Nagios-Spezialist !

CV

Aktualisiert: 01.02.2012

Mehr als 6 Jahre Erfahrung in verschiedenen Nagiosprojekten

Größtes Projekt: 1800 überwachte Server, verteilt und redundant

* Implementierung / Beratung
* Performance-Tuning
* Training

Persönliche Daten

Name:	**Norbert Klein**
Jahrgang:	1974
Ausbildung:	Diplom-Informatiker(FH)
Zertifizierungen:	Novell CLP/CLE 10
Fremdsprachen:	Englisch (verhandlungssicher), Französisch (fortgeschritten)
Berufserfahrung:	seit 2000

Kontakt

Webseite:	http://www.infosecprojects.net/
Email:	norbert.klein@infosecprojects.net

IT-Kenntnisse

Betriebssysteme
SLES 10, 11
openSUSE
Debian
Ubuntu

Programmiersprachen
Bash, PHP, Java
XHTML, CSS
SQL
Etwas Erfahrung mit Perl, Python, C

Produkte/Standards
Nagios, NRPE, NSClient++, NSCA, NConf, PNP4Nagios, NagVis, check_MK, MK Livestatus, Multisite, check_logfiles, check_multi, Pluginentwicklung, ...
GPFS
Apache, mod_security, mod_rewrite, mod_proxy
MySQL
Bind
Cacti, Weathermap-Plugin
iptables
Postfix
syslog-ng
Confluence
LVS/Keepalived Cluster
Snort
SELinux
OTRS
SNMP
ITIL (Grundkenntnisse)
OpenVPN

Hardware
Dell PowerEdge-Server
IBM xSeries-Server
WatchGuard Firebox

Projekte

05.09.2011 – 30.11.2011
Deutsche Telekom AG Ulm

- Applikationsbetreuung Mediencenter

08.08.2011 – 12.08.2011
Parken in Mainz GmbH (PMG) Mainz

- Erweiterung der Nagios-Umgebung mit SNMP-Checks für die digitalen Schalteingänge mehrerer Web-IOs.
- Integration der neuen Checks in NagVis.

07.03.2011 – 25.03.2011
UNION TANK Eckstein GmbH & Co. KG (UTA) Kleinostheim

- Installation und Konfiguration von Nagios zum Monitoring von Windows und Linux.
- Lokale Checks mit NRPE und NSClient++.
- Monitoring von DB2, MySQL, Windowsdiensten via WMI, Inhalt von Webseiten, Ports, downloadbaren Dateien, Prozessen, Dateisystemoperationen, Logdateien, ...
- Agentenloses Monitoring mit IBMs Application Development Client und ZenOSS' wmic.
- Plugins in Bash, Python und Java geschrieben.
- Dokumentation und Training.

2011-02-07 – 2011-02-10
Helmholtz-Zentrum für Umweltforschung GmbH (UFZ) Leipzig

- In Zusammenarbeit mit eXstor GmbH:
- Einrichtung von GPFS für ein Highperformance-Cluster (HPC) mit 86 physischen Knoten.
- GPFS Cluster-Design.
- Fileserver-Setup mit InfiniBand dual bonding und GPFS load balancing.
- Initiales Performance-Tuning.
- Betriebssysteme Red Hat Enterprise Linux und CentOS.

01.11.2010 – 10.01.2011
DB Systel GmbH Erfurt

- Konsolidierung der Dokumentation von mehreren Projekten mit Livelink.
- Ergebnis: Zentrale Dokumentation entsprechend der ITIL-Struktur der Projekte.

09.06.2010 – 18.06.2010
Parken in Mainz GmbH (PMG) Mainz

- Einrichtung einer Monitoring-Lösung für die Technik der Parkhäuser in Mainz mit Nagios, NagVis und PNP4Nagios.
- Erstellung der Dokumentation für die Anwender und Administratoren.
- Schwerpunkt hierbei war eine einfache und ansprechende grafische Darstellung der Systemzustände durch NagVis. Dafür wurden neue Iconsets erstellt und entsprechend in NagVis angeordnet, sodass man auf einen Blick den Status aller Parkhäuser sehen kann.
- Die Nagios-Konfiguration wurde so strukturiert, dass verschiedene Sichten auf die Technik der Parkhäuser in NagVis abgebildet werden konnten: Z.B. nach Standort, nach dem Typ der Technik, usw..
- Für die langfristige Protokollierung der Daten und deren grafischer Darstellung wird PNP4Nagios eingesetzt.
- Durch diese flexible Open-Source-Lösung konnten im Vergleich zu einer Lösung mit Microsoft SCOM (System Center Operations Manager) mehr als 5000€ Lizenzkosten allein für die Anschaffung eingespart werden!

02.03.2010 – 03.03.2010
Kommunales Rechenzentrum Niederrhein (KRZN) Kamp-Lintfort

- Einrichtung eines GPFS-Clusters.
- Installation von lin_taped mit Treiber und Utilities.
- Erstellung der benötigten udev-Regeln für die IBM-Tape-Devices.

29.11.2009
[Ein Webhoster]

- Programmierung eines Bash-Skriptes zur Bereinigung des Webcontents von Kunden nach einem erfolgten Hacker-Angriff.

11.11.2009 – 02.06.2010
DB Systel GmbH Erfurt

Konzeption einer über mehrere Rechenzentren verteilten, redundanten Monitoring-Architektur mit Nagios 3, NRPE, check_multi und check_logfiles für ca. 1800 Server.

Planung und Konzeption

- Ist-Analyse der bestehenden Monitoring-Umgebung durchgeführt.
- Grobkonzept zur Einführung von Nagios, NRPE, check_multi und check_logfiles mit zentraler Konfiguration erstellt.
- Konzept für ein Frontend zur Nagios-Konfiguration erstellt. Damit ist es auf einfache Weise möglich großflächige Änderungen in der Nagios-Konfiguration umzusetzen. Jede mögliche Operation kann damit auf beliebig vielen Hosts und/oder Services gleichzeitig erfolgen. Dieses Frontend dient auch als Schnittstelle zu bestehenden Systemen und generiert regelmäßig und automatisch eine aktuelle und vollständige Nagios-Konfiguration für alle beteiligten Nagiosserver. So ist das Monitoring in die Systemlandschaft integriert und die Daten bleiben aktuell.
- Globale Prozesse zum Betrieb und der Wartung der Architektur definiert.
- Thruk und MK Livestatus evaluiert.

Implementierung

- Checks des bestehenden Monitoringsystems in Nagios-Checks umgesetzt.
- Erstellung von SPEC-Dateien und RPM-Paketbau für alle beteiligten Nagios-Komponenten.
- Anbindung von Nagios an eine NetCool-Konsole per syslog-ng, logger und Bash-Skripten. Alle Checkergebnisse werden an Netcool gesendet, Synchronisation von Acknowledgements zwischen Nagios und Netcool. Heartbeat zwischen Nagios und Netcool eingerichtet.
- Verwendung von check_multi mit zentraler Konfiguration und in der Variante "Feed Passive" getestet.
- Zusätzliche Plugins als Bash-Skripte geschrieben.
- Helferskripte geschrieben für verschiedenen Operationen per external commands, die die Nagios-Weboberfläche nicht ermöglicht.
- Customizing der Nagios-Weboberfläche vorgenommen.
- Init-Skripte erstellt.
- Konfiguration verschiedener Dienste wie Postfix und Syslog/Syslog-ng durchgeführt.

Lasttests und Performance-Tuning

- Auswirkung der NSCA-Verschlüsselung auf die Performance bei einem verteiltem Setup untersucht.
- Einsatz von OCP-Daemons zur Performancesteigerung eingerichtet.
- Skript erstellt, welches die Performance für jedes Nagios-Plugin einzeln ermittelt und aufzeichnet.
- Automatisierung der Lasttests durch Bash-Skripte ermöglicht für beliebig viele Nagios-Instanzen, Hosts und Services.
- Nagios-Performancetuning, sodass mehr als 2000 Server mit insgesamt mehr als 51000 Services auf einem einzigen System mit 8 CPU-Kernen geprüft werden können. Dabei entsteht eine durchschnittliche Host- und Service-Latenz von weniger als 0,5 Sekunden bei einem Check-Intervall von 5 Minuten.

Dokumentation und Wissenstransfer

- Diagramme erstellt und Präsentationen durchgeführt.
- Ausführliche Dokumentation in Form von Word-Dokumenten und Wiki-Seiten geschrieben.

27.11.2009

Carpe diem GmbH Wiesbaden

- Training für Nagios 3 auf SLES 11 komplett, mit NConf, PNP4Nagios und NagVis. Praxisorientierter Workshop mit fertigem Nagios-VMware-Image für alle Teilnehmer.

05.11.2009
eXstor GmbH Wiesbaden

- Übersetzung der gesamten Webpräsenz ins Englische.

20.10.2009 – 26.10.2009
Mario Größler

- Betriebssystem- und Webserver-Härtung.
- Einrichtung einer Web-Application-Firewall.
- Anpassung des WAF-Regelsatzes an verschiedene Webanwendungen.

15.09.2009 – 01.10.2009
Deutsche Bausparkasse Badenia AG Karlsruhe

- Ausarbeitung und Test eines Deployments für einen gehärteten Apache-Reverse-Proxy. Hierbei ging es um das absolute Maximum an Absicherung was technisch machbar ist, mit Änderungen am Source-Code, Einsatz einer Web-Application-Firewall u.a..

07.09.2009
Carpe diem GmbH Wiesbaden

- Cacti-Training komplett, auf SLES 10.
  Inklusive Training für rrdtool und snmp.

27.07.2009
esacom GmbH Salzkotten

- Einrichtung von GPFS für ein HA-Cluster auf SLES 10.
- udev-Konfiguration für IBM-Tape und -Changer.

22.06.2009 – 06.07.2009
AVL Deutschland GmbH Mainz-Kastel

- Allgemeine Beratung zum Monitoring mit Nagios und Cacti.
- Erstellung von speziellen Data-Templates und den zugehörigen Data-Queries in Cacti zur Temperatur- und Lüfterdrehzahlmessung.
- Programmierung von snmp-Abfrage-Skripten in PHP zum Einlesen dieser Daten in Cacti. Die besondere Herausforderung hierbei war, dass die snmp-Daten nicht indexbasiert zur Verfügung standen bzw. nicht walkbar waren und mehrere IP-Adressen einem Host zugeordnet werden mussten.
- Schulung zu den Cacti-Plugins Discovery und Weathermap mit ausführlicher Dokumentation.

10.06.2009 – 16.06.2009
eXstor GmbH Wiesbaden

- Einrichtung des Hardware-Raids auf einem IBM-xSeries-306m-Server.
- Neuinstallation und Basiskonfiguration von SLES 11.
- Manuelle Installation des IBM-Tape-Treibers lin_tape, sowie Installation des Dämons lin_taped und der Tape-Utilities IBMtapeutil.

01.09.2008 – 09.06.2009
www.infosecprojects.net Wiesbaden

- Arbeiten an meinem eigenen Server, an meiner Webseite, Tutorials geschrieben, Marketing, SEO und Fortbildung im Bereich Security.

30.8.2008 - 31.8.2008
Newline-Medien GbR

- Einrichtung der Monitoring-Umgebung mit Cacti und Nagios auf Ubuntu-Linux.
- Konfiguration des lokalen Postfix-Mailservers als Relayclient.

01.07.2008 - 08.08.2008
Fox Mobile Distribution GmbH (früher Jamba! GmbH) Berlin

Neukonfiguration von Cacti und Nagios 3 auf Debian-Linux zur Überwachung von ca. 300 Servern.

Automatisierung der Aufnahme neuer Server in das Monitoring.

- Basisinstallation von Debian Etch
- Compilierung von Nagios und Cacti
- Einrichtung und Konfiguration von Datenbanken auf MySQL
- Manueller Umbau der Debianpakete von Groundwork Monitor Community Edition
- Nagios- und Cactimassenimporter als Bashskript geschrieben
- Nagioschecks als Bashscript geschrieben
- Einige Nagioschecks, die in Perl vorlagen, umgeschrieben
- Spine-Sourcecode (C) debugt und für bessere Testmöglichkeiten erweitert
- Bestehende Cacti-Plugins getestet
- Cacti-Plugin geschrieben (nur das Rahmenwerk, ohne Zugriff auf die Cacti-API)
- Direkte Zugriffe auf die Cactiarchivdateien mit rrdtool, um Fehler aufzuspüren
- snmp-Abfragen erstellt, u.a. auf die Isilon-MIB eines Isilon Storage Clusters
- Ausführliche Dokumentation mit Confluence

01.03.2008 – 31.03.2008
Satyamitra Network Wiesbaden

- PHP / YAML / MySQL-Projekt zur Verwaltung von Audioaufnahmen.

Tätigkeiten aus Festanstellung

10.2005 - 10.2007
//SEIBERT/MEDIA GmbH Wiesbaden
Linux/UNIX-Systemadministrator

Schwerpunkt Webserver
Betriebssysteme: Gentoo, FreeBSD
Dienste: Apache, Lighty, MySQL, Bind, Postfix, Qmail, Nagios, Cacti

- Einrichtung und Betrieb des Nagios-Servers
- Apachebetrieb mit mehreren 100 Domains
- mod_rewrite-Rules geschrieben
- Webserverumzüge durchgeführt
- LVS-Cluster mit redundanten Loadbalancern eingerichtet
- Webserver mit PHP-Loadbalancing eingerichtet
- Websoftware installiert wie OTRS, Foren, CMS-Systeme
- MySQL Master-Master-Replikation eingerichtet
- Bindbetrieb mit mehr als 1000 Domains
- Shell- und Perl-Skripte geschrieben
- C-Programm für FreeBSD zur Aufspürung von unerlaubt gestarteten Prozessen geschrieben
- Änderungen an der Konfiguration einer Watchguard Firebox durchgeführt
- Firewalls mit iptables eingerichtet
- Analyse von kompromitierten Servern

- SSL-Zertifikatsverwaltung
- Proaktive Forschung/Tests zur Erhöhung der IT-Sicherheit
- Mail-Loganalysen für Qmail
- Whitelist-Patch für das ra-plugin rblchecks für Qmail geschrieben (C)
- Kunden- und Mitarbeitersupport
- Schulung für SELinux, mod_security und Cfengine durchgeführt
- Dell-Server eingerichtet und im Rechenzentrum in Frankfurt eingebaut
- IT-Vorgänge in Prozesse gegliedert und dokumentiert
- Erstellung und Durchführung von Mitarbeiterumfragen mit LimeSurvey
- Hardware-/Software-Produkte evaluiert
- Rufbereitschaft

01.2004 - 09.2005
1&1 Internet AG Zweibrücken
1st-Level-Support

- Support für Linux- und Windowsserver
- Offizieller Ansprechpartner für englischsprachige Serverkunden
- Support für DSL, DSL-Hardware, Domains und Sales