

# 1 Kunde

Nine Internet Solutions AG  
Albisriederstrasse 243a, 8047 Zürich

Ansprechpartner:  
Samuel Sieg, samuel.sieg@nine.ch, +41 44 637 40 18

## 2 Thema

Orchestrierung von Security-Updates für Linux-Serversysteme

## 3 Beschreibung

### 3.1 Ausgangslage

nine.ch betreibt über 1500 Linux-Serversysteme. Die Installation von Software-Komponenten geschieht dabei über herkömmliche Debian-Pakete. Für diese Pakete werden regelmässig (mehrmals pro Woche) Sicherheitsupdates veröffentlicht, welche zeitnah auf sämtlichen Serversystemen installiert werden müssen.

Aktuell wird dies mit einer Sammlung einfacher Bash-Scripts bewerkstelligt. Diese sind jedoch nicht optimiert und nicht performant genug. Das Einspielen von Sicherheitsupdates verursacht jede Woche viele Stunden Aufwand.

### 3.2 Ziele der Arbeit und Liefergegenstände

Das Einspielen von Sicherheitsupdates ist weitestgehend automatisiert. Dabei sind zum Beispiel folgende Konstellationen zu berücksichtigen:

- Abhängigkeiten von Systemen (z.B. High Availability Cluster, Load-Balancer)
- Updates für wichtige Services, welche nicht einfach neu gestartet werden dürfen (z.B. Datenbankserver)
- Neustarts von Systemen nach bestimmten Updates (z.B. Kernel-Updates)

Das Lieferobjekt der Arbeit ist eine Software-Lösung, die das Einspielen der Sicherheitsupdates auf diesen Serversystemen kontrolliert. Die Software bietet dem Systemadministrator die Möglichkeit zu kontrollieren, auf welchen Systemen (oder Systemgruppen) ein Update durchgeführt wird, berücksichtigt dabei die gegenseitigen Abhängigkeiten und stellt sicher, dass gegebene Regeln nicht verletzt werden. Die Software zeigt darüber hinaus den aktuellen Zustand der Systeme, d.h. sie zeigt, welche Updates ausstehend sind und welche Updates erfolgreich bzw. fehlerhaft ausgeführt wurden.

Folgende nicht-funktionale Anforderungen sind besonders wichtig:

- Zuverlässigkeit: Die Software hat jederzeit einen korrekten und konsistenten Datenstand. Die verschiedenen Szenarien sind mit Software-Tests geprüft.
- Benutzbarkeit: Die Software ist für den Benutzer einfach zu bedienen und verständlich. Die Vorgänge sind nachvollziehbar.

## 4 Art der Arbeit

Der Kern der Aufgabe ist es, ein Reporting der anstehende Updates zu generieren und die Ausführung der Updates zu koordinieren. Es ist zu überlegen, wie die Informationen zwischen den Systemen ausgetauscht werden, damit die Aufgabe zeitnah und effektiv ausgeführt werden kann. Zu berücksichtigen sind hier vor allem auch die Abhängigkeiten der verteilten Systeme untereinander.

Eine wichtige Komponente stellt der zentrale Controller dar, der dem Administrator erlaubt, Regeln für die Updates, Gruppen und einzelne Systeme zu definieren.

Die eigentliche Software-Verteilung und -Installation übernimmt das bewährte Debian-Tool apt. Es existiert eine API, um die anstehenden Updates auszulesen und die Updates anzustossen, d.h. die Steuerung der Softwareinstallation wird nicht neu umgesetzt.

## 5 Rahmenbedingungen

### 5.1 Technische Vorgaben

Folgende technische Vorgaben sind zu berücksichtigen:

- Als Betriebssysteme werden aktuell ausschliesslich Debian (Version 6.0) und Ubuntu (Versionen 12.04 und 14.04) verwendet
- Als Programmiersprache muss wenn möglich Ruby verwendet werden. Für systemnahe Komponenten (z.B. Agents) kann alternativ auch Python oder Go eingesetzt werden
- Als Datenbankserver muss PostgreSQL verwendet werden

### 5.2 Infrastruktur

Falls benötigt, kann nine.ch für Entwicklungs- und Testzwecke virtuelle Server zur Verfügung stellen.

### 5.3 Sonstige Hinweise

nine.ch beabsichtigt, die im Rahmen dieser Arbeit entwickelte Software weiterzuentwickeln und diese nach Möglichkeit zusammen mit den Studenten als Open-Source-Software zu veröffentlichen. Aus diesem Grund räumen die Studenten nine.ch ein unentgeltliches, unwiderrufliches, nicht-exklusives, übertragbares Nutzungsrecht an allen im Rahmen dieser Arbeit entstandenen urheberrechtlich geschützten Werken (insbesondere Software) ein.