SYNGRESS®

FREE E-BOOK DOWNLOAD

Nagios 3 Enterprise Network Monitoring

Including Plug-Ins and Hardware Devices

- Download a VMware Linux Image Including Nagios and the Full Source Code of all Scripts and Configurations from the Book!
- Complete Case Study Demonstrates how to Deploy Nagios Globally in an Enterprise Network
- Monitor Third Party Hardware Devices with Nagios

Max Schubert
Derrick Bennett
Jonathan Gines
Andrew Hay
John Strand

Visit us at

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE
To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of valueadded features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs
Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS
For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET
Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING
Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING
Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

This page intentionally left blank

Nagios 3 Enterprise Network Monitoring Including Plug-Ins and Hardware Devices

Max Schubert
Derrick Bennett
Jonathan Gines
Andrew Hay
John Strand

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	BAL923457U
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0

ISBN 13: 978-1-59749-267-6

Publisher: Andrew Williams
Copy Editor: Beth Roberts
Page Layout and Art: SPi Publishing Services

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights, at Syngress Publishing; email m.pedersen@elsevier.com.

Authors

Max Schubert is an open source advocate, integrator, developer, and IT professional. He enjoys learning programming languages, designing and developing software, and working on any project that involves networks or networking. Max lives in Charlottesville, VA, with his wife and a small herd of rescue dogs. He would like to thank his wife, Marguerite, for her love, support and tolerance of his wild hours and habits throughout this project, his parents for stressing the importance of education, writing, and for instilling a love of learning in him. In addition, Max would like to express his gratitude to the following people who provided him guidance and assistance on his portion of this project: Sam Wenck, for his help in creating the early outline for the security chapter and for his friendship, Ton Voon and Gavin Carr for Nagios::Plugin and for allowing me to use the Nagios::Plugin::SNMP namespace for my own Perl extension to Nagios::Plugin, Joerg Linge and Hendrik Bäcker for the Nagios PNP perfdata / RRD graphing plugin, which I used extensively in this book, my friends Luke Nabavi and Marty Kiefer for their extensive encouragement during the writing of the book, many other friends who encouraged me when I was feeling overwhelmed, and a big thank you to all of the Nagios core developers, plugin authors, and enhancement contributors who's works we have discussed in this publication; it is you who make Nagios the wonderful framework it is today. I would like to also personally thank Andrew Williams, our fearless Publisher, for his encouragement, humor, and ability to make solid and rational decisions to keep us all on track. Finally, my heartfelt thanks to everyone on this writing team; we have produced what I feel is a very solid book in a very short period of time. Thank you all for making this an exciting and satisfying experience.

Derrick Bennett has been working professionally in the IT Field for over 15 years in a full spectrum of Network and Software environments. Being born a bit too late and missing the Assembly bandwagon I started with computers and programming with the Commodore Vic-20 and Basic language programs. From there my time has been spent between both the software and hardware. In the 90's as BBS Sysop, to the mid 90's as an MCSE supporting a large Windows network for a major corporation, to today working with customers of all types to deliver real world

solutions for their environments. During that work I was first exposed to Network monitoring on a global scale, and the pitfalls of trying to monitor enterprise networks over frame-relay and dial up links. While working in the corporate world and supporting large scale environments I also worked with smaller startups and new companies. This was during the initial years of the commercialization of the Internet and many small companies were working hard to provide commercial class service on low end budgets. It was through this work on both enterprise networks and small 5 servers shops that the true advantage of open source projects found their home for me. Since then I have continued working for various large networks where monitoring has always been key. It was through this work that I contributed source code changes to the NRPE project for Nagios adding in SSL encryption along with other updates for the Nagios Core. I have deployed Nagios in over 20 unique environments from 20 servers to a complete NOC covering hundreds of systems spread across every country. A majority of my work has been in integrating Nagios and other tools into existing applications, environments, and processes and making the job of running a system easier for those that maintain it. Even today I find my attraction to the systems and their software to be the same as when I programmed my first basic goto to today when I install a new server and its applications. In a never ending desire to reduce repetitive maintenance and to reduce downtime I hope that everyone reading this will find something that helps make their systems run even better than before. Like most the co-authors on this project I can be found on the Nagios-Dev mailing list nagios-devel@lists.sourceforge.net or at dbennett@anei.com.

I am thankful to those who have done all the great programming before me and to my parents Pat and Fred who not only inspired my involvement with computers but supported my obsessive love for them once I plugged the first one in. I also want to thank Charles and all the other people out there willing to financially support people, employees, or family, who are working on open source projects and supporting the future of great applications. Last I want to say thank you to Ethan, he has been truly devoted to the Nagios project and has contributed more than anyone else ever could. His true support of Nagios and the community is what makes all of these Nagios related resources so worthwhile and has made a good idea into a great application.

Jonathan Gines is a systems integrator, software engineer, and has worked for major corporations providing telecommunications and Internet services, healthcare management, accounting software development, and of course, federal government

contracting. His experience includes serving as an adjunct professor for Virginia Tech, teaching database design and development (yes, including relational algebra, relational calculus, and the ever dreadful normalization forms), developing modeling and simulation models in C++, and good ol' software development using open source programming technologies such as Perl, Java/J2EE, and some frustrating trial and error with Ruby. Jonathan has a graduate degree from Virginia Tech, and holds several certifications including the CISSP and the ITIL Foundation credential.

While not performing UNIX systems administration or troubleshooting enterprise software applications, Jonathan has just completed his doctorate coursework in Biodefense at George Mason University, and stays busy preparing for the PhD candidacy exam. Jonathan would like to thank his friends and immediate family for their loving support, but offers special acknowledgment to his brother, Anthony S. Gines. Anthony, thanks for always willing to lend a helping hand, and serving as an inspiration to try your best.

Andrew Hay is a security expert, trainer, and author of The OSSEC Host-Based Intrusion Detection Guide. As the Integration Services Program Manager at Q1 Labs Inc. his primary responsibility involves the research and integration of log and vulnerability technologies into QRadar, their flagship network security management solution. Prior to joining Q1 Labs, Andrew was CEO and co-founder of Koteas Corporation, a leading provider of end-to-end security and privacy solutions for government and enterprise. His resume also includes various roles and responsibilities at Nokia Enterprise Solutions, Nortel Networks, and Magma Communications, a division of Primus.

Andrew is a strong advocate of security training, certification programs, and public awareness initiatives. He also holds several industry certifications including the CCNA, CCSA, CCSE, CCSE NGX, CCSE Plus, Security+, GSEC, GCIA, GCIH, SSP-MPA, SSP-CNSA, NSA, RHCT, and RHCE.

Andrew would first like to thank his wife Keli for her support, guidance, and unlimited understanding when it comes to his interests. He would also like to thank Chris Fanjoy, Daniella Degrace, Shawn McPartlin, the Trusted Catalyst Community, and of course his parents, Michel and Ellen Hay, and in-laws Rick and Marilyn Litle for their continued support.

John Strand currently teaches the SANS GCIH and CISSP classes. He is currently certified GIAC Gold in the GCIH and GCFW and is a Certified SANS Instructor. He is also a holder of the CISSP certification. He started working computer security

with Accenture Consulting in the areas of intrusion detection, incident response, and vulnerability assessment/penetration testing. He then moved on to Northrop Grumman specializing in DCID 6/3 PL3-PL5 (multi-level security solutions), security architectures, and program certification and accreditation. He currently does consulting with his company Black Hills Information Security. He has a Masters degree from Denver University, and is currently also a professor at Denver University. In his spare time he writes loud rock music and makes various futile attempts at fly-fishing.

Contents

This page intentionally left blank

Foreword

The primary benefit, for anyone picking this book up and reading this Foreword, is to understand that the primary goal here was to explain the advanced features of Nagios 3 in plain English. The authors understand that not everyone who uses Nagios is a programmer. You also need to understand that you do not need to be a programmer to leverage the advanced features of Nagios to make it work for you. Gaining a better understanding of these advanced features is key to unlocking the power of Nagios 3.

The authors start by taking you through the new features of Nagios 3. Scaling Nagios 3, by understanding and implementing the advanced features of Nagios, is also discussed in detail. Understanding these features will help you to take 10 monitored hosts and scale to 100,000 monitored hosts similar to Yahoo! Inc. or Tulip It Services in India. These organizations didn't simply install the default Nagios configuration and start monitoring 100,000 hosts. As you can imagine, a rigorous tuning exercise was performed that included custom security and performance modifications to assist in the monitoring of hosts on their network.

The Plug-ins chapter alone is worth the price of this book. Never has such detail been put into the explanation of plug-in creation and use. As I said before, you don't need to be a programmer to understand the value of this chapter. The authors take the time to ensure that the scripts are explained in plain English so that anyone, from the new Nagios user to the seasoned professional, knows how to use the plug-ins to their advantage.

A real-world case study rounds out the book by explaining how fictional Fortune 500 Company ACME Enterprises implements Nagios 3 to monitor its offices in North America, Europe, and Asia. Most readers will benefit from the description of the ACME implementation and parallel it with the configuration of their own network.

Having just finished writing the *OSSEC Host-Based Intrusion Detection Guide,* I still had the writing bug. When my publisher asked me to contribute to a new book on Nagios 3, I jumped at the opportunity. Since I had previously used Nagios in both an enterprise environment and at home, I thought I could offer insight into my challenges and experiences with the product. I was introduced to my coauthors and was amazed to hear about their level of expertise with Nagios and past contributions to the project. It was obvious that Max Schubert, Derrick Bennett, and Jonathan Gines would be the teachers in this book, and I would be learning as much as I could from them.

In talking with my new coauthors, we realized we needed some additional help with the *Intrusion Detection and Security Analysis with Nagios* chapter. I had experience with intrusion detection and security analysis, but not with respect to Nagios. I reached out to my friend and colleague John Strand to see if he'd be interested in joining the authoring team. He had previously mentioned that he had used Nagios extensively during his incident handling engagements. John was thrilled to join the authoring team and we started immediately.

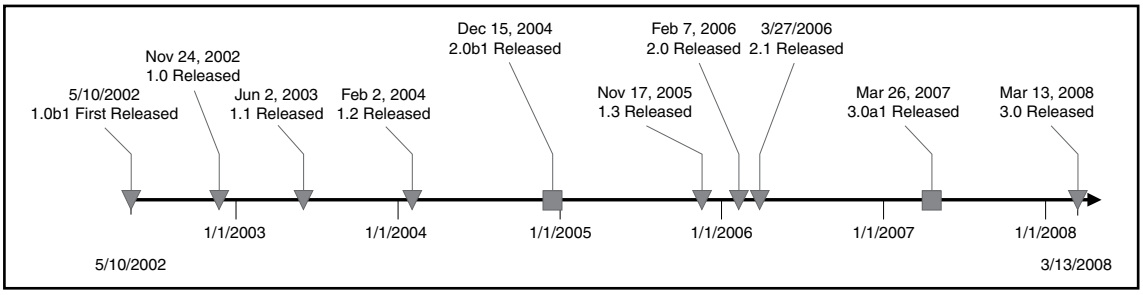
My coauthors and I hope you use this book as a resource to further your knowledge of Nagios 3 and make the application work for you. If Nagios 3 doesn't do what you need it to out of the box, this book will show you how to create your own custom scripts, integrate Nagios with other applications, and make your infrastructure easier to monitor.

—Andrew Hay, Coauthor
Nagios 3 Enterprise Network Monitoring

Introduction

A Brief History of Nagios

Nagios Timeline



In the Beginning, There Was Netsaint

Shortly after the first week of May 2002, Nagios, formerly known as Netsaint, started as a small project meant to tackle the then niche area of network monitoring. Nagios filled a huge need; commercial monitoring products at the time were very expensive, and small office and startup datacenters needed solid system and network monitoring software that could be implemented without "breaking the bank." At the time, many of us were used to compiling our own Linux kernels, and open source applications were not yet popular. Looking back it has been quite a change from Nagios 1.x to Nagios 3.x. In 2002, Nagios competed with products like *What's up Gold*, *Big Brother*,

and other enhanced ping tools. During the 1.x days, release 1.2 became very stable and saw a vast increase in the Nagios user base. Ethan had a stable database backend that came with Nagios that let administrators persist Nagios data to MySQL or PostgreSQL. Many users loved having this database capability as a part of the core of Nagios, Nagios 2.x and NEB, Two Steps Forward, One Step Back (to Some).

Well into the 2.0 beta releases, many people stayed with release 1.2 as it met all the needs of its major user base at that time. The 2.x line brought in new features that started to win over users in larger, "enterprise" organizations; at this time, Nagios also started to gain traction the area of application-level monitoring. Ethan and several core developers added the Nagios Event Broker (NEB), an event-driven plug-in framework that allows developers to write C modules that register with the event broker to receive notification of a wide variety of Nagios events and then act based on those events. At the same time, the relational database persistence layer was removed from Nagios to make the distinction clear between core Nagios and add-ons/plug-ins and to keep Nagios as flexible as possible. NDO Utils, a NEB-based module for Nagios, filled the gap the core database persistence functionality once held. During the 2.x release cycle, NDO Utils matured and was adopted by the very popular NagVis visualization add-on to Nagios.

Enter Nagios 3

With the 3.x release, we see the best of 1.x and 2.x and significant gains in configuration efficiencies and features that make using Nagios in larger environments much easier. The template system now supports multiple inheritance and custom, user-defined variables, a huge win for making maintainable and readable configurations. A number of configuration settings have been added specifically to make Nagios perform more efficiently when used with large numbers of services and hosts. Nagios will now parse and ingest multiline output from scripts, making it much easier to output stack traces, HTML errors, and other longer status messages. The GUI now makes a clear separation between "handled" (acknowledged) service and host problems, making Nagios even easier to use to focus on service and host problems that require attention.

Nagios in the Enterprise—a Flexible Giant Awakens

Move forward six years from the days of Netsaint, and Nagios is now a product that has proven to be a best-in-class open source monitoring solution. It competes well against most commercial applications, and in our opinion, it will in most cases have

a lower cost to deploy and a higher level of effectiveness than many commercial applications in the same market. It has become an application that is both flexible and relatively easy to maintain. For every issue we have seen, there has been a way to monitor it through Nagios using plug-ins from the Nagios community or to create a way to monitor so that 100% meets the needs of the environment Nagios is in. In the progression of Nagios, we have seen the majority of attention paid to core features and functionality. No marketing team has dictated what new color needs to be in the logo, no companies have bought each other to re-brand a good product and leave new development on the floor. We see continued development that only improves on a tool no system or network administrator should be without. The 3.0 Alpha release saw 25 major changes from 2.0 documented in the change log. With almost every subsequent 3.x release, there has been a list of more than 10 new features per version.

As a measure of any good project, one needs to look at the community using it. Since 2.0, the Nagios-Plugins and Nagios Exchange Web sites have grown dramatically—nagiosexchange.org demonstrates the large community involvement in Nagios with custom plug-ins, add-ons, and modifications that have been freely contributed to improve and extend this application. Need to visualize service and host data? NagVis, PNP, nagiosgrapher, and other add-ons will let you do that. Want to give users who are not familiar with Nagios a GUI to edit and create an initial configuration? Use a Web-based GUI add-on—Fruity, Lilac, and NagiosQL are just a few of the administration GUIs available. Want to receive alerts via your blog? Or IM? Or Jabber? Scripts exist to let you do just that. Do not want to create your own integration of Nagios with other network and system monitoring products? A number of choices exist for that as well.

The future looks bright for Nagios in the enterprise; all of the authors on this project firmly believe this, and we believe our book can help you to make best use of Nagios by showing you the wide variety of features of Nagios 3, describing a number of useful add-ons and enhancements for Nagios, and then providing you a cookbook-style chapter full of useful plug-ins that monitor a variety of devices, from HTTP-based applications to CPU utilization to LDAP servers and more. We hope you enjoy this book and get as much out of it by reading and applying the principles and lessons shown in it as we did during the process of writing it.

—The Authors