Serverdokumentation
Projekt: DigitalSchoolNotes

Projektgruppe: Adler, Brinnich, Hohenwarter, Karic, Stedronsky

Version 0.1 **09.09.2015** **Status: [ALPHA]**

	Datum	**Name**	**Unterschrift**
Erstellt	09.09.2015	Niklas Hohenwarter	
Geprüft			
Freigegeben			

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

Inhaltsverzeichnis

1 Changelog

Version	Datum	Status	Bearbeiter	Kommentar
0.1	09.09.2015	Erstellt	Hohenwarter	Draft

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.

3 User

Jedes Projektteam Mitglied hat einen eigenen Unix Account auf dem Projektserver. Der Vorname der Person ist der Benutzername. Eine SSH Anmeldung mit Passwort ist nicht möglich und kann nur mit SSH Key erfolgen. Das Benutzerpasswort folgt dem Schema vorname123 (z.B. adin123). 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. Dieser ist für alle Registrierungen und ähnliches zu verwenden. Alle Emails die an der oben genannte Adresse einlangen, werden an alle Teammitglieder weitergeleitet.

5 SSH

Aus Sicherheitsgründen wurde die Anmeldung mit Passwort verboten und es können hierfür nurnoch SSH Keys verwendet werden. Der SSH Port wurde auf 44 geändert.

6 Firewall

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

Ausnahmen:

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

7 Bruteforce Prevention

Um den SSH Zugang gegen Brute Force Attacken abzusichern wurde fail2ban installiert. Dieses Paket versucht Bruteforce Attacken zu verhindern. [3]

8 Dienstüberwachung

Monit ToDo

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, "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.