

Laborbericht - NVS - 5CHIF

Name: Juri Schreib

Datum: 2017-02-13

Ziel: Erfüllung der Aufgabenstellung

Software

Folgende Produkte wird auf den Servern installiert

Acadia

- OpenSSH (SSH, SFTP)
- E-Mail
 - Postfix (SMTP / MTA)
 - Dovecot (IMAP / MDA)
 - Roundcube (Webmail / MUA)
- Asterisk (VoIP)
- NGINX (Webserver)
 - NextCloud (Contacts, Calendar, File Server, Collaboration Tools, etc.)
 - Gitlab
 - Webmin (Computer Administration Front End)
- OpenVPN Server
- Für die Mittagspause
 - Grand Theft Auto San Andreas Multiplayer Server
 - Minecraft Server

Badlands

- OpenSSH (SSH, SFTP)
- LDAP (openLDAP)
- Bind (DNS Server)

Redwood

- Apache (Webserver)
 - Öffentliche Unternehmensportfolio (statische Website)
- OpenSSH (SSH, SFTP)

Der Computer wird über die Grafische Benutzeroberfläche von Uberspace verwaltet

R1

- DHCP

Alle Anwendungen (mit Ausnahm vom öffentlichen Webserver auf Rewood) werden in Docker Containern auf den Servern installiert um diese voneinander zu Isolieren und einfacher verwalten zu können. Dazu wird ein Dockerfile erstellt, welche definiert, wie

die einzelnen Container miteinander und mit der Außenwelt kommuniziert. Am physischen Server selbst wird nur Docker, openSSH (Administration) und IPTables (Firewall) installiert und nur Authentifizierungsoptionen konfiguriert.

Da Uberspace ein shared Host ist (viele Benutzer auf einem Server) ist eine ähnlich weitgehende Konfiguration nicht möglich. Es wird lediglich die Unternehmenswebseite auf Uberspace abgelegt und diese mit den vorinstallierten Werkzeugen öffentlich geschaltet.

Aufsetzen von Redwood

Info Zur Einsparung von Kosten wird ein bereits vorhandenes Uberspace-Konto für die Webseite genutzt. Als Platzhalter für die Unternehmenswebseite wird meine Private Seite genutzt.

Es wird auf Uberspace ein Konto erstellt und sich auf der Weboberfläche angemeldet

The screenshot shows the Uberspace dashboard for user BUJUHU. The header includes the Uberspace logo with the tagline 'HOSTING ON ASTEROIDS' and navigation links for 'TECHNIK', 'PREISE', 'SUPPORT', 'HAUSORDNUNG', 'BLOG', and 'MEIN UBERSPACE'. The user's name 'BUJUHU' is displayed in the center, with a welcome message: 'Willkommen zurück! Schön, dass du wieder einmal reinschaust. Können wir etwas für dich tun? Dann sag es uns – Uberspace antwortet! In der »Noch Fragen?«-Box, die wir ganz bewusst auf jeder unserer Seiten untergebracht haben, findest du unsere wichtigsten Kontaktmöglichkeiten.' Below this is a menu with items: 'WICHTIG', 'DATENBLATT', 'ZUGÄNGE', 'E-MAIL', 'DOMAINS', 'FINANZIELLES', 'WEITERSAGEN', and 'LÖSCHEN'. On the left, there is a section titled 'SICHERE DEINE DATEN!' with a warning about backups. On the right, there is a section titled 'NOCH FRAGEN?' with links to 'FAQ & Dokumentation', 'SCHREIB UNS' (mailto:hallo@uberspace.de), and 'TWITTERE MIT UNS' (twitter.com/ubernauten).

Danach wird der SSH Public Key eines Administrators im "Zugänge" Tab hinzugefügt.

ZUGANG ZUM WEBINTERFACE

... via Passwort:

Hier kannst du ein Passwort für den Web-Zugang vergeben. Ein eventuell bereits bestehendes Passwort wird dabei automatisch überschrieben.

Passwort beim Tippen anzeigen

Du kannst dir mit der Checkbox das Passwort beim Tippen zur Kontrolle im Klartext anzeigen lassen (wenn dir keiner über die Schulter schaut). Bei uns gespeichert wird es natürlich nur als Hashwert.

... via OpenID:

★ https://www.google.com/accounts/o8/id?id=AltOawl8W0hkphzreCsGpFUVoVt09fc_mSDZKVg
weg damit

Füge eine OpenID hinzu:

Wir schicken dich kurz bei deinem OpenID-Provider vorbei, damit dieser deine Identität bestätigt. Du kommst dann automatisch wieder hierher zurück.

Du hast noch keine OpenID oder möchtest eine zusätzliche? Dann findest du bei openid.net eine [Liste von OpenID-Providern](#), bei denen du dir eine besorgen kannst.

SSH-ZUGANG ZUM UBERSPACE

... via Passwort:

Hier kannst du ein Passwort für den SSH-Zugang vergeben. Ein eventuell bereits bestehendes Passwort wird dabei automatisch überschrieben.

Passwort beim Tippen anzeigen

Du kannst dir mit der Checkbox das Passwort beim Tippen zur Kontrolle im Klartext anzeigen lassen (wenn dir keiner über die Schulter schaut). Bei uns gespeichert wird es natürlich nur als Hashwert.

... via SSH-Schlüssel:

★ ssh-rsa AAAAB3NzaC...IDEy7fk20J
Bujuhu@Sakuya
weg damit

★ ssh-rsa AAAAB3NzaC...ytlKOAT4tJ bujuhu@reimu
weg damit

★ ssh-rsa AAAAB3NzaC...bnY/6uu+Bx
weg damit

Füge einen SSH-Schlüssel hinzu:

NOCH FRAGEN?

SCHAU IN UNSERE
FAQ & Dokumentation

SCHREIB UNS
hallo@uberspace.de
GNUPG-KEY B992F4EA2FE04419

TWITTERE MIT UNS
twitter.com/ubernauten

Danach verbindet sich ein Administrator über die Kommandozeile mit den Zugangsdaten, welche von Uberspace zur Verfügung gestellt wurden

```
bujuhu ~ ssh kochab.uberspace.de
Last login: Fri Feb 10 18:51:14 2017 from 80.109.104.102
[bujuhu@kochab ~]$
```

Mithilfe von Git wird die Unternehmenswebsite auf den Server geladen

```
git clone https://github.com/Bujuhu/bujuhu.at.git
```

Da auf dem Server mehrere Projekte unter verschiedenen Domains laufen, wird mithilfe einer htaccess Datei eine auf Uberspace dokumentierte Methode genutzt, mehrere pseudo-document roots zu verwenden. Dazu wird ein unterverzeichnis erstellt, das den selben namen wie die aufgerufne Domain trägt und danach folgedene Htaccess Dokumentation eingespielt

.htaccess

```
# Force Https
RewriteEngine On
RewriteCond %{HTTPS} !=on
RewriteCond %{ENV:HTTPS} !=on
RewriteRule .* https://%{SERVER_NAME}%{REQUEST_URI} [R=301,L]
```

```
# If there is a host-specific pseudo-DocumentRoot, use it instead of the default one
RewriteCond %{REQUEST_URI} !^/f?cgi-bin/
RewriteCond /var/www/virtual/bujuhu/%{HTTP_HOST} -d
RewriteRule (.*) /var/www/virtual/bujuhu/%{HTTP_HOST}$1
```

Im nächsten Schritt wird eine Domainweiterleitung eingerichtet. Zunächst wird in Uberspace mithilfe des `uberspace-add-domain` kommandos eine neue Domain hinzugefügt:

```
[bujuhu@kochab bujuhu.at]$ uberspace-add-domain -w -d kmu.schreib.at
The webserver's configuration is adapted; it will get active within at most 5 minutes.
Now you can use the following records for your dns:
  A -> 185.26.156.19
  AAAA -> 2a00:d0c0:200:0:b9:1a:9c13:6f
[bujuhu@kochab bujuhu.at]$
```

Die `-w` flag gibt an, dass die Domain dem Webserver bekannt gegeben wird.

Danach wird kontrolliert ob die Domain korrekt hinzugefügt wurde

WICHTIG **DATENBLATT** **ZUGÄNGE** **E-MAIL** **DOMAINS** **FINANZIELLES** **WEITERSAGEN** **LÖSCHEN**

WEBSERVER

Es sind folgende Domains in der Webserver-Konfiguration deines Uberspaces eingerichtet:

- ★ bujuhu.at
- ★ *.bujuhu.kochab.uberspace.de
- ★ kmu.schreib.at
- ★ schreib.at
- ★ www.bujuhu.at
- ★ www.schreib.at

Mit `uberspace-add-domain -d <domain.tld> -w` und `uberspace-del-domain -d <www.domain.tld> -w` etc. kannst du per SSH auf der Shell selbst neue Eintragungen im Webserver vornehmen.

MAILSERVER

Es sind folgende Domains in der Mailserver-Konfiguration deines Uberspaces eingerichtet:

- ★ bujuhu.at
- ★ schreib.at

Mit `uberspace-add-domain -d <domain.tld> -m` kannst du per SSH auf der Shell selbst neue Eintragungen im Mailserver vornehmen.


NOCH FRAGEN?

SCHAU IN UNSERE
FAQ & Dokumentation

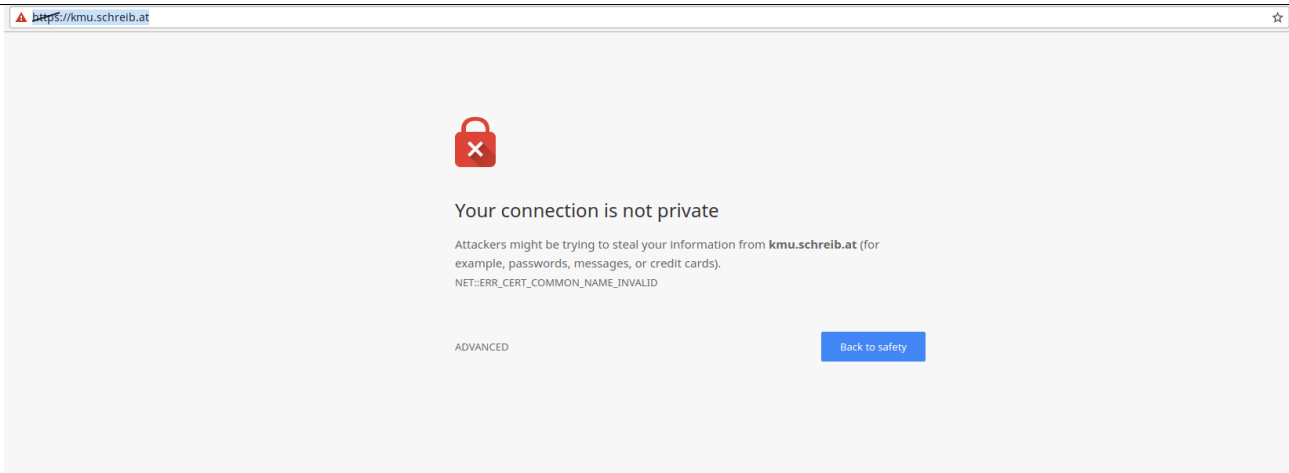
SCHREIB UNS
hallo@uberspace.de
GNUPG-KEY B992F4EA2FE04419

TWITTERE MIT UNS
twitter.com/ubernauten

Als nächstes werden neue DNS Einträge hinzugefügt, damit der Server über die neue Subdomain erreichbar ist. Dabei wird der Domainregistrar [Inwx](#) genutzt.

kmu	A	185.26.156.19	3600	 
kmu	AAAA	2a00:d0c0:200:0:b9:1a:9c13:6f	3600	 

Es wird getestet ob die Website erreichbar ist



Der Server ist bereits erreichbar, allerdings wurde noch kein gültiges Zertifikat ausgeteilt

Erstellen eines Let's Encrypt Zertifikats

Aktualisieren der Let's Encrypt Konfiguration

```
[bujuhu@kochab ~]$ cd .config/  
[bujuhu@kochab .config]$ ls  
letsencrypt  
[bujuhu@kochab .config]$ cd letsencrypt/  
[bujuhu@kochab letsencrypt]$ ls  
accounts archive cli.ini csr keys live renewal  
[bujuhu@kochab letsencrypt]$ nano cli.ini
```

cli.ini

```
rsa-key-size = 4096  
  
server = https://acme-v01.api.letsencrypt.org/directory  
  
authenticator = webroot  
  
# Don't change this without real good reasons. Our web frontend  
# uses a separate backend for answering ACME challenges which  
# *enforces* to use the default web root.  
# If you change this, things will break. You have been warned!  
webroot-path = /var/www/virtual/bujuhu/html  
  
config-dir = /home/bujuhu/.config/letsencrypt  
work-dir = /home/bujuhu/.local/share/letsencrypt/work  
logs-dir = /home/bujuhu/.local/share/letsencrypt/logs  
  
email = bujuhu@kochab.uberspace.de  
  
# Beware that Let's Encrypt does NOT support wildcard hostnames.  
# If you're using wildcards you have to add each subdomain explicitly.  
domains = bujuhu.at,schreib.at,www.bujuhu.at,www.schreib.at,kmu.schreib.at  
  
text = True
```

```
# To prevent being forced to agree manually to the terms
agree-tos = True
```

Danach wird werden neue Zertifikate mit demletsencrypt certonly kommando generiert

```
[bujuhu@kochab letsencrypt]$ letsencrypt certonly

-----
You have an existing certificate that contains a portion of the domains you
requested (ref: /home/bujuhu/.config/letsencrypt/renewal/bujuhu.at.conf)

It contains these names: bujuhu.at, schreib.at, www.bujuhu.at, www.schreib.at

You requested these names for the new certificate: bujuhu.at, schreib.at,
www.bujuhu.at, www.schreib.at, kmu.schreib.at.

Do you want to expand and replace this existing certificate with the new
certificate?

-----
(E)xpand/(C)ancel: E

IMPORTANT NOTES:
- Congratulations! Your certificate and chain have been saved at
  /home/bujuhu/.config/letsencrypt/live/bujuhu.at/fullchain.pem. Your
  cert will expire on 2017-05-14. To obtain a new or tweaked version
  of this certificate in the future, simply run certbot again. To
  non-interactively renew *all* of your certificates, run "certbot
  renew"
- If you like Certbot, please consider supporting our work by:

  Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
  Donating to EFF: https://eff.org/donate-le

[bujuhu@kochab letsencrypt]$ █
```

Das neue Zertifikat wird am Webserver mithilfe vonuberspace-add-certificate aktiviert

Es wird einige Minuten gewartet, um die Aktualisierung des Zertifikats abzuwarten

Juri Schreib

KMU Projekt Platzhalter

Die Website ist nun erreichbar.

http://localhost:4000/NVS/5CHIF_20170213_Schreib/