Serverdokumentation
Projekt: DigitalSchoolNotes

Projektgruppe: Adler, Brinnich, Hohenwarter, Karic, Stedronsky

Version 1.0 **21.09.2015** **Status: [RELEASE]**

	Datum	**Name**	**Unterschrift**
Erstellt	09.09.2015	Niklas Hohenwarter	
Geprüft	21.09.2015	Selina Brinnich	
Freigegeben			

Git-Pfad: /doc/serverdokumentation **Dokument:** serverdoc.tex

Inhaltsverzeichnis

1 Changelog

Version	Datum	Status	Bearbeiter	Kommentar
0.1	09.09.2015	Erstellt	Hohenwarter	Draft
0.2	21.09.2015	Bearbeitet	Hohenwarter	Alles verbessert
1.0	21.09.2015	QA	Brinnich	Rechtschreibung

2 Hosting

Unser Projektserver ist beim in Deutschland ansässigen Unternehmen Netcup[1] gehostet. Hier haben wir den Root-Server M angemietet(2 Cores Intel®Xeon® E5-26xxV3 (min. 2,3 GHz je Kern), 6 GB DDR4(ECC),120GB SSD, 1 GBit/s)[2]. Dieser ist unter der IP Adresse **37.120.161.195** erreichbar.

Auf den Server ist die Domain digitalschoolnotes.com geschaltet. Diese ist ebenfalls bei netcup gemietet.

Folgende Subdomains existieren:

- time.digitalschoolnotes.com Zeitaufzeichnung
- git.digitalschoolnotes.com Repository
- ontime.digitalschoolnotes.com Scrum Tool
- ci.digitalschoolnotes.com CI Tool

3 User

Jedes Projektteam Mitglied hat einen eigenen Unix Account auf dem Projektserver. Der Vorname der Person ist der Benutzername. Das Benutzerpasswort ist von jedem Teammitglied selbst gewählt. Alle Teammitglieder haben sudo rechte. Verantwortlich für die Serververwaltung ist Niklas Hohenwarter. Bei Problemen mit der Anmeldung oder anderem sind diese ihm bekannt zu geben.

4 Mailsystem

Das Projektteam hat einen Email-Verteiler mit der Adresse info@digitalschoolnotes.com. Jedes Teammitglied hat eine E-Mail Adresse nach dem Schema des TGMs. Der Scrummaster ist unter scrummaster@digitalschoolnotes.com erreichbar.

5 SSH

Aus Sicherheitsgründen wurde die Anmeldung mit Passwort verboten und es können hierfür nurnoch SSH Keys verwendet werden.

6 Firewall

Es werden prinzipiell alle eingehenden Ports geschlossen. Ausnahmen sind hier aufzulisten. Bei Änderungswünschen ist der Serveradministrator zu kontaktieren.

Ausnahmen:

- 22 SSH
- 53 DNS
- 80 HTTP
- 443 HTTPS

6.1 Konfiguration

Die Firewall wird mittels folgenden Befehlen aufgesetzt:

```
# Flush the tables to apply changes
iptables -F

# Default policy to drop 'everything' but our output to internet
iptables -P FORWARD DROP
iptables -P INPUT   DROP
iptables -P OUTPUT  ACCEPT

# Allow established connections (the responses to our outgoing
    traffic)
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Allow local programs that use loopback (Unix sockets)
iptables -A INPUT -s 127.0.0.0/8 -d 127.0.0.0/8 -i lo -j ACCEPT
iptables -A FORWARD -s 127.0.0.0/8 -d 127.0.0.0/8 -i lo -j
    ACCEPT

#Allowed Ports
iptables -A INPUT -p tcp --dport 22 -m state --state NEW -j
    ACCEPT
iptables -A INPUT -p tcp --dport 80 -m state --state NEW -j
    ACCEPT
iptables -A INPUT -p tcp --dport 443 -m state --state NEW -j
    ACCEPT
iptables -A INPUT -p tcp --dport 53 -m state --state NEW -j
    ACCEPT
iptables -A INPUT -p udp --dport 53 -m state --state NEW -j
    ACCEPT
```

Die Firewallrules werden beim Reboot automatisch wiederhergestellt. Dies geschieht durch das Paket ***iptables-persistent***. Konfiguration[3]:

```
# Install
sudo apt-get install iptables-persistent

# Save Rules
iptables-save > /etc/iptables/rules.v4
```

7 Bruteforce Prevention

Um den SSH Zugang gegen Brute Force Attacken abzusichern wurde fail2ban installiert. Dieses Paket versucht Bruteforce Attacken zu verhindern. [4]

7.1 Konfiguration

Das Paket wurde mittels ***sudo apt-get install fail2ban*** installiert. Die Standardkonfiguration wird verwendet.

8 Webserver

Als Webserver wird nginx verwendet. Aktuell existieren auf dem Server nur Weiterleitungen zu unserem Github Repository, Taiga, der Zeitaufzeichnung und dem CI Tool (Subdomains, siehe oben).

8.1 Konfiguration

Die Konfiguration ist in ***/etc/nginc/sites-available/redirects*** zu finden. Sie enthält folgendes:

```
server {
        listen 80; #Port
        server_name git.digitalschoolnotes.com; # Subdomain

        location / {
           rewrite ^ https://github.com/nhohenwarter-tgm/
              digitalschoolnotes permanent; # zieladresse der
              Weiterleitung
        }
}

server {
        listen 80;
        server_name ontime.digitalschoolnotes.com;

        location / {
           rewrite ^ tgm.axosoft.com permanent;
```

```
        }
}


server {
        listen 80;
        server_name time.digitalschoolnotes.com;

        location / {
           rewrite ^ https://goo.gl/IWrE2j permanent;
        }
}
```

Um die Weiterleitung zu aktivieren muss ein Link nach ***/etc/nginx/sites-enabled*** gesetzt werden. Dies geht mit dem Befehl ***ln -s /etc/nginx/sites-available/redirects /etc/nginx/sites-enabled/redirects***. Dannach muss der Nginx Service neu gestartet werden.

9 Literatur

[1] Netcup, "netcup - webhosting, vserver, servermanagement." `http://netcup.de/`. zuletzt besucht: 09.09.2015.

[2] Netcup, "netcup - webhosting, vserver, servermanagement." `https://www.netcup.de/vserver/#features`. zuletzt besucht: 09.09.2015.

[3] T. Krenn, "Iptables firewall regeln dauerhaft speichern." `https://www.thomas-krenn.com/de/wiki/Iptables_Firewall_Regeln_dauerhaft_speichern`. zuletzt besucht: 21.09.2015.

[4] T. Krenn, "Ssh login unter debian mit fail2ban absichern." `https://www.thomas-krenn.com/de/wiki/SSH_Login_unter_Debian_mit_fail2ban_absichern`. zuletzt besucht: 09.09.2015.