CHEMNITZER LINUX-TAG 2004

Landeskriminalamt Thüringen

NAGIOS - WACHSAMER SCHUTZHEILIGER IM NETZ

Alexander Schreiber

als@thangorodrim.de

Chemnitz, den 7. März 2004

Inhalt

- Übersicht & Name,
- Struktur Nagios,
- Web-Interface,
- Überwachung,
- HA- & hierarchisches Monitoring,
- weitere Tools,
- Ausblick,
- Q & A

Wozu Monitoring?

- Überblick über Zustand von Diensten, Systemen und Netz,
- rechtzeitige Information über Probleme,
- Vereinfachung der Fehlersuche im Problemfall („XYZ ist down“),
- Entlastung des Adminteams (keine manuelle Überwachung),
- Erkennung von Trends

Was ist Nagios?

- System-, Service- und Netzwerkmonitoringtool,
- Plugin-basierte Architektur,
- leistungsfähiges und flexibles Benachrichtigungssystem,
- Webinterface für Zustandsinformationen, Logs und Reports,
- Open Source (GPL v2),
- entwickelt für Linux, aber generell UNIX-tauglich
- beliebige Plattformen überwachbar,
- Autor: Ethan Galstad <nagios@nagios.org>
- Website: http://www.nagios.org/

Zum Namen

Nagios®

- ursprünglicher Name NetSaint (1999-2002),
- Namenskollision mit Security-Scanner Netsaint,
- mit neuem Namen „Nagios“ 2002 als Nagios 1.0b6,
- **Nagios**: network + hagios (griech. „heilig“)
- Name und Logo als Markenzeichen des Autors Ethan Galstad geschützt

Strukur von Nagios - Übersicht

- Nagios = Framework,
- zentrale Instanz: nagios-Daemon,
- persistente Datenhaltung,
- Plugin-System,
- externe Datenquellen,
- Benachrichtigungssystem,
- Web-Interface

Struktur: nagios-Daemon

- prüft Zustand zu überwachender Objekte:
  - überwacht Hosterreichbarkeit (`ping`),
  - startet Plugins,
  - verarbeitet Plugin-Ergebnisse,
  - verarbeitet angelieferte externe Daten,
- bildet Gesamtzustandsinformation,
- versendet Nachrichten,
- ergreift (optional) Maßnahmen

Struktur: persistente Datenhaltung

- Konfiguration: Textdateien,
- Speicherung der Zustandsdaten:
  - Datenbank PostgreSQL/MySQL
  - Textdateien
  - Empfehlung: Textdateien, da Bugs in Datenbankinterface,
- ausführliche Logdatei (Statusmeldungen, Benachrichtigungen, ...), wird automatisch rotiert

Struktur: Plugin-System

- Nagios selbst enthält keine Servicechecks,
- Servicechecks als Plugins,
- Package: `nagios-plugins`
- Plugin-Interface:
  - Plugin = aufrufbares Executable (Binary/Script) mit Parametern,
  - Zustandsmeldung über Exitcodes (ok/warn/error/fail) und kurze, einzeilige Textmeldung (z.B. `404 - not found`),
- Plugin-System sehr einfach erweiterbar!

Struktur: Externe Datenquellen

- extern angelieferte Daten = „passive service checks“
- nagios-Daemon liest Meldungen in Textformat aus named pipe,
- Anlieferung externer Meldungen entweder lokal oder via Netz,
- Eingliederung anderer Datenquellen (Monitoringsysteme),
- Daten nicht direkt überwachbarer Systeme (z.B. hinter Firewall) einbinden

Struktur: Benachrichtigungssystem

- Benachrichtigungen bei Ausfall und Wiederverfügbarkeit,
- via EMail, SMS, Pager, Instant Messaging, ...
- Kontakte werden zu Kontaktgruppen zusammengefasst,
- Wiederholung der Benachrichtigung ...
- sehr fein granular konfigurierbar:
  - pro Host,
  - pro Service,
  - pro Kontakt,
  - nach Zeit (z.B. nur Mail an Admins zur Arbeitszeit)

Struktur: Web-Interface 1/2

- Übersichten über aktuelle Zustände,
- Zustände farbkodiert: grün/gelb/rot/orange für ok/Warnung/kritisch/unbekannt,
- verschiedene Gliederungen,
- Zugriff auf Logs und Reports,
- durchgehend gut verlinkt

Struktur: Web-Interface 2/2

- zwei Betriebsmodi: authentisiert und nicht-authentisiert,
- authentisiert:
  - Anmeldung: Nutzer & Passwort,
  - Steuerung des Nagios-Daemons,
  - Eintragen von Downtimes, Bestätigen von Problemen,
  - Kommentare, Teile der Laufzeitkonfiguration ändern,
  - feine Abstufung der Rechte pro Nutzer,
- nicht-authentisiert: keine Eingriffe möglich

Überwachung von UNIX

- zahlreiche Plugins für lokale Überwachung (Disk, Prozesse, ...),
- SNMP,
- `nagios_statd`: Disk, CPU, Prozesse, Speicher, ...,
- NRPE (Nagios Plugin Remote Executor): Remote Ausführung von Nagios-Plugins, SSL,
- NSCA (Nagios Service Check Acceptor): läuft auf Nagios-Server, nimmt Meldungen von remote an,
- Zugriff auf Standard-Schnittstellen via Netz & Plugin (sysstat, ...)

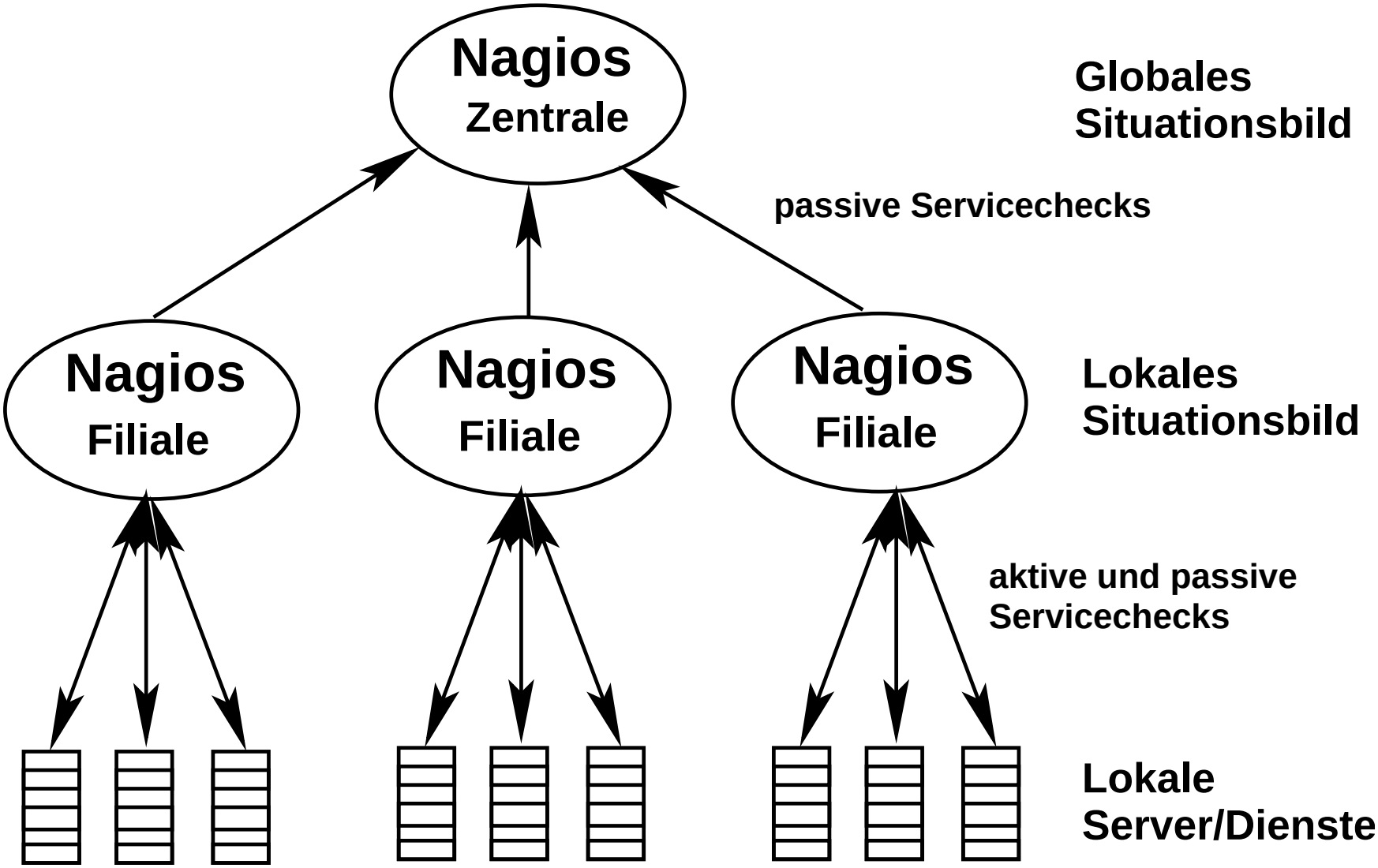
Überwachung Netzdienste

- Erreichbarkeit (`ping`),
- Plugins für SSH, HTTP(S), IRC, NTP, RPC, ...
- generische TCP und UDP Plugins,
- Datenbanken (MySQL, PostgreSQL, Oracle),
- SNMP

Überwachung von Windows

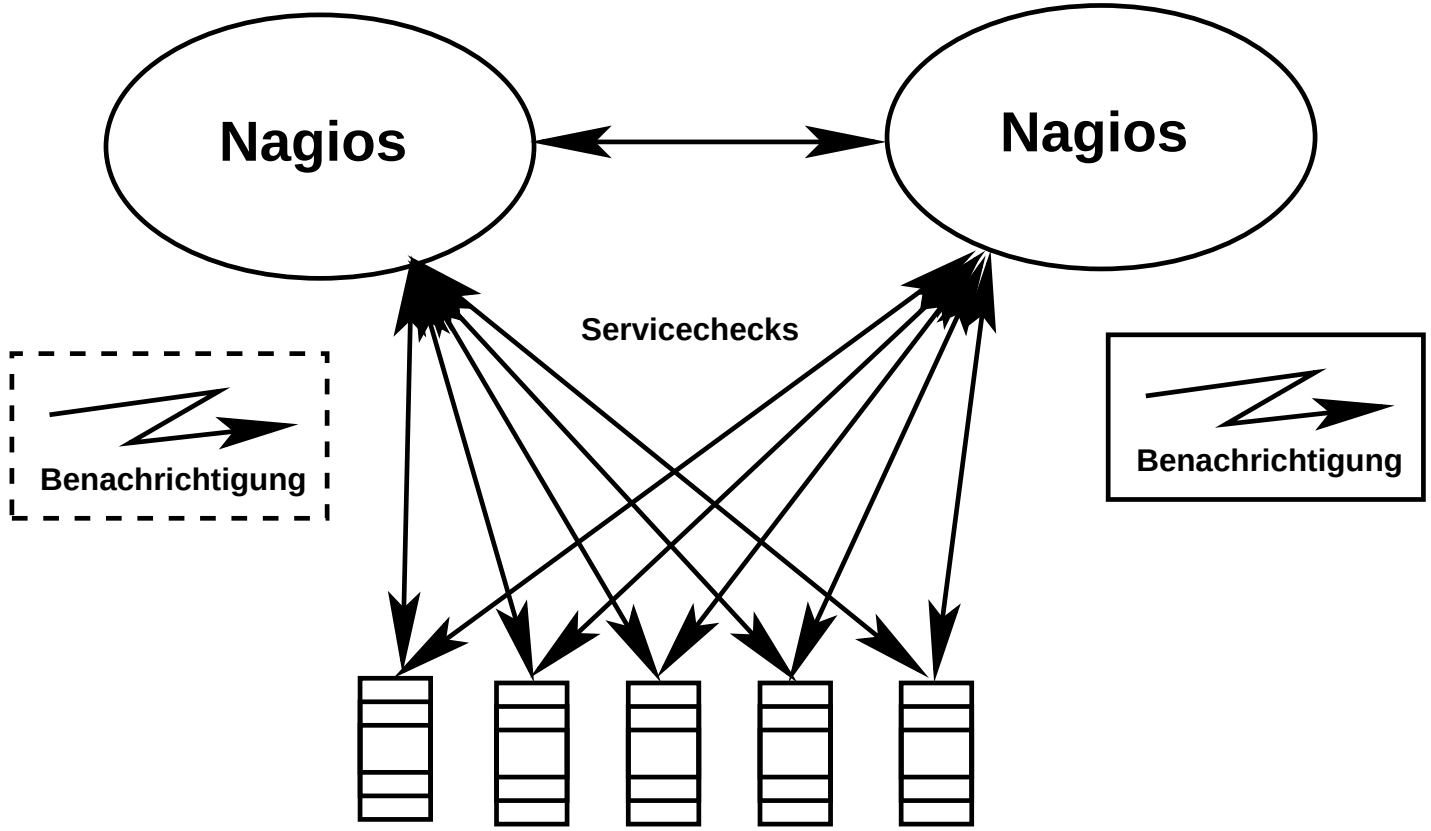
- SNMP,
- NSClient:
  - Serviceprozess auf Windows NT/2000/XP,
  - via Netz abfragbar,
  - Disk, CPU, Speicher, Services, Prozesse, Performancecounter,
- nrpe_nt:
  - Serviceprozess auf Windows,
  - Remote-Ausführung von Nagios-Plugins,

Hierarchisches Monitoring



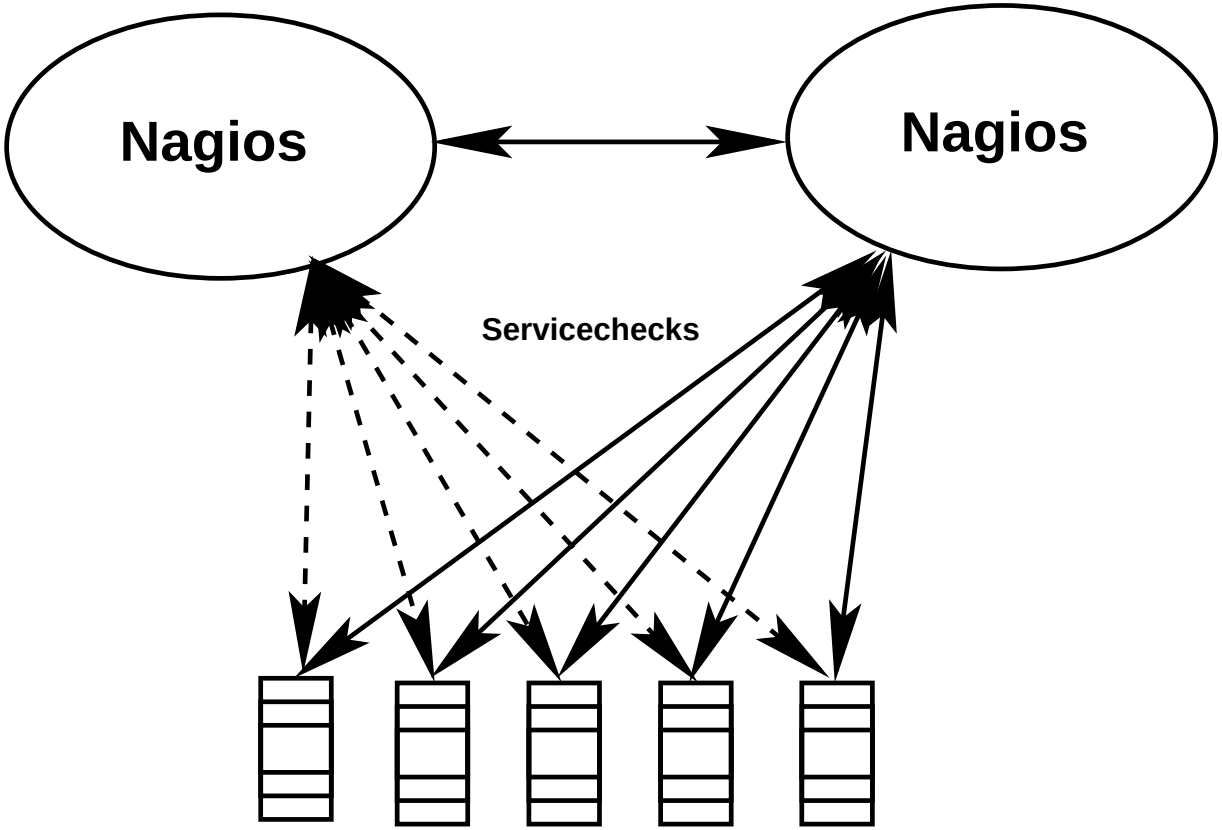
Hochverfügbares Monitoring 1/2

- Absicherung gegen Ausfall des Monitoringsystems/-servers,
- Variante 1: redundantes Monitoring



Hochverfügbares Monitoring 2/2

- Absicherung gegen Ausfall des Monitoringsystems/-servers,
- Variante 2: failover Monitoring



Zusatzsoftware

- zahlreiche Projekte um Nagios herum,
- Sensoren, Konfiguration, Auswertung, Anzeige,
- http://www.nagios.org/download/extras.php

Konfigurationshilfen

- Konfigurationsdateien recht umfangreich,
- mit vielen Hosts & Services schwer manuell wartbar,
- verschiedene Tools:
  - Nagat (Web): http://nagat.sourceforge.net/
  - NaWui (Web): http://sourceforge.net/projects/nawui/
  - NagMIN (WebAdmin): http://nagmin.sourceforge.net/
  - mkncf: http://www.thangorodrim.de/software/mkncf/

Ausblick: Nagios 2.0

- Schnittstelle zum direkten Zugriff auf interne Zustandsinformationen
- zahlreiche Detailverbesserung, „Modellpflege“,
- u.a. Änderungen im Konfigurationsformat,
- passive Hostchecks, Servicegruppen,
- Software praktisch fertig,
- Dokumentation fehlt noch
- Releasetermin mehrfach verschoben, derzeit „Sometime in 2004 . . . “

Q & A

Vielen Dank für Ihre Aufmerksamkeit!