Übungsprotokoll

SYTB – Systemtechnik Betriebssysteme

htlkrems Bautechnik & IT	**Übungsdatum:** KW 50/2021 – KW 03/2021	**Klasse:** 3AHIT	**Name:** Felix Schneider
	Abgabedatum: 20.01.2022	**Gruppe:** SYTB_2	**Note:**
Leitung: DI (FH) Alexander MESTL	**Mitübende:** Clemens Schlipfinger		

Übungsbezeichnung:

Apache Webserver

Inhaltsverzeichnis:

1 Aufgabenstellung

Einer unserer Server (idealerweise die Maschine, die primärer DNS ist) wird nun auch noch zumindest zwei Webseiten für den Client hosten. Dazu ist folgendes zu tun:

- Webserver Apache installieren (falls noch nicht erfolgt)
- Self-signed Key und Certificate erstellen
- Webserver für "name-based virtual hosting" auf Port 443 (https://) konfigurieren
- DNS-Zonendateien anpassen, wenn erforderlich

2 Abstract (English)

Short: We have to host two websites, with SSL enrypted.

One of our servers (ideally the machine that is primary DNS) will now also host at least two web pages for the client. To do this, do the following:

- Install Apache web server (if not already done)
- Create self-signed key and certificate
- Configure web server for "name-based virtual hosting" on port 443 (https://)
- Adjust DNS zone files if necessary

3 Theoretische Grundlagen

Das Zertifikat werden wir mit SSL Verschlüsseln. SSL steht für Secure Sockets Layer.

Ein selbstsigniertes Zertifikat verschlüsselt die Kommunikation zwischen Ihrem Server und allen Clients. Da es jedoch nicht von einer der vertrauenswürdigen Zertifizierungsstellen signiert ist, die in Webbrowsern enthalten sind, können Benutzer das Zertifikat nicht verwenden, um die Identität Ihres Servers automatisch zu überprüfen.

Ein selbstsigniertes Zertifikat kann sinnvoll sein, wenn Sie keinen Domänennamen haben, der mit Ihrem Server verknüpft ist, und für Fälle, in denen eine verschlüsselte Weboberfläche nicht benutzerorientiert ist. Wenn Sie einen Domainnamen haben, ist es in vielen Fällen besser, ein CA-signiertes Zertifikat zu verwenden. Wie Sie ein kostenloses vertrauenswürdiges Zertifikat mit dem Let's Encrypt-Projekt einrichten können, erfahren Sie hier.

3.1 Quellen

https://httpd.apache.org/docs/2.4/ssl/?classId=e5503c36-5c40-4fa8-b09b-d6858d501100&assignmentId=a97fc9b8-b8a7-4d6c-b250-a362e307404c&submissionId=8c8869cd-3124-30da-9d60-f1760378b2bd

https://www.digitalocean.com/community/tutorials/how-to-create-a-self-signed-ssl-certificate-for-apache-in-debian-10?classId=e5503c36-5c40-4fa8-b09b-d6858d501100&assignmentId=a97fc9b8-b8a7-4d6c-b250-a362e307404c&submissionId=8c8869cd-3124-30da-9d60-f1760378b2bd

https://httpd.apache.org/docs/2.4/vhosts/examples.html?classId=e5503c36-5c40-4fa8-b09b-d6858d501100&assignmentId=a97fc9b8-b8a7-4d6c-b250-a362e307404c&submissionId=8c8869cd-3124-30da-9d60-f1760378b2bd

4 Übungsdurchführung

4.1 Apache installieren

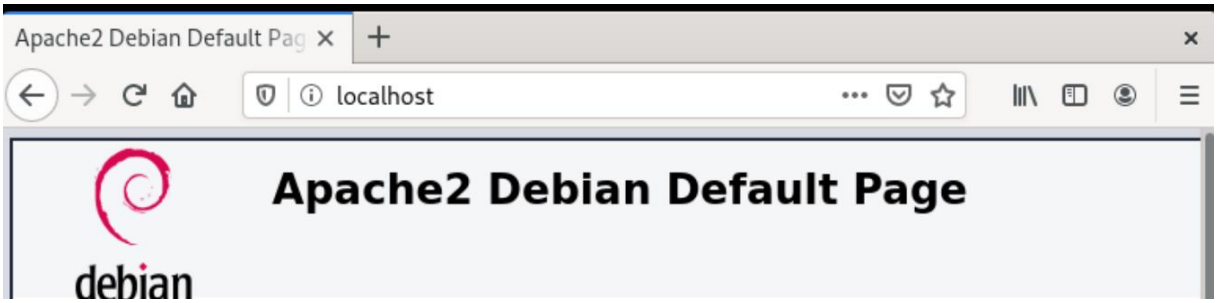
4.1.1 apt install apache2

Installieren Sie apache2.

```
root@debian:~# apt install apache2
Paketlisten werden gelesen… Fertig
Abhängigkeitsbaum wird aufgebaut… Fertig
Statusinformationen werden eingelesen… Fertig
Die folgenden zusätzlichen Pakete werden installiert:
  apache2-data apache2-utils ssl-cert
Vorgeschlagene Pakete:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Die folgenden NEUEN Pakete werden installiert:
  apache2 apache2-data apache2-utils ssl-cert
0 aktualisiert, 4 neu installiert, 0 zu entfernen und 0 nicht aktualisiert.
Es müssen 706 kB an Archiven heruntergeladen werden.
Nach dieser Operation werden 2.057 kB Plattenplatz zusätzlich benutzt.
Möchten Sie fortfahren? [J/n] j
Holen:1 http://deb.debian.org/debian bullseye/main amd64 ssl-cert all 1.1.0+nmu1
```

4.1.2 localhost erreichen

In einem Browser können Sie nun den localhost erreichen und die Apache2 Standardwebsite sehen.



4.1.3 Aufbau /etc/apache2

Dies ist der Aufbau des /etc/apache2 Verzeichnises.

```
root@debian:/etc/apache2# ls -la
insgesamt 96
drwxr-xr-x   8 root root  4096 16. Dez 12:39 .
drwxr-xr-x 121 root root 12288 16. Dez 12:39 ..
-rw-r--r--   1 root root  7224  7. Okt 19:49 apache2.conf
drwxr-xr-x   2 root root  4096 16. Dez 12:39 conf-available
drwxr-xr-x   2 root root  4096 16. Dez 12:39 conf-enabled
-rw-r--r--   1 root root  1782  8. Aug 2020  envvars
-rw-r--r--   1 root root 31063  8. Aug 2020  magic
drwxr-xr-x   2 root root 12288 16. Dez 12:39 mods-available
drwxr-xr-x   2 root root  4096 16. Dez 12:39 mods-enabled
-rw-r--r--   1 root root   320  8. Aug 2020  ports.conf
drwxr-xr-x   2 root root  4096 16. Dez 12:39 sites-available
drwxr-xr-x   2 root root  4096 16. Dez 12:39 sites-enabled
```

4.2 Websiten aufsetzen

Meine erste Website bekommt den Title Apache1 Debian Default Page und die zweite Website bekommt den Title Apache2 Debian Default Page. Dies hat nicht den Hintergedanken, dass bei der ersten Website Apache1 und bei der zweiten Apache2 verwendet wird, dies dient nur für Unterscheindungs- und Erkennungskriterien.

4.3 SSL konfigurieren

sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt

Der oben angegebene Befehl konfiguriert den Schlüssel und das Zertifikat des Servers.

```
root@debian:/etc/apache2# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyou
t /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt
Generating a RSA private key
.....................................................................+++++
.....................................................................................
.....................+++++
writing new private key to '/etc/ssl/private/apache-selfsigned.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:www.felixnet.local
Email Address []:
root@debian:/etc/apache2# cd /etc/ssl
root@debian:/etc/ssl#
```

4.4 Links erstellen oder a2ensite *filename*

4.4.1 Links erstellen

Wir verlinken auf die Datei in mods-available, die wir verwenden wollen.

```
root@debian:/etc/apache2/mods-enabled# ln -s ../mods-available/ssl.load .
```

```
root@debian:/etc/apache2/sites-enabled# ln -s ../sites-available/default-ssl.conf .
```

4.4.2 a2ensite *filename*

4.5 DNS Zonendatei konfigurieren

In der db.felixnet.local-Datei in /var/cache/bind/zones fügen wir einen neuen Eintrag unten an, der auf den Nameserver verweist.

```
  GNU nano 5.4                    db.felixnet.local
$ORIGIN .
$TTL 604800     ; 1 week
felixnet.local          IN SOA  ns.felixnet.local. debian21.felixnet.local. (
                                202111350  ; serial
                                604800     ; refresh (1 week)
                                86400      ; retry (1 day)
                                2419200    ; expire (4 weeks)
                                604800     ; minimum (1 week)
                                )
                        NS      ns.felixnet.local.
                        NS      slave.felixnet.local.
$ORIGIN felixnet.local.
$TTL 300        ; 5 minutes
debian-client           A       192.168.21.14
                        TXT     "314f63481bccfb97ef5290571d8588324b"
$TTL 604800     ; 1 week
debian21                CNAME   ns
ns                      A       192.168.21.1
slave                   A       192.168.21.2
site1                   CNAME   ns
site2                   CNAME   ns
```

4.6 Aufbau /var/www

```
root@debian:/var/www#  ls -al
insgesamt 20
drwxr-xr-x  5 root root 4096 13. Jan 12:36 .
drwxr-xr-x 12 root root 4096 16. Dez 12:39 ..
drwxr-xr-x  2 root root 4096 13. Jan 12:58 html
drwxr-xr-x  2 root root 4096 13. Jan 12:41 site1
drwxr-xr-x  2 root root 4096 13. Jan 12:53 site2
root@debian:/var/www#
```

In jeder der beiden site Verzeichnissen befindet sich eine Index.html Datei.

4.7 /etc/apache2

4.7.1 /etc/apache2/sites-available

In sites-available befinden sich 2 wichtige Kopien von default-ssl.conf. Einmal site1.conf und dann noch site2.conf. Diese Dateien sind ident, bis auf „site1“ bzw. „site2“.

```
root@debian:/etc/apache2/sites-available# ls -al
insgesamt 36
drwxr-xr-x 2 root root 4096 13. Jan 13:54 .
drwxr-xr-x 8 root root 4096 16. Dez 12:52 ..
-rw-r--r-- 1 root root 1378 13. Jan 13:43 000-default.conf
-rw-r--r-- 1 root root 6370 16. Dez 13:51 default-ssl.conf
-rw-r--r-- 1 root root 6488 13. Jan 13:45 site1.conf
-rw-r--r-- 1 root root 6487 13. Jan 13:47 site2.conf
```

VirtualHost *:80 ist für die Redirection auf den sicheren Weg (https) zuständig.

Mittels ServerAlias kann man noch einen Alias erstellen, sodass man die Website auch mit z.B.: site1 erreichen kann.

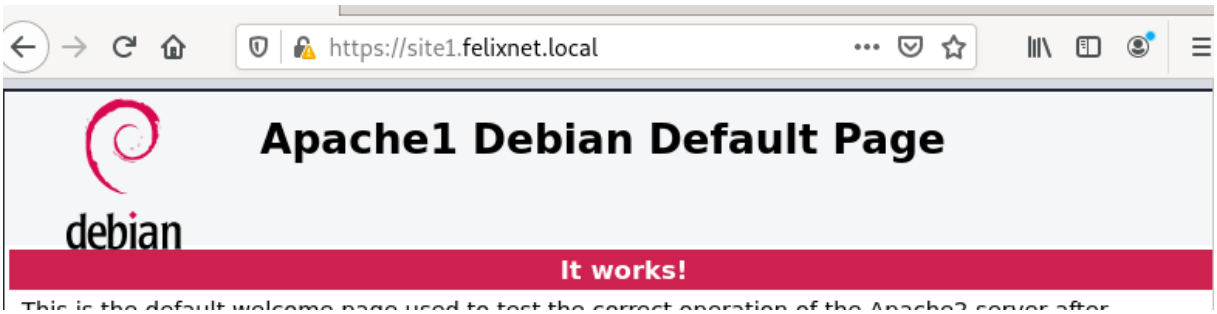
```
  GNU nano 5.4                          site1.conf *
<VirtualHost *:80>
        Servername site1.felixnet.local
        Redirect "/" "https://site1.felixnet.local/"
</VirtualHost>

<IfModule mod_ssl.c>
        <VirtualHost _default_:443>
                ServerAdmin webserver@email.com
                ServerName site1.felixnet.local

                DocumentRoot /var/www/site1

                # Available loglevels: trace8, ..., trace1, debug, info, notice, wa>
                # error, crit, alert, emerg.
                # It is also possible to configure the loglevel for particular
                # modules, e.g.
                #LogLevel info ssl:warn

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined

                # For most configuration files from conf-available/, which are
                # enabled or disabled at a global level, it is possible to
                # include a line for only one particular virtual host. For example >
                # following line enables the CGI configuration for this host only
                # after it has been globally disabled with "a2disconf".
                #Include conf-available/serve-cgi-bin.conf

                #   SSL Engine Switch:
                #   Enable/Disable SSL for this virtual host.
                SSLEngine on

                #   A self-signed (snakeoil) certificate can be created by installi>
                #   the ssl-cert package. See
                #   /usr/share/doc/apache2/README.Debian.gz for more info.
                #   If both key and certificate are stored in the same file, only t>
                #   SSLCertificateFile directive is needed.
                SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt
                SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

                #   Server Certificate Chain:
```

4.7.2 /etc/apache2/sites-enabled

In sites-enabled befinden sich 2 Links (site1.conf & site2.conf), die auf die jeweiligen Dateien in /sites-available verweisen.

```
root@debian:/etc/apache2/sites-enabled# ls -al
insgesamt 8
drwxr-xr-x 2 root root 4096 13. Jan 13:29 .
drwxr-xr-x 8 root root 4096 16. Dez 12:52 ..
lrwxrwxrwx 1 root root   35 16. Dez 12:39 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root   35 16. Dez 13:53 default-ssl.conf -> ../sites-available/default-ssl.conf
lrwxrwxrwx 1 root root   29 13. Jan 13:25 site1.conf -> ../sites-available/site1.conf
lrwxrwxrwx 1 root root   29 13. Jan 13:29 site2.conf -> ../sites-available/site2.conf
```

4.8 Test Client



5 Ergebnisse

Der Apache2 Webserver enthält 2 Websiten, die einwandfrei funktionieren.

6 Kommentar

Im Nachhinein ist die Ordnerstruktur und die Konfiguration der Webseiten logisch…