpu zenoss.cmd.darwin.ifconfig zenoss.cmd.darwin.memory zenoss.cmd.darwin.netstat_an zenoss.cmd.darwin.swap zenoss.cmd.darwin.swap zenoss.cmd.df zenoss.cmd.linux.ifconfig			

Figure 97: Zenoss zCollectorPlugins

Note that the Add Fields / Hide Fields appears greyed out but does actually work. The plugins shown on the left in the screenshot above are the default for the /Devices class. The /Devices/Server class has several more SNMP-based plugins, by default and the /Devices/Server/Windows class has an extra wmi.WinServiceMap plugin.

Documentation on these plugins seems a little sparse but here are a few clues:

Zen		
<u> </u>	/Devices /Server /Windows	
Main Views	Classes Events zProperties	Templates
Dashboard	Sortable Selection	
Event Console	Name: zCollectorPlugins	
Device List	Path: /Server/Windows	
Network Map		-
Classes	zenoss.snmp.NewDeviceMap X	Add Fields
Events	zenoss.snmp.DeviceMap X	
Devices	zenoss.snmp.DellDeviceMap ×	
Services	zenoss.snmp.HPDeviceMap ×	
Processes	zenoss.snmp.InterfaceMap ×	
Products	zenoss.snmp.RouteMap ×	
Tioducto	zenoss.snmp.lpServiceMap ×	
Browse By	zenoss.snmp.HRFileSystemMap ×	
Svstems	zenoss.snmp.HRSWInstalledMap ×	
Groups	zenoss.snmp.HRSWRunMap ×	
Locations	zenoss.snmp.CpuMap ×	
Networks	zenoss.snmp.DellCPUMap ×	
Reports	zenoss.snmp.DellPCIMap ×	
	zenoss.snmp.HPCPUMap ×	
Management	zenoss.snmp.InformantHardDiskMap ×	
Add Device Mibs Collectors	zenoss.wmi.WinServiceMap ×	
Settings Event Manager	Plugins (drag to change order)	
	Save Delete	

Figure 98: Zenoss default plugins for class /Devices/Server/Windows

- zenoss.snmp.InterfaceMap uses SNMP to query for interface info
- zenoss.snmp.IpServiceMap zenstatus daemon queries TCP/UDP port info
- zenoss.snmp.HRSWRunMap uses SNMP to get process info from Host
- zenoss.wmi.WinServiceMap
 - zenwin daemon uses WMI to query for Windows services

One way to find what plugins are applied by default to device classes is to inspect the migration script supplied

resources MIB

 $in\ /usr/local/zenoss/Products/ZenModeler/migrate/zCollectorPlugins.py\ .$

To see what plugins are active on a specific device, use the devices main page menu and select the "More" menu to find the "Collector Plugins" menu.

700					
Zen					
	/Devices /Network /Router /Cisco /group	-100-r1.class.exa	mple.org		
Main Views	▼ Status OS Hardwar	e Software	Events	Perf	Edit
Dashboard	Sortable Selection				
Event Console	Name: zCollectorPlugins				
Device List	Path: /Network/Router/Cisco				
Network Map					
Classes	zenoss.snmp.NewDeviceMap	X Add	l Fields		
Events	zenoss.snmp.DeviceMap	х			
Devices	zenoss.snmp.CiscoMap	X			
Services	zenoss.snmp.interfaceMap	x			
Processes	Zenoss.snmp.Cisconskp	×			
Products	Zenoss.simp.koutemap	<u>^</u>			
Browse By					
Systems					
Groups					
Locations					
Networks					
Reports					
Management					
Add Device					
Mibs					
Collectors					
Settings					
Event Manager	Plugins (drag to change order)				
	Save Delete				

Figure 99: Zenoss zCollectorPlugins for device group-100-r1.class.example.org

When modifying characteristics for specific devices, do note that the main page menu (from the arrow drop-down at the top left corner) has both a "More" submenu (which includes zProperties among other things) and a "Manage" submenu.

Zon	Tee				Device/I	P Search 🧕	
	U 33	TCORE			admi	n Preferences	Logout Help
	/Devices /Server /W	indows /wsw2k1.class.example.c	org			Zenoss s	server time: 11:54:58
Main Views	Statu	S OS Hardware So	ftware Events	Perf Edit			
Dashboard Event Console	More	Custom	.11 Status	: 🍘 Down			
Device List Network Map	Manage	zProperties		Component Type	Status		-
Classes	Run Commands	▶ Templates		WinService			
Events		Administration		Schedule	0		
Devices		Collector Plugins		IpRouteEntry	٢		
Processes		Last Modifications	00	FileSystem	٢		
Products		Last C Event History	00	lpService	•		
Browse By		Fil		Ipinterface	0		
Systems							
Locations	Device Informa	tion					
Networks Reports	Organizers	None		OS Tag #			
Management	Groups	None		Serial #			
Add Device	Systems	None		HW Make	<u>Microsoft</u>		
Mibs	Collector	localhost		HW Model	<u>.1.3.6.1.4.1.311.1.1.3.1.2</u>		
Collectors				OS Make	<u>Microsoft</u>		
Settings				0S Version	Windows 2000 Version 5	<u>0</u>	
Event Manager				Rack Slot	0		
				sysName	WSVR2K1		
				Contact			
	2			Location			

Figure 100: Zenoss Device More submenu

A Admin Preferences Logo A Devices /Discovered /deodar.skills-1st.co.uk Zenoss server tim Main Views Status 05 Hardware Software Events Perf Edit Dashboard More Model Device Model Device Model Device Model Device	н
Main Views Status O5 Hardware Software Events Perf Edit Dashboard More Model Device Model Device Model Device Device List Manage Change Class Class	
Main Views Status OS Hardware Software Events Perf Edit Dashboard More Model Device Model Device Device List Manage Change Class	: 19:10
Main Views Status O5 Hardware Software Events Perf Edit Dashboard More Model Device Model Device Device List Manage Change Class	
Dashboard Event Console Device List Manage Change Class	
Event Console Model Device Model Device Change Class	
Device List Manage Change Class	
Natwork Man Change Class	
Run Commands Reset IP elds	
Classes Davies	
Events zenoss.snmp.InterfaceMa	
Services zenoss.snmp.RouteMap	
Processes used community	
Products Zenoss.snmp.lpServiceM Push Changes	
Browse By Zenoss.snmp.HRSWRunM Clear Heartbeats	
Systems Delete Device	
Groups	
Locations	
Networks Departs	
Management	
Add Device	
Mibs	
Settings	
Event Manager Plugins (drag to change order)	
Save Delete	

Figure 101: Zenoss Device Manage submenu

8.2.4 Running commands on devices

A few Commands are defined out-of-the-box and can be seen using the left-hand "Settings" menu and then selecting the "Commands" tab. New commands can be added using the "Add User Command" drop-down menu.



Figure 102: Zenoss Commands provided out-of-the-box

From a device's main page, there is a submenu to "Run Commands".

Zon	Tee"				Device/	1P Search 🤇		
	1233	I CORE			adm	in Preferences	Logout	Hel
A	/Devices /Network /S	witch /group-100-s2.class.examp	le.org			Zenoss s	erver time: 13	3:11:
Main Views	Status	OS Hardware Sof	tware Events	Perf Edit				
Dashboard								
vent Console	More	s.example.org IP:1	172.31.100.21 Statu	is: ⊘ Up				٦
evice List letwork Map	Manage		C	omponent Type	Status			
125505	Run Commands			pRouteEntry	٢			
vents		DNS forward		pinterface				
evices		DNS reverse						_
ervices		ping						
rocesses		Last	00					
roducts		Last C	00					
rowse By		Fil traceroute						
 ∨stems								
froups								
ocations	Device Informat	ion						
letworks	Organizers			os				
eports	Location	None		Tag #				
anagement	Groups	None		Serial #				
dd Device	Systems	None		HW Make	<u>Cisco</u>			
libs	Collector	localhost		HW Model	<u>2924XLv</u>			
ollectors				OS Make	<u>Unknown</u>			
Settings				0S Version	IOS 12.0(5.1)XP			
Event Manager				Rack Slot	0			2

Figure 103: Zenoss Run Commands for a particular device

Although much of the availability monitoring that has been demonstrated so far relies on SNMP, it is also possible to use ssh or telnet to contact remote devices and run monitoring scripts on them.

8.3 Problem management

The Zenoss event management system can collect events from syslogs, windows event logs, SNMP TRAPs and XML-RPC, in addition to managing events generated by Zenoss itself (such as availability and performance threshold events).

When an event arrives in the Status table of the events database, the default state of the event is set to "New". The event can then be Acknowledged, Suppressed or Dropped. From there, an event will be archived into the Event History database in one of four ways.

- Manually moved to the historical database (historifying)
- Automatic correlation (good event clears bad event)
- An event class rule
- A timeout

Events automatically have a duplication detection rule applied so that if an event of the same *class*, from the same *device*, with the same *severity* arrives, then the repeat count of an existing event will simply be incremented.

Global configuration parameters for the event system can be configured from the "Event Manager" left-hand menu.

By default, status events of severity below Error, are aged out to the Event History database after 4 hours. Historical events are never deleted.

Zon			Device/IP 1	Search 🔍		
261	USS TORE		admin	Preferences	Logout	Hel
A	/ZenEventManager			Zenoss s	erver time: 1	14:52:1
Main Views	Edit Fields H	fistory Fields Commands Modifications				
Dashboard	Connection Informatio	on				
Event Console Device List Network Map	Backend Type User Name Password	mysql Zenoss				
Classes	Database	events				
Events Devices	Hostname	localhost				
Services Processes	Port	3307				
Products	Cache				_	
Browse By	Cache Clear Count	20				
Systems	History Cache Timeout	300				
Locations	History Cache Clear Count	20				1
Networks Reports	Maintenance					
Management	Event Aging Threshold (hours)		4			
Add Device	Don't Age This Severity and Above		Error			
Mibs	Delete Historical Events Older Than (days))	р 7			
Settings	Default Syslog Priority		3			
Event Manager	Save Changes	Save				

Figure 104: Zenoss Event Manager configuration

8.3.1 Event console

The main Event Console is reached from the "Event Console" menu on the left. The default is to show all status events with a severity of Info or higher, sorted first by severity and then by time (most recent first). Events are assigned different severities:

•	Critical	Red
•	Error	Orange
•	Warning	Yellow
•	Info	Blue
•	Debug	Grey
•	Clear	Green

The events system has the concept of active status events and historical events (two different database tables in the MySQL events database).

Events in the console can be filtered by Severity (Info and above by default) and by State (New, Acknowledged and Suppressed where New and Acknowledged are shown by default). Any event which has been Acknowledged changes to a wishy-washy version of the appropriate colour. There is also a Search box at the top right for filtering events.

🥹 Zenoss: Events - M	lozilla Firefox 🅘							
<u>F</u> ile <u>E</u> dit ⊻iew Hi <u>s</u> t	ory <u>B</u> ookmarks <u>T</u>	ools <u>H</u> elp						
🍓 • 🗼 • 💽 🙆	To http://zeno	ss:8080/zpc	ort/dmd/Event	s/viewEvents?notabs=1	•	G - Google		
	TM					Davisa/IB Sasuel	6	
Zeno	SSICO	RE				admin Drefer	ences	Logout H
Event	Console					2	enoss serv	/er time: 16:3
Main Views	t updated 2008-07-04 16:37	:13.	Soy In	fo I State Acknowledged I	Stop 60	1.6	View Eve	nt History
Dashboard	ct: <u>All_None_Acknowledg</u>	ed Unacknowle	dged					1-14 of 28
Event Console	device 🔥	component	eventClass	summary	firstTime	lastTime	count	TT
Network Map	blue-atlas.skills-1st.co		/Status/Ping	ip 10.0.0.2 is down	2008/07/04	2008/07/04	369	
Classes			/Pert/Snmp	threshold of zenperfsnmp cycle time			34	
Events	wsvr2k1 class exampl		/Status/Ping	exceeded: current value 535.96 ip 172.16.223.11 is down		16 30 05 000 2008/07/04		
Services								
Processes					03:02:09:000			Q
	wsvr2k1.class.exampl			Windows Service 'Schedule' is down	2008/06/20	2008/06/24		Q
Browse By	group-100-a1.class.ex		/Status/Ping	ip 172.31.100.3 is down	2008/06/20	2008/06/20	2	
Groups	bino.skills-1st.co.uk	ftp	/Status/OSProc	Process not running: ftp	2008/07/03	2008/07/04	175	
Locations					22:11:55.000	16:34:24.000		
Reports	group-100-s2.class.ex	snmp	/Status/Snmp	snmp agent down	2008/07/04 14:53:08.000	2008/07/04 16:34:04.000	9	Q
Management	group-100-r1.class.exa	<u>snmp</u>	/Status/Snmp	snmp agent down	2008/07/04	2008/07/04	69	Ta I
Add Device	localhost		/Perf/Snmp	threshold of zenperfsnmp cycle time	2008/07/04	2008/07/04	12	
Mibs	zanaca skilla 1 st sa ul	Topportoppop	/Status/Lloarths	exceeded: current value 451.04	02:18:15.000	12:49:00.000	11	
Collectors	Zenoss.skills-Tst.co.ul	zenpensnmp	/Status/Heartbe	heartbeat failure	04:23:08.000	04:52:02.000	1	Q
Event Manager	adsl2.skills-1st.co.uk	IP: PPPoA_1	<u>/Perf/Interface</u>	threshold of Utilization 75 perc	2008/07/02	2008/07/04	248	
	group-100-r1 class ex	Point to mem5minEre	/Perf/Snmn	exceeded: current value 351.27	2008/07/03	2008/07/04	4	
	31000 100 11.0033.0A	manerini te		on group-100-r1.class.example.org (oid	14:33:46.000	00:31:00.000		
	group-100-r1.class.exa	<u>cpu5min</u>	/Perf/Snmp	Error reading value for "cpu5min" on	2008/07/03	2008/07/04	4	
				group room class.example.olg (00	74.55.40.000	00.37.00.000		

Figure 105: Zenoss Event Console

From the Console, events can be selected by checking the box alongside the event and the drop-down can be used for various functions including "Acknowledge" and "Move to History". The drop-down can also be used to generate any test event with the "Add Event" option (if you are a CLI person rather than a GUI person, the zensendevent command is also available).

The column headers of the Event Console can be used to change the sorting criteria and the icon at the far right of the event can be used to display the detailed data of fields.

8.3.2 Internally generated events

Events are automatically generated by Zenoss if an availability metric is missed (such as a ping check failing or a service check failing). Similarly, if performance sampling is setup along with thresholds, then events will be generated if the threshold is breached. Reasonable defaults for such events are configured out-of-the-box. Events are organised in class hierarchies which have zProperties, just like Devices. To modify the properties of an event, select the "Events" option from the left-hand menu.

Zon			Device/IP	Search 🔍
	USS CORE		admin	Preferences Logout H
4	/Events /Status			Zenoss server time: 17:1
Main Views Dashboard Event Console Device List Network Man	Classes Mappings Events zProperties Status Events 10 15 0 0		SubClass Count 1	4 Instance Count 2
Classes Events Devices	SubClasses Select: <u>All None</u>	SubClasses	Instances	Evente
Services Processes Products	Heartbeat	0	0 0	<u>Events</u> 0 4
Browse By	C Nacios	0	0	0 5
Systems Groups Locations	F Perf F Ping	0	0	0 4
Networks Reports	□ Snmp □ Update □ □ Web	0	0	0
Management Add Device	∏ WinService ∏ Wmi	0 1	2	1
Collectors Settings	T XmlRpc	0	0	0
Event Manager	EventClass Mappings	Evaluation	Eve	rage size 40 ok

Figure 106: Zenoss Event classes and subclasses

To modify the context of any event, select the event and use the zProperties tab.

Zon			Device/IP	Search 🤇		
	U 33 100		admin	Preferences	Logout	He
	/Events /Status /OSProcess			Zenoss s	erver time: 1	8:08
Main Views Dashboard	Classes Map	ings Events ZProperties				
Event Console Device List Network Map	Property zEventAction	Value status		Type string	Path /	
Classes Events	z Event Clear Classes			lines	1	
Services Processes Products	ZEventSeverity Save Delete Local P	Original 🔽		int	1	
Browse By	Delete					

Figure 107: Zenoss zProperties for the event class / Event / Status / OSProcess

Events are mapped to Event Classes by Event Class instances. Event Class instances are looked up by a non-unique key called EventClassKey. When an event arrives it is:

- Parsed
- Assigned to the appropriate class and class key
- Context is then applied:
 - \circ $\;$ Event context is defined in the zProperties of an event class
 - After the event context has been applied, then the device context is applied whereby the ProductionState, Location, DeviceClass, DeviceGroups, and Systems, are all attached to the event in the event database.
- Once these properties have been associated with the event, Zenoss attempts to update the zEventProperties. This allows a particular device or class of devices to override the default values for any given event.

To change the event mapping, select the event class and use the Mappings tab.



Figure 108: Zenoss Event mapping

The "Edit" tab allows editing of any of these fields.

8.3.3 SNMP TRAP reception and configuration

Zenoss automatically listens for SNMP TRAPs on UDP/162 (the well-known trap port) using the zentrap process. Some generic TRAPs (2 3 and 4 for Link Down, Link Up and Authentication Failure) are automatically mapped to defined classes. Other generic TRAPs (such as 0, 1 for Cold Start and Warm Start) appear as the /Unknown event class, as will any specific TRAPs. It is simple to map such events to an already

configured event class by selecting the occurrence of the event and using the pull-down menu to select "Map Events to Class" - pick the correct class from the scrollable list.

It is also possible to create new event classes. Starting from Events on the left menu, navigate to the place in the event class hierarchy under which you want to create a new class and use the drop-down menu to "Add New Organizer" and give the class a unique name.



Figure 109: Zenoss menu to create a new event class

8.3.4 email / pager alerting

"Alerting Rules" are Zenoss's way of sending email and/or paging notifications. These are configured on a per-user basis, starting from the "Preferences" menu towards the top right of the web console. The "Alerting Rule" tab then shows existing rules and permits rule creation / deletion.

Zen		RE	_	_	Device/IP Search	
	/ZenUsers /admin				Zenoss s	ervertime: 12:03:11
Main Views Dashboard	Edit Administered 0	bjects Event Views Alerting R	ules			
Event Console Device List Network Map	Add Alerting Rule	Delay Repeat Time Does not repeat	<u>Action</u> email	<u>Enabled</u> True	<u>Send Clear</u> True	
Classes Events Devices Services	Delete Rules					

Figure 110: Zenoss menu to create Alerting Rule

Using the "Edit" tab permits changes of existing alerting rules. Different rules can be applied based on a combination of severity, event state, production state and a more generic filter. The Production State is assigned to a device or device class:

- Production
- Pre-Production
- Test
- Maintenance
- Decommissioned

The Production State can be set or changed using the "Edit" tab from a device main page. The default is Production. The Production State attribute can be used to control whether a device is monitored at all, whether alerts are sent and whether a device is represented on the Zenoss main dashboard. It is very simple to modify the Production State to put a device or class of devices into maintenance, for example.



Figure 111: Zenoss Editing alerting rule

The email or pager message of the Alerting Rule is configured by the "Message" tab and the "Schedule" tab can be used to create different alerting rules at different times.

Zon		Device/IP Search 🤇	
		admin Preferences	Logout Hel
△	/ZenUsers /admin /Alerting Rules /jc_email	Zenoss	server time: 12:17:4
Main Views	Edit Message Schedule		
Dashboard	State at time: 2008/07/08 12:17:28		
Event Console	Message (or Subject)		
Network Man	[zenoss] %(device)s %(summary)s		
	Body		
Classes	Device: %(device)s		
Events	Severity: %(severityString)s		
Devices	Time: %(firstTime)s		
Services	%(message)s		
Processes	Event Detail		
Products	Clear Message (or Subject)		
Browse By	[[zenoss] CLEAR: %(device)s %(clearOrEventSummary)s		
Systems	Event: '%/eumman/e'		
Groups	Cleared by: %(clearSummary)s'		
Locations	At %(clearFirstTime)s		
Networks	Component: %(component)s		
Reports	Severity: %(severityString)s		
Management	Save		
Add Device			
Mibs	Message Format is a python format string. Fields are specified as %(fieldname)s. The list of fields available i	n the event database is: dedupid,	evid, device,
Collectors	component, eventClass, eventKey, summary, message, severity, eventState, eventClassKey, eventGroup, sta suppid manager agent DeviceClass Location Systems DeviceGroups inAddress facility priority ntevid o	teChange, firstTime, lastTime, co wnerid_clearid_DevicePriority	unt, prodState,
Settings	eventClassMapping, monitor.	intens, creans, period nong,	
Event Manager			

Figure 112: Zenoss Alerting rule message format

Global parameters for email and paging, along with other useful parameters, can be defined from the "Settings" left-hand menu.

	CORL						a	dmin Preferences
								Zenoss
Settings	Commands	Users	ZenPacks	Menus	Portlets	Daemons	Versions	Backups
State a	t time: 2008/07/0	08 13:03:14	N.					
SMTP Host				smtp.ourshac	k.com			
SMTP Port (usually 25)				25				
SMTP Username (blank	for none)			s1bjc				
SMTP Password (blank	for none)			iololololok				
From Address for Emai	ls	_						
Use TLS?		Use th	his only if au	thentication	is require	d		
Page Command				\$ZENHOME/b	in/zen			
Dashboard Production	State Threshold			1000				
Dashboard Priority Thre	eshold			2				
State Conversions				Production:10 <u>Pre</u> -Production Test:400 Maintenance:3 Decommissio	00 h:500 000 ned:-1			
Priority Conversions				Highest:5 High:4 Normal:3 Low:2 Lowest:1 Trivial:0				
Administrative Roles				Administrator Analyst Engineer Tester				
Google Maps API Key	Help			ABQIAAAAypyC	g1nKibn1ufo	QNdNGyhRzY	YB7sE	
				Save				

Figure 113: Zenoss Settings parameters

The out-of-the-box email notifications provide handy links back to Zenoss to manipulate the event that is being reported on.



8.3.5 Event automations

Any event can be configured to run an automatic script. This can be in addition to the email / pager alerting rules described above. Such automation scripts are known as Zenoss Commands and are run by the zenactions daemon. They are configured from the "Event Manager" left-hand menu using the "Commands" tab.



Figure 115: Zenoss Event Command definition

8.4 Performance management

Zenoss can collect performance data and threshold it using either SNMP (through the zenperfsnmp daemon) or by commands (typically ssh), using the zencommand daemon. The data is stored and displayed using RRD Tool.

8.4.1 Defining data collection, thresholding and graphs

Configuration of performance data collection, thresholding and display is done through *templates*. As with other Zenoss objects, templates can be applied to a specific device or to a higher level in the device class object hierarchy. To see all the defined templates, navigate to the Devices page and use the left-hand dropdown menu and the "More" submenu to choose "All Templates".

🥹 Zenoss: Devices - Mozilla Firefox 🎱 📃 🗖					
<u>F</u> ile <u>E</u> dit <u>∨</u> iew	Hi <u>s</u> tory <u>B</u> ookmarks	<u>T</u> ools <u>H</u> elp			
< • 🔶 • 🥑	💿 🏠 🖸 http://zer	noss:8080/zport/dmd/Devices/performanceTer	nplates 🔹 🕨 💽 Google 🛛		
700			Device/IP Search		
Zen		ORE	admin Preferences Logout He		
\triangle	/Devices		Zenoss server time: 14:11		
Main Views	Classes Ev	vents zProperties Templates			
Dashboard	All Performa	ance Templates			
Event Console	Select: <u>All None</u>				
Device List Network Man	Name	Definition Path	Description		
	Device	/Devices	Basic template that only collects sysUpTime.		
Classes	Device	/Devices/Network/Router/Cisco	Cisco template that collects cpu and free memory. Has CPU threshold at 90%		
Events		/Devices/Server	Net-SNMP template for late vintage unix device. Has CPU threshold.		
Devices	Device	/Devices/Server/Windows	Windows template that requires Informant MB		
Services	Device	/Devices/Server/Scan	Blank device template. No collection on port scanned devices.		
Processes	Device	/Devices/Server/Cmd	ZenPlugin template for late vintage unix device. Has CPU threshold.		
Floudets	Device	/Devices/Power/UPS/APC	APC Device Profile that tracks battery capacity, load and runtime		
Browse By	Device	/Devices/Ping	Blank Template.		
Systems	Device HRMB	/Devices/Server/Windows/devices/wsvr2k1.class.example.org	Windows template that requires Host Resources MB		
Groups	Device HRMB	/Devices/Server	Windows template that requires Host Resources MB		
Locations	File System	/Devices/Server	Filesystem template that uses HOST-RESOURCES mib. Has a 90% threshold.		
Networks	File System	/Devices/Server/Cmd	Filesystem template that uses ZenPlugins		
Reports	HardDisk	/Devices/Server/Windows	HardDisk I/O template that requires Informat MB		
Management	☐ IpService	/Devices	Place holder for future use.		
Add Device	CSProcess	/Devices	Monitors for OSProcess object		
Mibs	Unused Device HRMB	/Devices/Server	Windows template that requires Host Resources MB		
Collectors	WinService	/Devices	Place holder for future use.		
Settings Event Manager	EthernetCsmacd	/Devices	Standard ethernet interface template with 75% utilization threshold		
Event Manager	ethernetCsmacd	/Devices/Server/Cmd	Ethernet interface template for ZenPlugins with 75% utilization threshold		
	ethernetCsmacd 64	/Devices	Template for 64-bit interface counters. Must use SNMP v2c for it to work.		
	1 of 20 K Device	▼ > >(show all	Page Size 40 ok		

Figure 116: Zenoss All Templates showing all defined performance templates

With the exception of the templates with "HRMIB" in the name, the above figure shows the default templates as-shipped. Note that these are *defined* templates – there is no indication here as to which are active on what objects.

Note in the screenshot above that there are several templates called "Device". Templates can be *bound* to a device or device class to make it active. When determining what data to collect, the zenperfsnmp (or zencommand) daemon first determines the list of Template **names** that are bound to this device or component. For device *components* this is usually just the meta type of the component (e.g. FileSystem, CPU, HardDisk, etc.) For devices, this list is the list of names in the device's *zDeviceTemplates* zProperty.

<u>F</u> ile <u>E</u> dit ⊻iev	v Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		
🤹 • 🧼 • 🧿	🛛 📀 🏠 🖸 http://zenoss:8080/zpo	rt/dmd/Devices/Server/Linux/devices/bino.skills-	1s 🔹 🕨 💽 Google
Zon			Device/IP Search
Zen	USS CORE		admin Preferences Logout He
A	/Devices /Server /Linux /bino.skills-1st.co.uk	(Zenoss server time: 3:11
Main Views	▼ Status OS Hardware	Software Events Perf Edit	
Dashboard	zProperties Configuration		
Event Console	Property	Value	Type Path
Network Man	z Collector Client Timeout	180	int /
	z Collector Decoding	latin-1	string /
Classes	z Collector Log Changes	True 🔽	boolean /
Events	z Collector Plugins	Edit	lines /Server/Linux
Devices	z Command Command Timeout	15.0	float /
Services	z Command Cycle Time	60	int /
Products	z CommandExistance Test	test-f%s	string /
	z Command Login Timeout	10.0	float /
Browse By	z Command Login Tries	1	int /
Systems	zCommandPassword		string /
Groups	zCommandPath	/opt/zenoss/libexec	string /
Networks	z CommandPort	22	int /
Reports	z Command Protocol	ssh	string /
Add Device	z Command Search Path		lines /
Mibs Collectors Settings Event Manager	zCommandUsername		string /
	zDeviceTemplates	Device Device_ <u>HRMIB</u>	lines /Server/Linux
	zFileSystemMapIgnoreNames		string /
	z File System MapIgnore Types		lines /

Figure 117: Zenoss zProperties showing zDeviceTemplate

The default, out-of-the-box, is that the device template called *Device* is bound to each device discovered. As noted in the previous screenshot, there are several templates called Device. The Device template for the class /Devices simply collects sysUpTime. The template called Device for /Devices/Server collects a number of parameters supported by the net-snmp MIB. The template called Device for /Devices/Server/Windows collects various MIB values from the Informant MIB.

For each template name Zenoss searches first the device itself and then up the Device Class hierarchy looking for a template with that name. Zenoss uses the first template that it finds with the correct name, ignoring others with the same name that might exist further up the hierarchy. So, the zenperfsnmp daemon will collect net-SNMP MIB information for Unix / Linux servers and will collect Informant MIB information for Windows servers (as /Devices/Server/Windows is more specific than /Devices/Server). Any actual device can have a local copy of a template and change parameters to suit that specific device.

Template bindings can either be modified by changing the zProperties zDeviceTemplates field or there is a "Bind Templates" menu dropdown from the templates display of any device. (Do remember that, for a device, both the Templates menu and the zProperties menu are off the "More" dropdown submenu).



Figure 118: Zenoss Bind Templates menu

Be aware that when selecting templates to bind, you need to select *all* the templates you want bound (use the Ctrl key to select multiples).

So, what do these templates actually provide?

Templates contain three types of sub objects:

- Data sources what data to collect and method to use eg. MIB OID
- Thresholds expected bounds for data and events to raise if breached
- Graph definitions how to graph the data points

△	/Devices /Server /Templates	s /Device			Zenoss :	server tin	me: 3:33:		
Main Views	Performance Ten	nplate							
Dashboard	State at time: 20	08/08/08 03:29:38							
Event Console	Name Device								
Device List	Description								
Network Map	Net-SNMP template for late vintage unix device. Has CPU								
Classes	threshold.	threshold.							
Events	Save								
Devices									
Services	▼ Data Sources								
Processes	Select: <u>All None</u>					11111			
Products	Name	Source		Source Type	En	abled			
Browse By	「 <u>laLoadInt5</u>	1.3.6.1.4.1	.2021.10.1.5.2	SNMP	Tru	ie			
Systems	☐ <u>memAvailReal</u>	1.3.6.1.4.1	.2021.4.6.0	SNMP Tru		rue			
Groups	memAvailSwap	1.3.6.1.4.1.2021.4.4.0		SNMP True		le			
Locations	☐ <u>memBuffer</u>	.1.3.6.1.4.1.2021.4.14.0		SNMP	P True				
Networks	□ <u>memCached</u>	.1.3.6.1.4.1	.1.3.6.1.4.1.2021.4.15.0		True				
Reports	<u>ssCpuRawIdle</u>	1.3.6.1.4.1	.2021.11.53.0	SNMP	True				
	ssCpuRawSystem	1.3.6.1.4.1	.2021.11.52.0	SNMP	True				
Management	ssCpuRawUser	1.3.6.1.4.1	.2021.11.50.0	SNMP	True				
Add Device	ssCpuRawWait	1.3.6.1.4.1	.2021.11.54.0	SNMP	True				
Mibs	sysUpTime	1.3.6.1.2.1	.25.1.1.0	SNMP	Tru	ie	_		
Collectors	1 of 10 📧 🔍 laLoadInt5 💌	> > show all			Page	Size 40	ok		
Settings									
Event Manager	Thresholds					_			
	Name	<u>Type</u>	Data Points		<u>Severity</u>	Enabled	1		
	CPU Utilization	MinMaxThreshold	ssCpuRawIdle_ssCpuRawIdle		Warning	True			
	 Graph Definitions 						-		
	Select: <u>All None</u>								
	Seg Name	Graph Points			Units	Height	Width		
	0 Load Average	laLoadInt5			load	100	500		
	0 Load Average 5 min	laLoadInt5			processes	100	500		
	1 CPU Utilization	ssCpuRawSystem, ssCpuR	RawUser, ssCpuRawWait		percentage	100	500		
	2 CPU Idle	CPU Utilization, ssCpuRaw	vIdle		percentage	100	500		

Figure 119: Zenoss Device template for /Devices/Server

Zenoss provides two built in types of Data Sources, SNMP and COMMAND. Other types can be provided through ZenPacks. Clicking on the Data Source displays details which can then be modified. Typically an SNMP Data Source will provide a single Data Point (a MIB OID value). Typically the name of the data point will be the same as the name of the data source. This means that when you come to select threshold values or values to graph, you will be selecting names like ssCpuRawWait_ssCpuRaw_wait.

<u>۸</u>	/Devices /Server /Templates /Device /memAvailReal			Zenoss server time: 3:41:50	
Main Views Dashboard	Data Source State at time: 200	8/08/08 03:41:04			
Event Console Device List Network Map	Name Source Type Enabled	memAvailReal SNMP True v			
Classes Events	OID	1.3.6.1.4.1.2021.4.6.0 Save			
Devices Services	Test Against Device		Test		
Processes Products	DataPoints			Type	
Browse By	memAvailReal			GAUGE	

Figure 120: Zenoss Data Source memAvailReal

Note that there is a useful Test button to check your OID against a node that Zenoss knows about. However, beware that this Test button appears to use snmpwalk underthe-covers so if a MIB OID has multiple instances then the snmpwalk will return values successfully. When zenperfsnmp actually collects data, it requires the correct instance as well as the correct MIB OID. If your test is successful but you subsequently see empty graphs with a message of "Missing RRD file" then the problem is likely to be that the MIB instance is incorrect.

Data sources can be added or deleted with the dropdown AddDataSource and DeleteDataSource menus.

Thresholds can be applied to any of the data points collected, along with events to generate if the threshold is breached.

Zon)PE	Device/IP Search
	000		admin Preferences Logout Help
A	/Devices /Server /Templates	/Device /CPU Utilization	Zenoss server time: 3:47:48
Main Views	Min/Max Threshol	d	
Dashboard	State at time:	2008/08/08 03:47:29	
Event Console	Name	CPU Utilization	
Device List Network Map Classes Events Devices	Data Points	IaLoadint5_JaLoadint5 memAvaiReal_memAvaiIReal memAvaiISwap_memAvaiISwap memBuffer_memBuffer memCached_memCached ssCpuRawidle_ssCpuRawidle ssCpuRaw User_ssCpuRaw System ssCpuRawWatssCpuRaw Wat	
Processes	Min Value	sysUp Time_sysUp Time	
Troducts	Max Value		
Browse By Systems	Event Class	/Perf/CPU	
	Severity	Warning 💌	
Locations	Escalate Count	5	
Networks	Enabled	True 💌	
Reports		Save	

Figure 121: Zenoss Threshold on CPU collected data

All of the data points defined in the data sources section are supplied in the top selection box. If an event is to be generated, dropdowns are provided to select the event class and severity. You can also specify an escalation count.

Thresholds can be added or deleted from the Thresholds dropdown menu.

🥹 Zenoss: Devic	e - Mozilla Firefox 🎱						
<u>F</u> ile <u>E</u> dit <u>∨</u> iew	Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> o	ols <u>H</u> elp					
🤹 • 🧼 • 🥑	💿 🏠 🖸 http://zenoss	s:8080/zport/dmd/De	vices/Server/rrdTemplates	/Device 🔹 🕨 🚺	Google		
Classes	un estiviu.						
Events	Save						
Devices							
Processes	✓ Data Sources						
Products	Select: <u>All</u> <u>None</u>						1111
Browse By	Name	Source		Source Type	En	abled	
Systems	IaLoadInt5	1.3.6.1.4	.1.2021.10.1.5.2	SNMP	True	e	
Groups		1.3.6.1.4	.1.2021.4.6.0	SNMP	True	8	
Locations	memAvailSwap	1.3.6.1.4	.1.2021.4.4.0	SNMP	True	в	
Networks	memBuffer	.1.3.6.1.4	4.1.2021.4.14.0	SNMP	True	True	
Reports	memCached	.1.3.6.1.4	4.1.2021.4.15.0	SNMP	SNMP Tru		
Management	ssCpuRawidie	1.3.6.1.4	1 2021 11 53.0	SNMP	True	frue	
Add Device	ssCpuRawSystem	1.3.6.1.4	1 3 6 1 4 1 2021 11 50 0		SNMP Tri		
Mibs	SSCPURAWUSEr	136141202111540		SNMP	SNMP		
Collectors		1.3.6.1.2	1.25.1.1.0	SNMP	True	-	
Event Manager	1 of 10 R lal oadint5	S S1 show all			Page Size 40 ok		
	Thresholds						
		Type	Data Points	<u>S(</u>	everity	Enabled	
	Add Threshold	Min Max Threshold	ssCpuRawldle_ssCpuRawld	le Wa	arning	True	
	Delete Threshold						
	Berete Hinddhola	1					
	Add to Graphs				///////////////////////////////////////	1.111	1111
		Graph Points			<u>Units</u>	Height	Width
	0 Load Average	la Loadint5			load	100	500
	0 Load Average 5 min	a Caultan Sustan as Caul	In the second second		processes	100	500
	CPU Utilization	CPUL Utilization as Couloud	daw user, ssupukaw wali		percentage	100	500
	P CPU Idle	memAvailSwan			KButee	100	500
	B Free Swap	memAvailSwap			hutes	100	500
	4 Free Memory	memAvairteai			bytes	100	500

Figure 122: Zenoss Dropdown menu for data thresholds

Note that this dropdown menu (as is also true of the Data Sources dropdown) has an option to "Add to Graphs".

Graphs can be defined for a wide combination of the collected data points and thresholds. The menu panels are basically a frontend to the RRD graphing tool and, with lots of samples provided, you don't need to get into the details of RRD Tool; however if you wish to, there is plenty of scope to do so.

Graphs can be added, deleted or re-sequenced using the dropdown. Existing graphs are modified by clicking on the graph name.

an					Device/IP Sear	ch		
					admin Pre	eferences	Logout	Help
<u> </u>	/Devices /Server /Templates /Device /CP	U Utilization				Zenoss	server time	: 4:03:54
ews	Graph Definition Graph	Custom Definition	Graph Co	mmands				
	Graph Points							
le	Select: All None						11111	
	Seg Name	Түг	<u>ie</u>	Description				
	O CopuRawWait	Thre	eshold	cpuRawWait				
	1 Ss CpuRaw System	Data	aPoint	ssCpuRawSystem_ssCpuRawSystem				
	2 SSCpuRawUser	Data	aPoint	ssCpuRawUser_ssCpuRawUser				
	3 SSCpuRawWait	Data	aPoint	ssCpuRawWait_ssCpuRawWait				
	State at time: 2008/08/08	04:03:42			_			
	Name	CPU Utilization						
- 8	Height	100						
	Width	500		_				
	Units	percentage						
	Logarithmic Scale	False 🔽						
	Base 1024	False V						
	Mn Y	-1		_				_
ıt	Max Y	-1		_				
	Has Summary	True						
	nas Summary	Savo 1						
		Save						
agor								2

Figure 123: Zenoss Performance template graph definition

Note that graphs can display both data points and thresholds.

All graphs are stored, by default, under /usr/local/zenoss/zenoss/perf/Devices . There is a subdirectory for each device. Component data rrd files are under the os subdirectory with further subdirectories for filesystems, interfaces and processes.

8.4.2 Displaying performance data graphs

To view performance graphs, the Operating System component graphs can be seen from the OS page of a device, by clicking on the relevant interface, filesystem or process. The rest of the performance graphs can be found under the Perf tab.



Figure 124: Zenoss Performance graphs for eth1 interface on bino

You can change the range of data with the "Hourly" dropdown (to daily, weekly, monthly or yearly). Data can be scrolled using the < > bars at either side and the "+" and "-" magnifiers can be used to zoom in / out. By default, all graphs on the page are linked (so that if you change the range on one, it changes for all). They can be decoupled with the "Link Graphs?" check box.

Here is a partial screenshot of the graphs for bino under the Perf tab.



Figure 125: Zenoss Performance graphs available under the Perf tab for bino

Note that the "Reports" left-hand menu also provides access to various reports, including performance reports.

Zon			Device/IP Search 🤒	
			admin Preferences Logout	: Help
A	/Reports		Zenoss server time	: 4:48:11
Main Views	Status			
Dashboard	Report Organizers		Q	
Event Console	Select: <u>All None</u>	<u> </u>		
Device List	Name	SubFolders	Reports	
Network Map	Custom Device Reports	0	0	
Classos	Device Reports	0	8	
Glasses	「 <u>Event Reports</u>	0	3	
Events	Graph Reports	0	0	
Devices	Multi-Graph Reports	0	0	
Services	Performance Reports	0	7	
Processes	User Reports	0	1	
Products	1 of 7 📧 < Custom Device Reports 💌 > > show all		Page Size 40	ok
Browse By				
Systems				
Groups				
Locations				
Networks				
Reports				
Management				
Add Device				

Figure 126: Zenoss Reports menu

Following the "Performance Reports" link provides access to all performance reports for all devices.



Figure 127: Zenoss Performance Reports menu

8.5 Zenoss summary

Zenoss is an extremely comprehensive systems and network management product, satisfying most of my requirements. One feels that the object-oriented architecture is extremely flexible and powerful with most things you require already configured outof-the-box. The automatic discovery and topology mapping options are the most powerful of the products discussed here. It can accommodate Nagios and Cacti plugins and has its own addon architecture in the form of ZenPacks. Zenoss will use SNMP to gain status and performance information from a device but it also has ssh and telnet as alternatives, for those devices where SNMP is inappropriate.

The Quick Start Guide gets you running fast and the Admin Guide provides what it says – a reasonable comprehensive Administrator's Guide. There is also a book by Michael Badger, published June 2008, "Zenoss Core Network and System Monitoring", which is well worth the investment (available both in paper and in electronic format). However, one feels that there is **so** much more in the detail of Zenoss that one needs to know and can find no information on!

My only real negative comment on Zenoss, other than the lack of detailed technical information, is that it is a rapidly evolving product and it feels rather buggy. The current (August 2008) poll on the zenoss-users forum for input to Zenoss 2.3, has many requesters with code reliability and better documentation at the top of their lists!

9 Comparison of Nagios, OpenNMS and Zenoss

Necessarily, comparisons are based on a mixture of "fact" and "feeling" and you need a clear definition of what features are important to your environment before comparisons can be valid for you.

Nagios is an older, more mature product. It evolved from the NetSaint project, emerging as Nagios in 2002. OpenNMS also dates back to 2002 but feels like the lead developer, Tarus Balog, has learned some lessons from observing Nagios. Zenoss is a more recent offering, evolving from an earlier project by developer Erik Dahl and emerging to the community as Zenoss around 2006.

All the products expect to use SNMP - OpenNMS and Zenoss use SNMP as the default monitoring protocol. They all provide other alternatives – Zenoss supports ssh and telnet along with customised ZenPacks; Nagios has NRPE and NSCA agents (both of which, of course, require installing on remote nodes); OpenNMS doesn't have much else to offer out-of-the-box but it can support JMX and HTTP as well as having support for Nagios plugins.

All the products have some user management to define users, passwords and roles with customisation of what a user sees.

OpenNMS and Zenoss use RRD Tool to hold and display performance data; Nagios doesn't really have a performance data capability – Cacti might be a good companion product.

Most surprisingly, given that they all rely on SNMP, none of the products has an SNMP MIB Browser built-in to assist with selecting MIBs for both status monitoring and performance data collection.

There are advocates for and against "agentless" monitoring. Personally, I don't believe in "agentless". Once you have got past ping then you have to have some form of "agent" to do monitoring. The question is, should a management paradigm use an agent that is typically part of a box build (like ssh, SNMP or WMI for Windows), or should the management solution provide its own agent, like Nagios provides NRPE (and most of the commercial management products come with their own agents). If your management system wants its own agents, you then have the huge problem of how you deploy them, check they are running, upgrade them, etc, etc. OpenNMS and Zenoss have a strong dependency on SNMP although Zenoss also supports ssh and telnet monitoring, out-of-the-box (if your environment permits these). SNMP may be old and "Simple", but all three products support SNMP V3 (for those who are worried about the security of SNMP) and virtually everything has an SNMP agent available.

The other form of "agentless" monitoring basically comes down to port sniffing for services. Whilst this can work fine for smaller installations, the n-squared nature of lots of devices and lots of services doesn't scale too well. All three products do port sniffing so it comes down to how easy it is to configure economic monitoring.

9.1 Feature comparisons

The following tables start with my requirements definition and compare the three products on a feature-by-feature basis. (OOTB = Out-Of-The-Box).

	Nagios	OpenNMS	Zenoss
Node discovery	Config file for each node	Config file with include / exclude ranges	GUI, CLI and batch import from text or XML file
Automatic discovery	No	Yes – nodes within configured n/w ranges	Yes – networks & nodes
Interface discovery	Possible through config file	Yes including switch ports	Yes including switch ports
Discover nodes that don't support ping	Yes - use check_ifstatus plugin	Yes – send_event.pl	Yes – use SNMP, ssh or telnet
SQL Database	No	PostgreSQL	mySQL & Zope ZEO
Service (port) discovery	Yes – use plugin (TCP, UDP,)	Yes – various out-of- the-box	Yes – TCP and UDP
Application discovery	Yes – define service	Not without extra agent eg. NRPE	Yes – with ssh, zenPacks or plugins

9.1.1 Discovery

	Nagios	OpenNMS	Zenoss
Supports NRPE / NSClient	Yes	Yes	Possible
SNMP support	V1, 2 & 3	V1, 2 & 3	V1, 2 & 3
L3 topology map	Yes	No	Yes – upto 4 hops
L2 topology map	No	No	No (but may be in plan!)

9.1.2 Availability monitoring

	Nagios	OpenNMS	Zenoss
Ping status monitoring	Yes	Yes	Yes
Alternatives to ping status	Yes – any plugin eg. check_ifstatus	Nagios plugins	Yes – ssh, telnet, ZenPacks, Nagios plugins
Port sniffing	Yes	Yes	Yes
Process monitoring	Yes – with plugins	Nagios plugins	Yes – Host Resources MIB
"Agent" technology	Generally relies on Nagios plugins deployed	SNMP out-of-the-box; customised plugins possible	SNMP, ssh client, WMI for Windows, ZenPacks to be deployed
Availability reports	Yes	Yes	Yes

9.1.3 Problem management

	Nagios	OpenNMS	Zenoss
Configurable event console	No	Yes	Yes
Severity customisation	Yes	Yes	Yes
	Nagios	OpenNMS	Zenoss
--------------------------------	---	--	--
Event configuration	No	Flexible. Lots OOTB	Flexible. Lots OOTB
SNMP TRAP handling	No	Flexible. Lots OOTB	Flexible. Lots OOTB
email / pager notifications	Yes	Yes – with configurable escalation	Yes
Automation		auto-actions on events	auto-actions on events
		good news / bad news correlation on alarms and notifications	good news / bad news correlation on events and notifications
De-duplication	No automatic repeat count mechanism but events do not continue to be raised for existing problems	Yes	Yes
Service / host dependencies	Yes		No
Root-cause analysis	UNREACHABLE status for devices behind network single point of failure. Also, host / service	Outages / Path outages	No
	dependencies.		

9.1.4 Performance management

	Nagios	OpenNMS	Zenoss
Collect performance data using SNMP	No	Yes	Yes
Collect performance data using other methods	No	NSClient, JMX, HTTP	ssh, telnet, other methods using ZenPacks

	Nagios	OpenNMS	Zenoss
Threshold performance data	No	Yes	Yes
Graph performance data	No	Yes – lots provided OOTB	Yes – lots provided OOTB
MIB compiler	No	No	Yes
MIB Browser	No	No	No (though a MIB Browser ZenPack is said to be available for 2.2)

9.2 Product high points and low points

This section is far more subjective – your mileage may vary!

9.2.1 Nagios "goodies" and "baddies"

Good points	Bad points
Good, stable code for systems management	No auto-discovery
Good correlation between service events and host events	Weak event console
Command to check validity of config files	No OOTB collection or thresholding of performance data
Command to reload config files without disrupting Nagios operation	No easy way to receive and interpret SNMP TRAPs
Good documentation	No MIB compiler or browser

9.2.2 OpenNMS "goodies" and "baddies"

Good points	Bad points
Good OOTB functionality	Written in Java – log files hopeless! Difficult to get individual daemon status
Code feels solid	No map (that works reasonably)
Clean, standard configuration through well-organised xml files	GUI is wordy – difficult for the eye to focus on the important things

Good points	Bad points
Single database (PostgreSQL)	Need to bounce entire OpenNMS when almost any config file is changed
LOTS of trap customisation OOTB	Event / alarm / notification architecture is currently a mess (under review)
Ability to do some configuration through web Admin menu	No way to change colours of events
Easy import of TRAP MIBs (mib2opennms)	No MIB compiler or browser
Chargeable support available from The OpenNMS Group	
Supports Nagios plugins	No pdf documentation. Wiki hard to find detailed information.
Some good Howto documents for basic configuration on the wiki	Lots of things undocumented when you get down to details.

9.2.3 Zenoss "goodies" and "baddies"

Good points	Bad points
Good OOTB functionality	No correlation between service events and host events
Architecture good based around object- oriented CMDB database	Implementation feels buggy
Topology map (upto 4 hops)	
Lots of plugins & zenPacks available	No MIB browser
email notifications include URL links back to Zenoss	No way to change colours of events
Commercial version available	Commercial version available
Good "Quick Start" manual , Administrators manual and book	Lots of things undocumented when you get down to details
Supports Nagios & Cacti plugins	

9.3 Conclusions

What to choose? Back to your requirements!

For smallish, systems management environments, Nagios is well tested and reliable with a huge community behind it. For anything more than simple ping checks plus SNMP checks, bear in mind that you may need a way to install remote plugins on target hosts. Notifications are fairly easy to setup but if you need to produce analysis on your event log then Nagios may not be the best choice.

OpenNMS and Zenoss are both extremely competent products covering automatic discovery, availability monitoring, problem management and performance management and reporting. Zenoss has some topology mapping and has better documentation but the code feels less reliable. OpenNMS currently has a rather messy architecture around events, alarms and notifications, though this is said to be under review. I also struggle to believe that you have to recycle the whole of OpenNMS if you have changed a configuration file! The code feels very stable though.

My choice, hoping fervently that code reliability and documentation improves, is Zenoss.

10 References

- 1. "itSMF Pocket Guide: IT Service Management a Companion to ITIL", IT Service Management Forum
- 2. Multi Router Traffic Grapher (MRTG) by Tobi Oetiker, http://oss.oetiker.ch/mrtg/
- 3. RRDtool high performance data logging and graphing system for time series data <u>http://oss.oetiker.ch/rrdtool/</u>
- 4. netdisco network management application http://www.netdisco.org/
- 5. The Dude network monitor by MicroTik, <u>http://www.mikrotik.com/thedude.php</u>
- 6. nagios host, service and network monitoring program <u>http://www.nagios.org/</u>
- 7. Zenoss network, systems and application monitoring <u>http://www.zenoss.com/</u>
- 8. OpenNMS distributed network and systems management platform http://www.opennms.org/
- 9. cacti network graphing solution <u>http://www.cacti.net/</u>
- 10. SNMP Requests For Comment (RFCs) <u>http://www.ietf.org/rfc.html</u>
- 11. V1 RFCs 1155, 1157, 1212, 1213, 1215
- 12. V2 RFCs 2578, 2579, 2580, 3416, 3417, 3418
- 13. V3 RFCs 2578-2580, 3416-18, 3411, 3412, 3413, 3414, 3415
- 14. SNMP Host Resources MIB, RFC s 1514 and 2790 http://www.ietf.org/rfc.html
- 15. PHP scripting language <u>http://www.php.net/</u>
- 16. "Zenoss Core Network and System Monitoring" by Michael Badger, published by PACKT Publishing, June 2008, ISBN 978-1-847194-28-2.

11 Appendix A Cacti installation details

Cacti 0.8.6j-64.4 was installed on an Open SuSE 10.3 Linux system.

Prerequisites are:

- A web server (Apache 2.2.4-70)
- PHP (5.2.5-8.1)
- RRDTool (1.2.23-47)
- net-snmp (5.4.1-19)

• MySQL (5.0.45-22)

Cacti, as well as all of the prerequisites, were available on the Open SuSE 10.3 standard distribution DVD.

Use the "Installation under Unix" instructions available from $\underline{http://www.cacti.net/downloads/docs/html/install_unix.html}$.

A few modifications were required such as:

- No PHP5 configuration was done as the files documented in the installation guide did not exist
- Configuration of Apache2 required no modifications in /etc/apache2/conf.d/php5.conf
- Cacti was installed using the standard SuSE Yast mechanism
- Create the MySQL database by:

cd /usr/share/cacti

```
mysql -user=root -p (and supply the root password when prompted)
```

create database cacti;

source cacti.sql;

GRANT ALL ON cacti.* TO <u>cactiuser@localhost</u> IDENTIFIED BY

'cacti';

(Note that cacti in the above command is the password for the user

cactiuser)

- You need to manually create the Operating System user cactiuser with password cacti
- When pointing your web browser at http://<your server>/cacti/ ensure that you include the trailing slash. Use a web logon of admin, password admin .
- Ensure that apache2 and mysql are either manually started (/etc/init.d/<name> start) or start them automatically at system start using chkconfig
- Ensure that the cactiuser user id can execute the /usr/share/cacti/poller.php script that is run by /etc/crontab.
- Also ensure that the directory that the RRD data is written to (/var/lib/cacti) is writeable by this user.
- cacti.log is in /var/log/cacti
- I found (through /var/log/messages) that poller.php was being run twice, once in /etc/crontab as cactiuser and once in /etc/cron.d/cacti as user wwwrun comment out the line in /etc/cron.d/cacti and check again that cactiuser can write to the data files in /var/lib/cacti .

• The initial console page is a good starting point to add devices to monitor and associated graphs.

About the author

Jane Curry has been a network and systems management technical consultant and trainer for 20 years. During her 11 years working for IBM she fulfilled both pre-sales and consultancy roles spanning the full range of IBM's SystemView products prior to 1996 and then, when IBM bought Tivoli, she specialised in the systems management products of Distributed Monitoring & IBM Tivoli Monitoring (ITM), the network management product, Tivoli NetView and the problem management product Tivoli Enterprise Console (TEC). All these products are based around the Tivoli Framework product and architecture.

Since 1997 Jane has been an independent businesswoman working with many companies, both large and small, commercial and public sector, delivering Tivoli consultancy and training. Over the last 5 years her work has been more involved with Open Source offerings.