Nagios System And Network Monitoring

Praxisbuch Nagios (German Animal)
High Performance MySQL
Netzwerkforensik in virtuellen Umgebungen
Network Monitoring System for Servers Using Nagios 3.2
Network Monitoring with Nagios
AI and Machine Learning for Network and Security Management
Learning Nagios 4
Nagios
The Definitive Guide to CentOS
Security Data Visualization
Nagios Core Administration Cookbook
Nagios Core Administration Cookbook (Second Edition)
Network Monitoring Using Nagios and Autoconfiguration for Cyber Defense Competitions
Implementierung einer automatisierten Inventarisierung und Überwachung der Funktionsfähigkeit komplexer IT-Infrastrukturen in Unternehmen
Implementing IBM InfoSphere BigInsights on IBM System x
Practical Packet Analysis
The system of monitoring the utilities status - Nagios
C++ Networking 101
Nagios
Das Nagios / Icinga Kochbuch
Nagios - Das Praxisbuch
Zenoss Core 3.x Network and System Monitoring
Learning Nagios 4
Nagios, 2nd Edition
Nagios Core Administration Cookbook
Learning Nagios
Nagios, 2nd Edition
Building a Monitoring Infrastructure with Nagios
Nagios 3 Enterprise Network Monitoring
Building a National Distributed E-Infrastructure -- PL-Grid
Netzwerküberwachung mit Nagios in einem heterogenen Netzwerk am Beispiel einer Notruf- und Serviceleitstelle
CompTIA CySA+ Study Guide with Online Labs
Learning Nagios 3.0
Linux Firewalls
CompTIA CySA+ Study Guide
Mastering FreeBSD and OpenBSD Security
Nagios
Security Monitoring
Nagios

FRANCIS JAIR

Praxisbuch Nagios (German Animal) Packt Publishing Ltd Annotation For system administrators, network engineers, and security analysts, it is essential to keep a track of network traffic. Zenoss Core is an enterprise-level systems and network monitoring solution that can be as complex as you need it to be. And while just about anyone can install it, turn it on, and monitor "something", Zenoss Core has a complicated interface packed with features. The interface has been drastically improved over version 2, but it's still not the type of software you can use intuitively _ in other words, a bit of guidance is in order. The role of this book is to serve as your Zenoss Core tour guide and save you hours, days, maybe weeks of time. This book will show you how to work with Zenoss and effectively adapt Zenoss for System and Network monitoring. Starting with the Zenoss basics, it requires no existing knowledge of systems management, and whether or not you can recite MIB trees and OIDs from memory is irrelevant. Advanced users will be able to identify ways in which they can customize the system to do more, while less advanced users will appreciate the ease of use Zenoss provides. The book contains step-by-step examples to demonstrate Zenoss Core's capabilities. The best approach to using this book is to sit down with Zenoss and apply the examples found in these pages to your system. The book covers the monitoring basics: adding devices, monitoring for availability and performance, processing events, and reviewing reports. It also dives into more advanced customizations, such as custom device reports, external event handling (for example, syslog server, zensendevent, and Windows Event Logs), custom monitoring templates using SNMP data sources, along with Nagios, and Cacti plugins. An example of a Nagios-style plugin is included and the book shows you where to get an example of a Cacti-compatible plugin for use as a command data source in monitoring templates. In Zenoss Core, ZenPacks are modules that add monitoring functionality. Using the Nagios plugin example, you will learn how to create, package, and distribute a ZenPack. You also learn how to explore Zenoss Core's data model using zendmd so that you can more effectively write event transformations and custom device reports. Implement Zenoss core and fit it into your security management

environment using this easy-to-understand tutorial guide.
High Performance MySQL No Starch Press
Studienarbeit aus dem Jahr 2008 im Fachbereich Informatik - Allgemeines, Note: 1,0, FOM Essen, Hochschule für Oekonomie & Management gemeinnützige GmbH, Hochschulleitung Essen früher Fachhochschule, Sprache: Deutsch, Abstract: In dieser Arbeit wird Nagios als Network Monitoring Service eingesetzt. Es werden neben grundsätzlichen Themen der Netzwerküberwachung Besonderheiten einer Notruf- und Serviceleitstelle dargestellt. Die Arbeit orientiert sich an der Praxis und wird ergänzt durch eine Beispielkonfiguration. Zum Abschluß wird ein Ausblick für weitere Konfigurationsmöglichkeiten, wie Hochverfügbarkeit oder grafischen Visualisierung, gegeben.
Netzwerkforensik in virtuellen Umgebungen NOITE S.C.
System administrators need to stay ahead of new security vulnerabilities that leave their networks exposed every day. A firewall and an intrusion detection systems (IDS) are two important weapons in that fight, enabling you to proactively deny access and monitor network traffic for signs of an attack. Linux Firewalls discusses the technical details of the iptables firewall and the Netfilter framework that are built into the Linux kernel, and it explains how they provide strong filtering, Network Address Translation (NAT), state tracking, and application layer inspection capabilities that rival many commercial tools. You'll learn how to deploy iptables as an IDS with psad and fwsnort and how to build a strong, passive authentication layer around iptables with fwknop. Concrete examples illustrate concepts such as firewall log analysis and policies, passive network authentication and authorization, exploit packet traces, Snort ruleset emulation, and more with coverage of these topics: –Passive network authentication and OS fingerprinting –iptables log analysis and policies –Application layer attack detection with the iptables string match extension –Building an iptables ruleset that emulates a Snort ruleset –Port knocking vs. Single Packet Authorization (SPA) –Tools for visualizing iptables logs Perl and C code snippets offer practical examples that will help you to maximize your deployment of Linux firewalls. If you're responsible for keeping a network secure, you'll find Linux Firewalls invaluable in your attempt to understand attacks and use iptables—along with psad and fwsnort—to detect and even prevent compromises.
Network Monitoring System for Servers Using Nagios 3.2 "O'Reilly Media, Inc."
AI AND MACHINE LEARNING FOR NETWORK AND SECURITY MANAGEMENT Extensive Resource for Understanding Key Tasks of Network and Security Management AI and Machine Learning for Network and Security Management covers a range of key topics of network automation for network and security management, including resource allocation and scheduling, network planning and routing, encrypted traffic classification, anomaly detection, and security operations. In addition, the authors introduce their large-scale intelligent network management and operation system and elaborate on how the aforementioned areas can be integrated into this system, plus how the network service can benefit. Sample ideas covered in this thought-provoking work include: How cognitive means, e.g., knowledge transfer, can help with network and security management How different advanced AI and machine learning techniques can be useful and helpful to facilitate network automation How the introduced techniques can be applied to many other related network and security management tasks Network engineers, content service providers, and cybersecurity service providers can use AI and Machine Learning for Network and Security Management to make better and more informed decisions in their areas of specialization. Students in a variety of related study programs will also derive value from the work by gaining a base understanding of historical foundational knowledge and seeing the key recent developments that have been made in the field.
Network Monitoring with Nagios Apress
Network monitoring can be a complex task to implement and maintain in your IT infrastructure. Nagios, an open-source host, service and network monitoring program can help you streamline your network monitoring tasks and reduce the cost of operation.With this shortcut guide, we'll go over how Nagios fits in the overall network monitoring puzzle. We'll also cover installation and basic usage. Finally, we'll show you how to extend Nagios with other tools to extend functionality.
AI and Machine Learning for Network and Security Management No Starch Press
High Performance MySQL is the definitive guide to building fast, reliable systems with MySQL. Written by noted experts with years of real-world experience building very large systems, this book covers every aspect of MySQL performance in detail, and focuses on robustness, security, and data integrity. High Performance MySQL teaches you advanced techniques in depth so you can bring out MySQL's full power. Learn how to design schemas, indexes, queries and advanced MySQL features for maximum performance, and get detailed guidance for tuning your MySQL server, operating system, and hardware to their fullest potential. You'll also learn practical, safe, high-performance ways to scale your applications with replication, load balancing, high availability, and failover. This second edition is completely revised and greatly expanded, with deeper coverage in all areas. Major additions include: Emphasis throughout on both performance and reliability Thorough coverage of storage engines, including in-depth tuning and optimizations for the InnoDB storage engine Effects of new features in MySQL 5.0 and 5.1, including stored procedures, partitioned databases, triggers, and views A detailed discussion on how to build very large, highly scalable systems with MySQL New options for backups and replication Optimization of advanced querying features, such as full-text searches Four new appendices The book also includes chapters on benchmarking, profiling, backups, security, and tools and techniques to help you measure, monitor, and manage your MySQL installations.
Learning Nagios 4 "O'Reilly Media, Inc."
The future for Nagios in the enterprise is certainly bright! Nagios 3 Enterprise Network Monitoring can help you harness the full power of Nagios in your organization. Nagios 3 contains many significant new features and updates, and this book details them all for you. Once up and running, you'll see how a number of useful add-ons and enhancements for Nagios can extend the functionality of Nagios throughout your organization. And, if you want to learn how to write your own plugins...this is the book for you! In these pages you'll find a cookbook-style chapter full of useful plugins that monitor a variety of devices, from HTTP-based applications to CPU utilization to LDAP servers and more. Complete Case Study Demonstrates how to Deploy Nagios Globally in an Enterprise Network Monitor Third Party Hardware Devices with Nagios
Nagios Packt Pub Limited
An introduction to a range of cyber security issues explains how to utilize graphical approaches to displaying and understanding computer security data, such as network traffic, server logs, and executable files, offering guidelines for identifying a network attack, how to assess a system for vulnerabilities with Afterglow and RUMINT visualization software, and how to protect a system from additional attacks. Original. (Intermediate)

The Definitive Guide to CentOS John Wiley & Sons
This book will introduce Nagios to readers who are interested in monitoring their systems. All the concepts in the book are explained in a simplified manner, presented in an easy-to-understand language with lots of tips, tricks, and illustrations. This book is great for system administrators interested in using Nagios to monitor their systems. It will also help professionals who have already worked with earlier versions of Nagios to understand the new features of Nagios 4 and provides usable solutions to real-life problems related to Nagios administration. To effectively use this book, system administration knowledge is required. If you want to create your own plug-ins, knowledge of scripting languages like Perl, shell and Python is expected.
Security Data Visualization Packt Publishing Ltd
This book will introduce Nagios to readers who are interested in monitoring their systems. All the concepts in the book are explained in a simplified manner, presented in an easytounderstand language with lots of tips, tricks, and illustrations.This book is great for system administrators interested in using Nagios to monitor their systems. It will also help professionals who have already worked with earlier versions of Nagios to understand the new features of Nagios 4 and provides usable solutions to reallife problems related to Nagios administration. To effectively use this book, system administration knowledge is required. If you want to create your own plugins, knowledge of scripting languages like Perl, shell and Python is expected.
Nagios Core Administration Cookbook Prentice Hall
Build real-world, end-to-end network monitoring solutions with Nagios This is the definitive guide to building low-cost, enterprise-strength monitoring infrastructures with Nagios, the world’s leading open source monitoring tool. Network monitoring specialist David Josephsen goes far beyond the basics, demonstrating how to use third-party tools and plug-ins to solve the specific problems in your unique environment. Josephsen introduces Nagios “from the ground up,” showing how to plan for success and leverage today’s most valuable monitoring best practices. Then, using practical examples, real directives, and working code, Josephsen presents detailed monitoring solutions for Windows, Unix, Linux, network equipment, and other platforms and devices. You’ll find thorough discussions of advanced topics, including the use of data visualization to solve complex monitoring problems. This is also the first Nagios book with comprehensive coverage of using Nagios Event Broker to transform and extend Nagios. Understand how Nagios works, in depth: the host and service paradigm, plug-ins, scheduling, and notification Configure Nagios successfully: config files, templates, timeperiods, contacts, hosts, services, escalations, dependencies, and more Streamline deployment with scripting templates, automated discovery, and Nagios GUI tools Use plug-ins and tools to systematically monitor the devices and platforms you need to monitor, the way you need to monitor them Establish front-ends, visual dashboards, and management interfaces with MRTG and RRDTool Build new C-based Nagios Event Broker (NEB) modules, one step at a time Contains easy-to-understand code listings in Unix shell, C, and Perl If you’re responsible for systems monitoring infrastructure in any organization, large or small, this book will help you achieve the results you want–right from the start. David Josephsen is Senior Systems Engineer at DBG, Inc., where he maintains a collection of geographically dispersed server farms. He has more than a decade of hands-on experience with Unix systems, routers, firewalls, and load balancers in support of complex, high-volume networks. Josephsen’s certifications include CISSP, CCNA, CCDA, and MCSE. His co-authored work on Bayesian spam filtering earned a Best Paper award at USENIX LISA 2004. He has been published in both ;login and Sysadmin magazines on topics relating to security, systems monitoring, and spam mitigation. Introduction CHAPTER 1 Best Practices CHAPTER 2 Theory of Operations CHAPTER 3 Installing Nagios CHAPTER 4 Configuring Nagios CHAPTER 5 Bootstrapping the Configs CHAPTER 6 Watching CHAPTER 7 Visualization CHAPTER 8 Nagios Event Broker Interface APPENDIX A Configure Options APPENDIX B nagios.cfg and cgi.cfg APPENDIX C Command-Line Options Index
Nagios Core Administration Cookbook (Second Edition) No Starch Press
CentOS is just like Red Hat, but without the price tag and with the virtuous license. When belts have to be tightened, we want to read about an OS with all the features of a commercial Linux variety, but without the pain. The Definitive Guide to CentOS is the first definitive reference for CentOS and focuses on CentOS alone, the workhorse Linux distribution, that does the heavy lifting in small and medium-size enterprises without drawing too much attention to itself. Provides tutorial and hands-on learning but is also designed to be used as a reference Bases all examples on real-world tasks that readers are likely to perform Serves up hard-won examples and hints and tips from the author's experiences of CentOS in production
Network Monitoring Using Nagios and Autoconfiguration for Cyber Defense Competitions Packt Publishing Ltd
How well does your enterprise stand up against today's sophisticated security threats? In this book, security experts from Cisco Systems demonstrate how to detect damaging security incidents on your global network--first by teaching you which assets you need to monitor closely, and then by helping you develop targeted strategies and pragmatic techniques to protect them. Security Monitoring is based on the authors' years of experience conducting incident response to keep Cisco's global network secure. It offers six steps to improve network monitoring. These steps will help you: Develop Policies: define rules, regulations, and monitoring criteria Know Your Network: build knowledge of your infrastructure with network telemetry Select Your Targets: define the subset of infrastructure to be monitored Choose Event Sources: identify event types needed to discover policy violations Feed and Tune: collect data, generate alerts, and tune systems using contextual information Maintain Dependable Event Sources: prevent critical gaps in collecting and monitoring events Security Monitoring illustrates these steps with detailed examples that will help you learn to select and deploy the best techniques for monitoring your own enterprise network.
Implementierung einer automatisierten Inventarisierung und Überwachung der Funktionsfähigkeit komplexer IT-Infrastrukturen in Unternehmen BoD – Books on Demand
Virtual, hands-on learning labs allow you to apply your technical skills using live hardware and software hosted in the cloud. So Sybex has bundled CompTIA CySA+ labs from Practice Labs, the IT Competency Hub, with our popular CompTIA CySA+ Study Guide, Second Edition. Working in these labs gives you the same experience you need to prepare for the CompTIA CySA+ Exam CS0-002 that you would face in a real-life setting. Used in addition to the book, the labs are a proven way to prepare for the certification and for work in the cybersecurity field. The CompTIA CySA+ Study Guide Exam CS0-002, Second Edition provides clear and concise information on crucial security topics and verified 100% coverage of the revised CompTIA Cybersecurity Analyst+ (CySA+) exam objectives. You’ll be able to gain insight from practical, real-world examples, plus chapter reviews and exam highlights. Turn to this comprehensive resource to gain authoritative coverage of a range of security subject areas. Review threat and vulnerability management topics Expand your

knowledge of software and systems security Gain greater understanding of security operations and monitoring Study incident response information Get guidance on compliance and assessment The CompTIA CySA+ Study Guide, Second Edition connects you to useful study tools that help you prepare for the exam. Gain confidence by using its interactive online test bank with hundreds of bonus practice questions, electronic flashcards, and a searchable glossary of key cybersecurity terms. You also get access to hands-on labs and have the opportunity to create a cybersecurity toolkit. Leading security experts, Mike Chapple and David Seidl, wrote this valuable guide to help you prepare to be CompTIA Security+ certified. If you’re an IT professional who has earned your CompTIA Security+ certification, success on the CySA+ (Cybersecurity Analyst) exam stands as an impressive addition to your professional credentials. Preparing and taking the CS0-002 exam can also help you plan for advanced certifications, such as the CompTIA Advanced Security Practitioner (CASP+). And with this edition you also get Practice Labs virtual labs that run from your browser. The registration code is included with the book and gives you 6 months unlimited access to Practice Labs CompTIA CySA+ Exam CS0-002 Labs with 30 unique lab modules to practice your skills.

Implementing IBM InfoSphere BigInsights on IBM System x No Starch Press

This book is an invaluable resource for aspiring network administrators aiming to deepen their understanding of networking concepts while strengthening their C++ programming skills. Across eleven chapters, this book bridges the gap between network administration and programming, providing readers with a holistic approach to mastering network operations. Readers begin with a deep dive into network fundamentals such as TCP/IP models, sockets, and protocols. They then progress to practical programming, employing C++ to establish TCP/UDP client-server connections, handle network errors, and deal with application layer protocols such as HTTP/HTTPS, FTP, SMTP, IMAP, and DNS. The book then guides readers through Virtual Private Networks (VPNs), detailing their importance, functioning, and distinct types of VPNs. It explores wireless networking and asynchronous programming, providing clear illustrations of WiFi, Bluetooth, and Zigbee setup using C++. It covers critical wireless standards and security protocols. For a comprehensive understanding, the book illustrates network configuration management using C++ to automate crucial network operations tasks, thus highlighting the power of programming in network management. Advanced topics include network testing and simulations, which provide insights into performance enhancement and network robustness. A detailed exploration of network monitoring enhances the reader's skillset, teaching ways to conduct fault, performance, security, and account monitoring. In the end, the book rounds up with network troubleshooting, elucidating several essential network troubleshooting tools and methodologies. Key Learnings Understand TCP/IP model and protocols with hands-on C++ programming. Master TCP/UDP client-server connections and error handling. Grasp application layer protocols like HTTP/HTTPS, FTP, SMTP, IMAP, and DNS. Discover the importance and use of VPNs and how to set them up. Learn about wireless networking and asynchronous programming. Gain insights into network configuration management. Understand network testing methodologies and simulations. Learn to monitor various aspects of a network using Nagios. Learn about essential network troubleshooting tools and methodologies. Enhance network performance and reliability through C++ programming. The essence of this book lies in its practical approach. With ample illustrations, code snippets, and hands-on exercises using C++, this book stands out as a definitive guide for anyone aiming to become a competent network administrator, equipped with the power of programming. Table of Contents Introduction to Networking and C++ Understanding Internet Protocols - TCP and UDP Network Interfaces and Addressing Application Layer Protocols VPNs Wireless Networks Asynchronous Programming Network Testing and Simulation Network Configuration and Management Network Monitoring Network Troubleshooting Audience This book is suitable for every computer programmer or computer science graduate with a basic understanding of C++. No prior networking knowledge is required. Familiarity with fundamental C++ concepts, such as variables, loops, and basic syntax, is assumed. By focusing on practical examples and clear explanations, this guide ensures a fast-paced learning experience.

Practical Packet Analysis diplom.de

Inhaltsangabe:Einleitung: In heutigen Unternehmen gehört der Computer neben dem Telefon und dem Fax zur Standardausrüstung. Die Vernetzung der Computertechnik und die erforderlichen Applikationen sind in Unternehmen für eine effektive und reibungslose Kommunikation von Geschäftsprozessen unabdingbar. Die steigende Anzahl der Hardware, deren komplexere Vernetzung und die hohe Anzahl unterschiedlicher Softwareprodukte in Verbindung mit Lizenzrechten erhöhen den administrativen Aufwand für ein Unternehmen rasant. Laut einer IDC–Studie steigen die IT–Investitionen in den Jahren 2006-2011 in den verschiedensten Branchen weiter an. Vor allem bei Softwareinvestitionen ist eine Wachstumsrate bis zu 6,3 Prozent zu beobachten. Durch derartige Prognosen ist zu erkennen, dass neben der Hardwareverwaltung auch die Software- und damit verbundene Lizenzverwaltung für den administrativen Sektor weiter in den Vordergrund rückt. Das bedeutet für ein Unternehmen und deren IT–Abteilung Mehraufwand sowohl im finanziellen als auch im organisatorischen Sektor. Auf Grund von Analysen im IT–Sektor und Rücksprachen mit leitenden IT–Fachleuten aus den verschiedenen Branchen kann rückblickend geschlussfolgert werden, dass im Bereich der Verwaltung und Überwachung der IT–Infrastruktur (auch als IT–Asset–Management bezeichnet) in Unternehmen immer noch hohe Defizite vorhanden sind. Für die Inventarisierung und Überwachung derartiger Bereiche sind häufig Lösungen (soweit vorhanden) umgesetzt, die folgende Unstimmigkeiten aufweisen können: - erheblicher Arbeitsaufwand, den IST–Zustand über die einzelnen Bereiche aufrecht zu erhalten und zu überwachen. - realisierte Insellösungen, damit sind technische Systeme gemeint, die nur innerhalb ihrer eigenen Grenzen wirksam sind und nicht mit Systemen in der Umgebung zusammenwirken können. - hohe Komplexität und dadurch aufwändig in der Administration. - unzureichender Informationsgehalt der inventarisierten bzw. überwachten Komponenten. - hohe Anschaffungskosten (hinsichtlich der Lizenzkosten oder der Softwareeinführung). - fehlende offene Schnittstellen für die Anpassung anhand eigener im Unternehmen erforderlicher Bedürfnisse. Zugleich ist die IT–Landschaft in den letzten Jahren heterogener und dynamischer geworden und die Komplexität der IT–Infrastrukturen stark gestiegen. Ein Unternehmen und deren Geschäftsprozesse stützen sich gegenwärtig immer mehr auf vorhandene heterogene IT–Netzwerkstrukturen. Durch diese Abhängigkeit [...]

The system of monitoring the utilities status - Nagios Nagios, 2nd Edition

Good system administrators recognize problems long before anyone asks, "Hey, is the Internet down?" Nagios, an open source system and network monitoring tool, has emerged as the most popular solution for sys admins in organizations of all sizes. It's robust but also complex, and Nagios: System and Network

Monitoring, 2nd Edition, updated to address Nagios 3.0, will help you take full advantage of this program. Nagios, which runs on Linux and most *nix variants, can be configured to continuously monitor network services such as SMTP, POP3, HTTP, NNTP, SSH, and FTP. It can also supervise host resources (processor load, disk and memory usage, running processes, log files, and so on) and environmental factors, such as temperature and humidity. This book is your guide to getting the most out of this versatile and powerful monitoring tool. Inside Nagios, you'll learn how to: Install and configure the Nagios core, all standard plugins, and selected third-party plugins Configure the notification system to alert you of ongoing problems-and to alarm others in case of a serious crisis Program event handlers to take automatic action when trouble occurs Write Perl plugins to customize Nagios for your unique needs Quickly understand your Nagios data using graphing and visualization tools Monitor Windows servers, SAP systems, and Oracle databases The book also includes a chapter that highlights the differences between Nagios versions 2 and 3 and gives practical migration and compatibility tips. Nagios: System and Network Monitoring, 2nd Edition is a great starting point for configuring and using Nagios in your own environment.

C++ Networking 101 No Starch Press

Cloud-Umgebungen auf Basis virtueller Maschinen und virtueller Netzwerke gewinnen immer mehr an Bedeutung. Während diese Infrastrukturen für Kunden und Anbieter viele Vorteile bieten, verkomplizieren sich zeitgleich netzwerkforensische Untersuchungen, die durch Strafverfolgungsbehörden oder IT-Sicherheitsteams durchgeführt werden. Dieses Buch untersucht und bewertet die neu auftretenden Probleme, definiert ein angepasstes Vorgehensmodell für die Netzwerkforensik in virtuellen Umgebungen und stellt zwei Lösungen vor, die in hochdynamischen und flexiblen virtuellen Netzwerken auf Basis von Open vSwitch und OpenFlow geeignete Techniken zur Untersuchung bieten. Somit sind forensische Arbeiten zur Aufklärung von Straftaten oder IT-Sicherheitsvorfällen möglich, die bisher mit den traditionellen Techniken nicht umgesetzt werden konnten.

Nagios O'Reilly Germany

FreeBSD and OpenBSD are increasingly gaining traction in educational institutions, non-profits, and corporations worldwide because they provide significant security advantages over Linux. Although a lot can be said for the robustness, clean organization, and stability of the BSD operating systems, security is one of the main reasons system administrators use these two platforms.There are plenty of books to help you get a FreeBSD or OpenBSD system off the ground, and all of them touch on security to some extent, usually dedicating a chapter to the subject. But, as security is commonly named as the key concern for today's system administrators, a single chapter on the subject can't provide the depth of information you need to keep your systems secure.FreeBSD and OpenBSD are rife with security "building blocks" that you can put to use, and Mastering FreeBSD and OpenBSD Security shows you how. Both operating systems have kernel options and filesystem features that go well beyond traditional Unix permissions and controls. This power and flexibility is valuable, but the colossal range of possibilities need to be tackled one step at a time. This book walks you through the installation of a hardened operating system, the installation and configuration of critical services, and ongoing maintenance of your FreeBSD and OpenBSD systems.Using an application-specific approach that builds on your existing knowledge, the book provides sound technical information on FreeBSD and Open-BSD security with plenty of real-world examples to help you configure and deploy a secure system. By imparting a solid technical foundation as well as practical know-how, it enables administrators to push their server's security to the next level. Even administrators in other environments--like Linux and Solaris--can find useful paradigms to emulate.Written by security professionals with two decades of operating system experience, Mastering FreeBSD and OpenBSD Security features broad and deep explanations of how how to secure your most critical systems. Where other books on BSD systems help you achieve functionality, this book will help you more thoroughly secure your deployments.

Das Nagios / Icinga Kochbuch Packt Publishing

Provides information on ways to use Wireshark to capture and analyze packets, covering such topics as building customized capture and display filters, graphing traffic patterns, and building statistics and reports.

Related with Nagios System And Network Monitoring:
© Nagios System And Network Monitoring Physiology Lab Experiments
© Nagios System And Network Monitoring Physics Waves Practice Problems
© Nagios System And Network Monitoring Pic Of Anatomy Of Abdomen