

Profile Norbert Klein

Linux System Administrator

- * **SLES (Novell Suse Linux Enterprise Server)**
- * **GPFS (IBM General Parallel File System)**
- * **Nagios and Cacti**
- * **Apache hardening**
- * **IDS/IPS systems with Snort**
- * **Training**

Personal Data

Year of birth: 1974
Degree: Diplom-Informatiker(FH)
Certification: Novell CLP/CLE 10
Foreign languages: English (fluent),
French (advanced)
IT experience since: 2000

Hourly rate: 65€ + VAT, all-inclusive, on location
55€ + VAT, remote

Daily rate: 520€ + VAT, all-inclusive, on location
440€ + VAT, remote

Contact

Web: <http://www.infosecprojects.net/>
Email: norbert.klein@infosecprojects.net
Mobile: 0172 4728123

IT knowledge / experience

Operating systems

SLES 10, 11
openSUSE
Debian

Programming languages

Bash, Perl, PHP, C
XHTML, CSS
SQL

Products / standards

Apache, mod_security, mod_rewrite, mod_proxy
MySQL
Bind
Nagios, NRPE, NSCA, NConf, PNP4Nagios, NagVis
Cacti, Weathermap-Plugin
iptables
Postfix
syslog-ng
Confluence
LVS/Keepalived Cluster
Subversion
XEN
Snort
Cfengine
SELinux
LVM
OTRS
SNMP
ITIL (basic knowledge)
OpenVPN

Hardware

Dell PowerEdge-Server
IBM xSeries-Server
WatchGuard Firebox

Projects

2010-06-09 – 2010-06-18

Parken in Mainz GmbH (PMG) Mainz

- Setup of a monitoring solution for the technology of the parking decks in Mainz based on Nagios, NagVis and PNP4Nagios.
- Documentation for end users and administrators.
- The main focus here was to create a graphical front-end with NagVis which is nice and easy to use. For that I created some new iconsets and arranged them in NagVis so that the status of all parking decks can be viewed on one screen.
- The Nagios configuration has been structured in a way that different views of the parking deck technology can be displayed in NagVis: e.g. according to location, according to the type of the devices, etc..
- The long-term logging of all the data and its graphical presentation has been realised with PNP4Nagios.
- This flexible open source solution saved more than 5000 Euro initial licence fees compared to a solution with Microsofts SCOM (System Center Operations Manager)!

2010-03-02 – 2010-03-03

Kommunales Rechenzentrum Niederrhein (KRZN) Kamp-Lintfort

- Setup of a GPFS cluster.
- Installation of lin_taped with driver and utilities.
- Creation of necessary udev rules for the IBM tape devices.

2010-11-29

[A web hoster]

- Writing of a bash script to clean up the web content of customers after a successful hacking attack.

2010-11-11 – 2010-06-02

DB Systel GmbH Erfurt

Design of a distributed and redundant monitoring architecture with Nagios 3, NRPE, check_multi and check_logfiles for about 1800 Servers.

Planning and design

- As-is analysis of the existing monitoring environment.
- Rough concept for setting up Nagios, NRPE, check_multi and check_logfiles with central configuration.
- Concept for a Nagios configuration frontend which allows large-scale modifications of the Nagios configuration. Every change can be made on an arbitrary number of hosts and/or services. This frontend also serves as an interface to existing systems and generates a new Nagios configuration automatically based on the data of those systems. Thus, the monitoring is integrated in the IT environment and the Nagios configuration remains up-to-date.
- Definition of processes for operation and maintenance of this architecture.
- Evaluation of Thruk and MK Livestatus.

Implementation

- Porting of checks from the existing monitoring system to Nagios.
- Writing of SPEC files and RPM packaging for all Nagios components.
- Connecting Nagios to a Netcool console via syslog-ng, logger and bash scripts. Every check result is sent to Netcool. Acknowledgements are synchronized between Nagios and Netcool. A heart beat is sent from Nagios to Netcool.
- Usage of check_multi with central configuration. "Feed passive" tested.
- Writing of additional Nagios plugins as bash scripts.
- Writing of helper scripts for several operations via external commands which are not yet supported by the Nagios web interface.
- Customizing of the Nagios web frontend.
- Creation of new init scripts.
- Configuration of several services like Postfix and syslog/syslog-ng.

Load testing and performance tuning

- Testing of the performance impact if nsca encryption is enabled in a distributed Nagios environment.
- Using of OCP daemons for performance improvement.
- Writing of a script which allows to analyse the performance of every single Nagios plugin.
- Writing of bash skripts to automate load testing for an arbitray number of running Nagios instances, hosts and services.
- Nagios performance tuning so that more than 2000 servers with more than 51000 services can be monitored on a single machine with 8 cpu cores. The average host and service latency is below 0.5 seconds. The check interval is 5 minutes.

Documentation and knowledge transfer

- Creation of diagrams and presentations.
- Very detailed documentation as word documents and wiki pages.

2009-11-27

Carpe diem GmbH Wiesbaden

- Nagios 3 training on SLES 11, with NConf, PNP4Nagios and NagVis. Workshop with ready-to-run Nagios VMware images for all participants.

2009-11-05

eXstor GmbH Wiesbaden

- Translation of the whole web presence into English.

2009-10-20 – 2009-10-26

Mario Größler

- OS and web server hardening. Setup of a web application firewall.
- Adjustment of the WAF rule set to various web applications.

15.09.2009 – 01.10.2009

Deutsche Bausparkasse Badenia AG Karlsruhe

- Design and test of a deployment for a hardened Apache reverse proxy.
The absolute maximum of security was required with modifications of the source code, the deployment of a web application firewall, etc.

2009-09-07

Carpe diem GmbH

- Training for Cacti, rrdtool and snmp on SLES 10.

2009-07-27

esacom GmbH

- Set-up of GPFS for a HA cluster on SLES 10.
- udev configuration for IBM tape and changer.

2009-06-22 – 2009-07-06

AVL Deutschland GmbH

- General consulting regarding Nagios and Cacti.
- Creating of special data templates and their associated data queries in Cacti for temperature and fan speed measuring.
- Programming of PHP scripts to import these snmp values into Cacti.
- The challenge here was that the snmp data was not provided in an index-based structure and could not be walked. Additionally there was the requirement that several IP addresses had to be associated with one single device in Cacti.
- Training for the Cacti plugins Discovery and Weathermap along with detailed documentation.

2009-06-10 – 2009-06-16

eXstor GmbH

- Setting up the hardware raid for an IBM xSeries 306m server.
- New installation and configuration of SLES 11.
- Manual installation of the IBM tape driver lin_tape, installation of the daemon lin_taped and the tape utilities IBMtapeutil.

2008-09-01 – 2009-06-09

www.infosecprojects.net

- I have worked on my own server and my web site including marketing and SEO. I improved my skills in Linux security.

2008-08-30 - 2008-08-31

Newline-Medien GbR

- Setup of a monitoring solution based on Cacti and Nagios on Ubuntu Linux.
- Configuration of the local Postfix mail server as relay client.

2008-07-01 - 2008-08-08

Fox Mobile Distribution GmbH (formerly known as Jamba! GmbH) Berlin

Reconfiguration of Cacti and Nagios on Debian Linux for about 300 servers.

Automatic integration of new servers into the monitoring environment.

- Basic installation of Debian Etch
- Compiling of Nagios and Cacti
- Creating and configuration of databases in MySQL
- Modification of the Debian packages of Groundwork Monitor Community Edition
- Writing of a bash script for mass importing new servers into Nagios and Cacti
- Writing of Nagios checks as bash scripts
- Modification of existing Perl Nagios checks
- Debugging of the Spine source code (C)
- Testing of existing Cacti plugins
- Writing of a Cacti plugin (just the framework, no access to the Cacti API)
- Direct queries of Cacti archives with rrdtool
- Creating of snmp requests for an Isilon-MIB of an Isilon Storage Cluster
- Writing of a detailed documentation in Confluence

2008-03-01 – 2008-03-31

Satyamitra Network

- PHP / YAML / MySQL project for the administration of audio recordings.

Permanent positions

2005-10-01 - 2007-10-30

//SEIBERT/MEDIA GmbH Wiesbaden

Linux/UNIX system administrator

Focus: web servers

Operating systems: Gentoo, FreeBSD

Daemons/Applications: Apache, Lighty, MySQL, Bind, Postfix, Qmail, Nagios, Cacti

- Setup and operation of the Nagios monitoring server
- Apache web server with several hundred domains
- Writing of mod_rewrite rules
- Relocations of web servers
- Setup of a LVS cluster with redundant load balancers
- Web server with PHP load balancing
- Installation of web software like OTRS, forums, CMS
- MySQL Master-Master replication
- Running Bind with more than 1000 domains
- Writing of scripts in Bash and Perl
- Writing of a small program in C which detects malicious processes
- Configuration of a Watchguard Firebox
- Firewalls with iptables
- Analysis of hacked servers
- Administration of SSL certificates
- Research and tests to increase the security of the servers
- Log analysis of Qmail logs
- Writing of a whitelist patch for the ra-plugin rblchecks of Qmail (C)
- Support for customers and employees
- Trainings given for SELinux and Cfengine
- Setup of DELL servers and integration in our rack in the data center
- I investigated procedures in our IT department to split them to processes
- Surveys with LimeSurvey
- Evaluation of hardware and software products
- On-call duty

01.2004 - 09.2005

1&1 Internet AG Zweibrücken

1st-Level-Support

- Support for Linux and Windows servers
- Official contact person for English customers
- Support for DSL, DSL hardware, domains und sales

Advanced training

To stay up-to-date I take part in various training courses.

2009-11-17 - 2009-11-18

IBM Deutschland Research & Development GmbH Böblingen

FCM Workshop (Flash Copy Manager)