

Laborbericht - NVS - 5CHIF

Name: Juri Schreib

Datum: 2017-04-03

Ziel: Erfüllung der Aufgabenstellung

Projektdokumentation

Zeitaufwand zur Erfüllung der einzelnen Komponenten

- Netzwerkplanung und Konfiguration (4h)
- Auswahl der Softwarelösungen, definieren der Anforderungen (1h)
- Aufsetzen des Teamspeak servers (1h)
- Aufsetzen des öffentlichen Webservers (kmu.schreib.at) (3h)
- Aufsetzen von OpenLDAP und phpldapadmin auf Badlands (2h)
- Basiskonfiguration von Acadia (NGINX, Webmin) (2h)
- Aufsetzen von Sandstorm mit anbindung an OpenLDAP (1h)
- Aufsetzen von Nextcloud mit anbindung an OpenLDAP (2h)
- Aufsetzen des E-Mails servers inklusive Roundcube mit anbindung an OpenLDAP (8h)
- Dokumentation (5h)

Gesamter Zeitaufwand für das Projekt: 30h

Technische Dokumentation

Hinweis Die Technische Dokumentation ist nur eine gekürzte Fassung der Laborberichte.

KMU 1 Netzwerkplanung

Netze

ID	Name	Network Address	Subnet
1	Management	10.0.0.0	255.255.255.0
10	DMZ	10.0.10.0	255.255.255.0
20	Intranet	10.0.20.0	255.255.255.0
30	VOIP	10.0.30.0	255.255.255.0
40	Staff	10.0.40.0	255.255.255.0
50	Guest	10.0.50.0	255.255.255.0

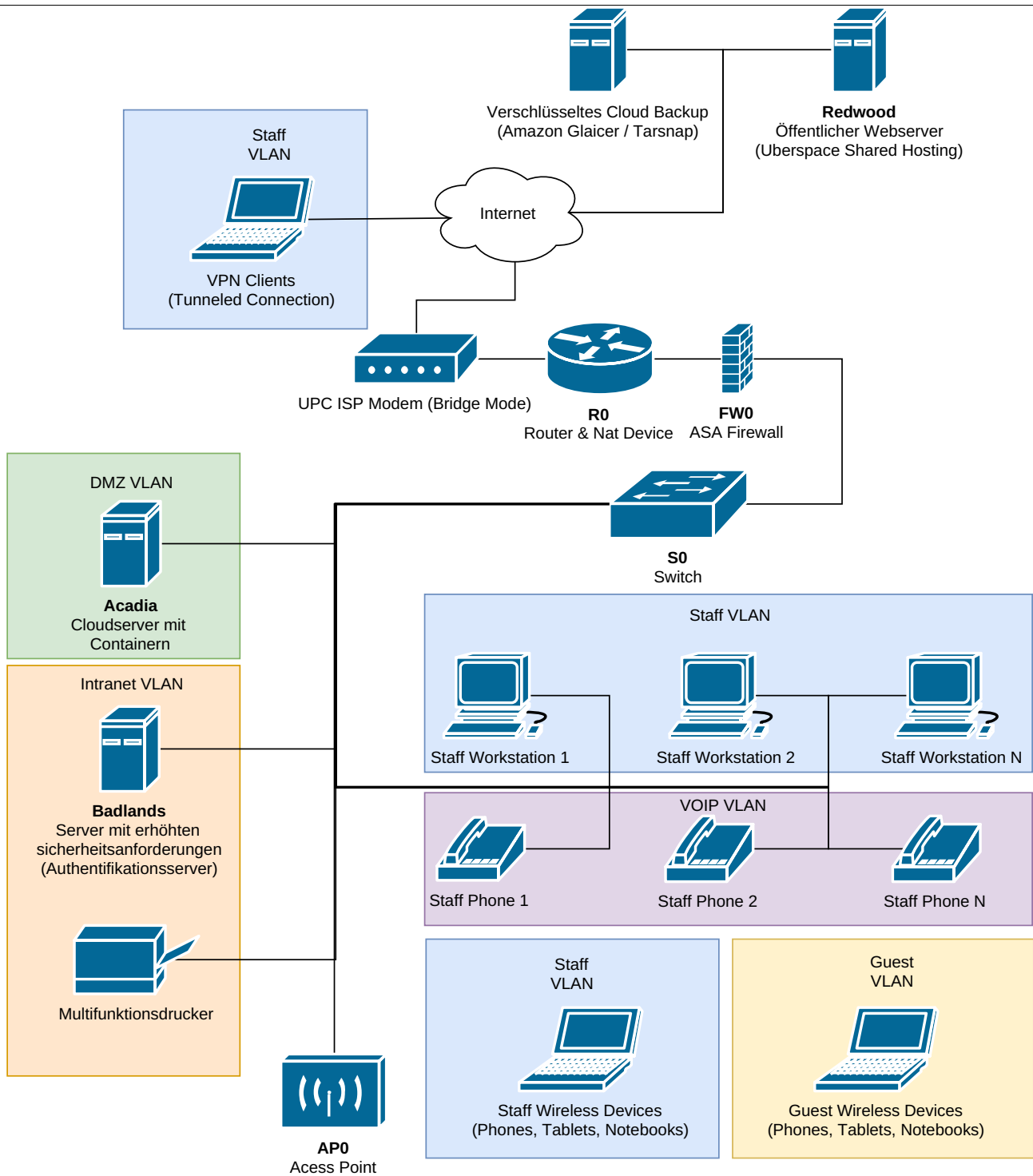
Netzwerkgeräte

Server und Netzwerkgeräte

Hostname	IP	VLAN	Gateway	DNS
R0	<i>ISP provided Public IP</i>	-	-	<i>ISP Provided DNS Server</i>
	10.0.0.1	1	-	-
	10.0.10.1	10	-	-
	10.0.20.1	20	-	-
	10.0.30.1	30	-	-
	10.0.40.1	40	-	-
	10.0.50.1	50	-	-
	10.0.50.1	60	-	-
FW0	10.0.0.2	1	10.0.0.1	10.0.0.1
SW0	10.0.0.3	1	10.0.0.1	10.0.0.1
AP0	10.0.0.4	1	10.0.0.4	10.0.0.4
Acadia	10.0.10.2	10	10.0.10.1	10.0.10.1
Badlands	10.0.20.2	20	10.0.20.1	10.0.20.1
Drucker	10.0.20.100	20	10.0.20.1	10.0.20.1
Redwood	<i>Hoster provided Public IP</i>	-	-	<i>Hoster provided public DNS Server</i>
Cloud Backup	<i>N/A</i>	-	-	-

Endnutzengeräte

Hostname	IP	VLAN	Gateway	DNS
Staff Phone	<i>(DHCP)</i> 10.0.30.2 - 10.0.30.254	30	10.0.30.1	10.0.30.1
Staff Workstations, VPN Clients & Staff wireless Devices	<i>(DHCP)</i> 10.0.40.2 - 10.0.40.254	40	10.0.40.1	10.0.40.1
Guest Wireless Devices	<i>(DHCP)</i> 10.0.50.2 - 10.0.50.254	50	10.0.50.1	10.0.50.1



Betriebssystemauswahl

Zu beginn werden nur 2 Betriebssysteme verwendet

Ubuntu (Serverbetriebssystem)

Auf allen Unternehmensservern wird Ubuntu 16.04 LTS installiert. Folgende Eigenschaften begünstigen die Verwendung von Ubuntu gegenüber anderen Betriebssystemen

- Lange Updatecyclen (nur sicherheitsaktualisierungen werden sofort zur verfügung gestellt)
- Aufwändiger Produkttestcyclus
- Hohe kompatibilität mit anderer Software
- Minimales Betriebssystem mit wenig vorinstallierten überflüssigen Werkzeugen

- Hohe performance
- Kostenfrei
- Linux basierend und somit leicht ins Unternehmen eingleiderbar

Linux Mint (Endnutzerbetriebssystem)

Linux Mint in Version 18.1 64bit in der Cinnamon Variante wird auf allen Desktop Unternehmensgeräten vorinstalliert. Durch folgende Eigenschaften hebt sich Linux Mint von den Konkurrenzprodukten ab:

- Einfache, an Windows angelehnte Grafische Benutzeroberfläche
- Am häufigsten genutztes Desktop Betriebssystem
- Meisten wichtigen Werkzeuge sind bereits vorinstalliert
- Kostenfrei
- Linux basierend und somit leicht ins Unternehmen eingleiderbar

Sollten Mitarbeiter ein anderes Betriebssystem zur Arbeit bevorzugen, ist ihnen erlaubt ihr eigenes Gerät zur Arbeit mitzunehmen und im Unternehmenswlan oder über VPN zu nutzen. Allerdings wird dieses Gerät nicht von der Unternehmens-Systemadministration verwaltet.

Sprich, der Mitarbeiter ist selbst dafür verantwortlich, sein Gerät sicher und aktuell zu halten, sowie die Unternehmensdaten zu schützen.

Software

Folgende Produkte wird auf den Servern installiert

Acadia

- OpenSSH (SSH, SFTP)
- E-Mail
 - Postfix (SMTP / MTA)
 - Dovecot (IMAP / MDA)
 - Roundcube (Webmail / MUA)
- Teamspeak (VoIP)
- NGINX (Webserver)
 - NextCloud (Contacts, Calendar, File Server, Collaboration Tools, etc.)
 - Gitlab
 - Webmin (Computer Administration Front End)
- Sandstorm

Badlands

- OpenSSH (SSH, SFTP)
- LDAP (openLDAP)
- phpldapadmin

Redwood

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

Der Computer wird über die Grafische Benutzeroberfläche von Uberspace verwaltet

R1

- DHCP

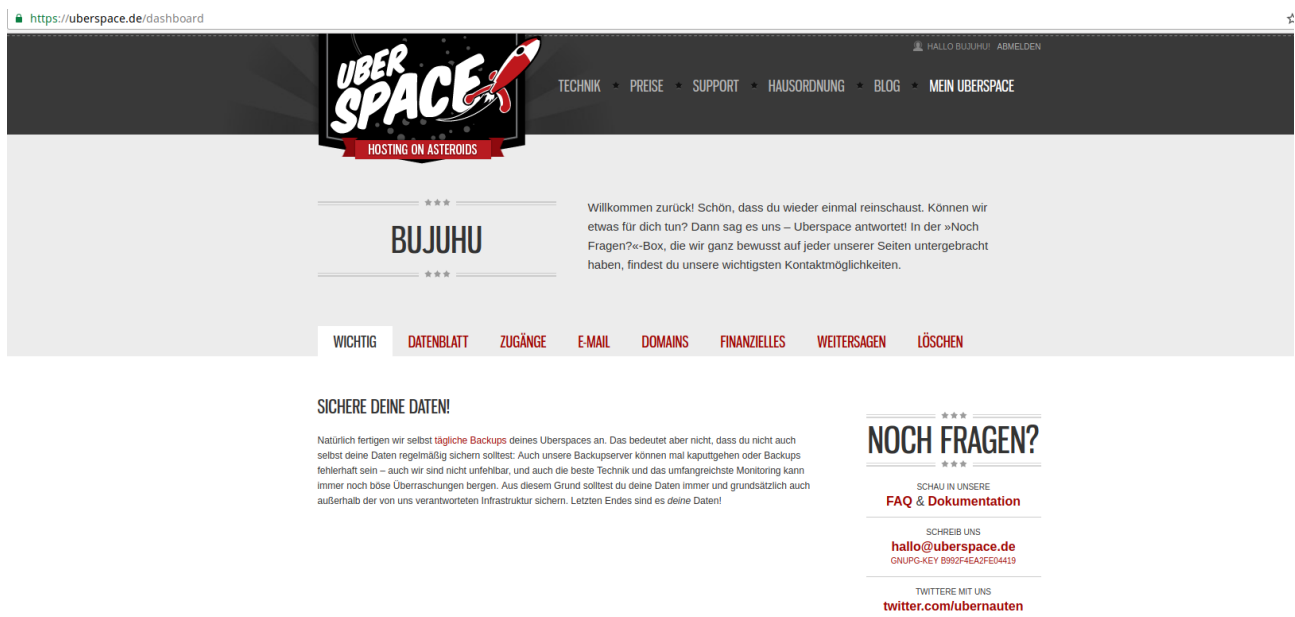
Alle Anwendungen (mit Ausnahm vom öffentlichen Webserver auf Rewood) werden in Docker Containern auf den Servern installiert um diese voneinander zu Isolieren und einfacher verwalten zu können. Dazu wird ein Dockerfile erstellt, welche definiert, wie die einzelnen Container miteinander und mit er Außenwelt Kommuniziert. Am Physischen Server selbst, wird nur Docker, openSSH (Administration) und IPTables (Firewall) installiert und nur authentifizierungsoptionen konfiguriert.

Da Uberspace ein shared Hoster 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 Unternehmenswebsite wird meine Private seite genutzt.

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



The screenshot shows the Uberspace dashboard at <https://uberspace.de/dashboard>. The user is logged in as 'BUJUHU'. The dashboard features a navigation menu with links for 'TECHNIK', 'PREISE', 'SUPPORT', 'HAUSORDNUNG', 'BLOG', and 'MEIN UBERSPACE'. Below the navigation, there is a section for 'BUJUHU' 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, there are several tabs: '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 for '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	 

Hinzufügen eines Zertifikats auf der Unternehmenswebsite

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 von `uberspace-add-certificate` aktiviert

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

Juri Schreib

KMU Projekt Platzhalter

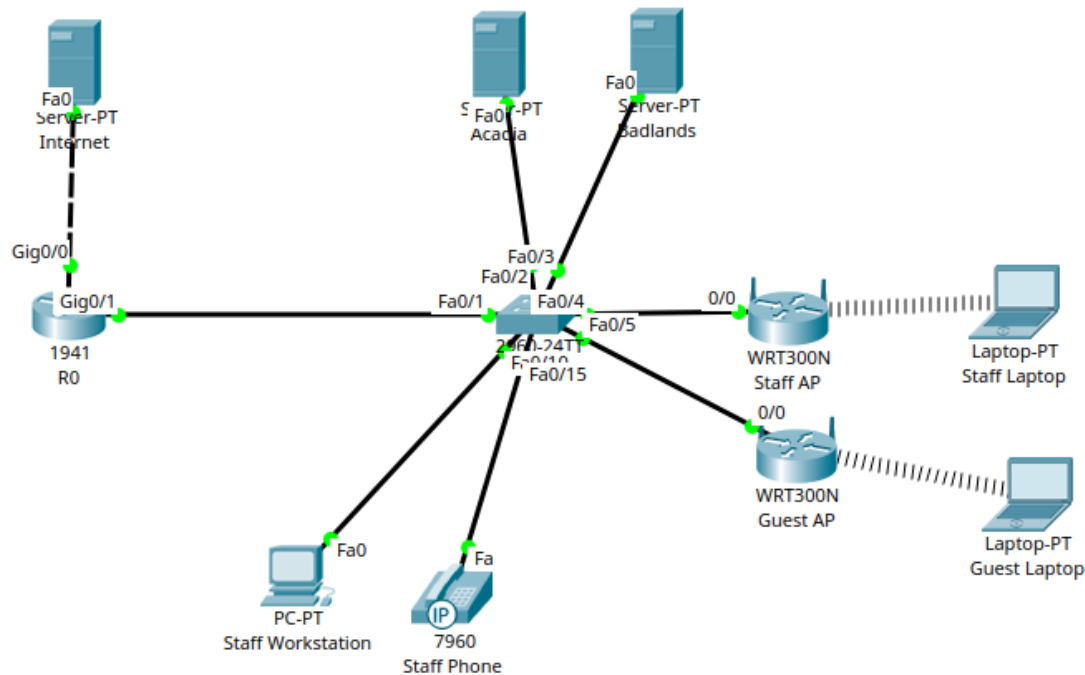
Die Website ist nun unter kmu.schreib.at erreichbar.

Information zum ASA Gerät

Da die ASA mit der standard Lizenz nur 2-Vlans forwarding konfiguriert werden kann, wird ein 2. kleineres Testnetzwerk modelliert, um die funktionsweise der ASA zu testen und demonstrieren. Da der DHCP Server nach der [Dokumentation](#) auf dem Router läuft, wird am Router einfach inter-vlan routing genutzt, um zwischen den verschiedenen VLANs zu kommunizieren.

Das Device hardening wird im ersten Schritt erstmal ausgelassen. Es geht erst mal darum, eine funktionierendes Netzwerk aufzusetzen.

Netzwerkkonfiguration



IP Konfiguration

Dem Router wird die öffentliche IP Adresse 1.1.1.2 im Netz 1.1.1.0/24 zur Verfügung gestellt. Das Internet wird durch einen Server mit der IP Adresse 1.1.1.1 emuliert.

Alle anderen statischen IP Adressen und Interfaces werden so wie in [3 Software & Unternehmenswebsite](#) definiert vergeben.

Da es im Packet Tracer keinen Access Point gibt, der 802.1Q unterstützt, wird dieser durch 2 Access Points ersetzt, die sich in den jeweiligen vlans (Guest & Staff) befinden und einer sich in dem jeweiligen Subnet befindlichen IP Adresse zugewiesen werden. Der Einfachheit halber bleibt auf diesen Geräten NAT und DHCP aktiviert.

Konfiguration Staff AP

Static IP

Internet IP Address: 10 . 0 . 40 . 2
Subnet Mask: 255 . 255 . 255 . 0
Default Gateway: 10 . 0 . 40 . 1
DNS 1: 10 . 0 . 20 . 2
DNS 2 (Optional): 0 . 0 . 0 . 0
DNS 3 (Optional): 0 . 0 . 0 . 0

Host Name: _____

Domain Name: _____

MTU: Size: 1500

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server: Enabled Disabled

Start IP Address: 192.168.0. 100

Maximum number of Users: 50

IP Address Range: 192.168.0. 100 - 149

Konfiguration Guest AP

Static IP

Internet IP Address: 10 . 0 . 50 . 2
Subnet Mask: 255 . 0 . 0 . 0
Default Gateway: 10 . 0 . 50 . 1
DNS 1: 10 . 0 . 20 . 2
DNS 2 (Optional): 0 . 0 . 0 . 0
DNS 3 (Optional): 0 . 0 . 0 . 0

Host Name: _____

Domain Name: _____

MTU: Size: 1500

IP Address: 192 . 168 . 0 . 1

Subnet Mask: 255.255.255.0

DHCP Server: Enabled Disabled

Wireless Configuration

SSID	Verschlüsselungsmethode	Password
KMU_Guest	-	-
KMU_Staff	kmuprojekt	WPA2/PSK (AES)

Konfiguration Staff AP

Network Mode: Mixed

Network Name (SSID): KMU_Staff

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: Enabled Disabled

Security Mode: WPA2 Personal

Encryption: AES

Passphrase: kmuprojekt

Key Renewal: 3600 seconds

Konfiguration Guest AP

Network Mode: Mixed

Network Name (SSID): KMU_Guest

Radio Band: Auto

Wide Channel: Auto

Standard Channel: 1 - 2.412GHz

SSID Broadcast: Enabled Disabled

Security Mode: Disabled

Nat Konfiguration am Router

Im echten Netzwerk muss die öffentliche Ip Adresse, mit der des ISPs ersetzt werden.

Das Interface g0/0 wird als outside interface definiert. Alle subinterface von g0/1 als inside.

```
ip nat pool NAT 10.0.0.1 10.0.50.255 netmask 255.255.0.0
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip classless
!
ip flow-export version 9
!
!
access-list 1 permit 10.0.0.0 0.0.255.255
```

DHCP Konfiguration am Router

Da DHCP im Guest Vlan in diesem Modell vom Access-Point übernommen wird, muss nur ein DHCP pool im Staff VLAN aktiviert werden.

```
ip dhcp pool Staff
network 10.0.40.0 255.255.255.0
default-router 10.0.40.1
dns-server 10.0.20.2
ip dhcp excluded-address 10.0.40.1 10.0.40.100
```

Authentication & Router hardening

Gleichzeitig mit dem Router hardening wird auf den Geräten SSH aktiviert.

Konfiguration die über alle Geräte hinweg gleich ist:

```
banner motd #unauthorized access prohibited#
security passwords min-length 10
service password-encryption
enable secret ciscoclass
username cisco privilege 15 secret ciscoclass
ip domain-name schreib.at
crypto key generate rsa
2048
ip ssh version 2
ip ssh time-out 90
ip ssh authentication-retries 2
line vty 0 15
login local
transport input ssh
transport output ssh
exec-timeout 20
line con 0
login local
transport output ssh
exec-timeout 20
```

Port Security Konfiguration am Switch

Die Port Security wird bei allen Ports auf sticky gestellt. Nicht benutzer Ports werden administrativ deaktiviert

```
interface FastEthernet0/1
  switchport mode trunk
  switchport port-security mac-address sticky
  !
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/3
  switchport access vlan 20
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/4
  switchport access vlan 40
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/5
  switchport access vlan 50
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/6
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/7
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/8
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/9
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/10
  switchport access vlan 40
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/11
  switchport access vlan 40
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/12
  switchport access vlan 40
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/13
  switchport access vlan 40
  switchport mode access
  switchport port-security mac-address sticky
  !
interface FastEthernet0/14
  switchport access vlan 40
  switchport mode access
  switchport port-security mac-address sticky
```



```

interface FastEthernet0/15
  switchport access vlan 30
  switchport mode access
  switchport port-security mac-address sticky
!
interface FastEthernet0/16
  switchport access vlan 30
  switchport mode access
  switchport port-security mac-address sticky
!
interface FastEthernet0/17
  switchport access vlan 30
  switchport mode access
  switchport port-security mac-address sticky
!
interface FastEthernet0/18
  switchport access vlan 30
  switchport mode access
  switchport port-security mac-address sticky
!
interface FastEthernet0/19
  switchport access vlan 30
  switchport mode access
  switchport port-security mac-address sticky
!
interface FastEthernet0/20
  switchport access vlan 30
  switchport mode access
  switchport port-security mac-address sticky
!
interface FastEthernet0/21
  switchport mode access
  switchport port-security mac-address sticky
  shutdown
!
interface FastEthernet0/22
  switchport mode access
  switchport port-security mac-address sticky
  shutdown
!
interface FastEthernet0/23
  switchport mode access
  switchport port-security mac-address sticky
  shutdown
!
interface FastEthernet0/24
  switchport mode access
  switchport port-security mac-address sticky
  shutdown

```

Die SSH Verbindung wird getestet

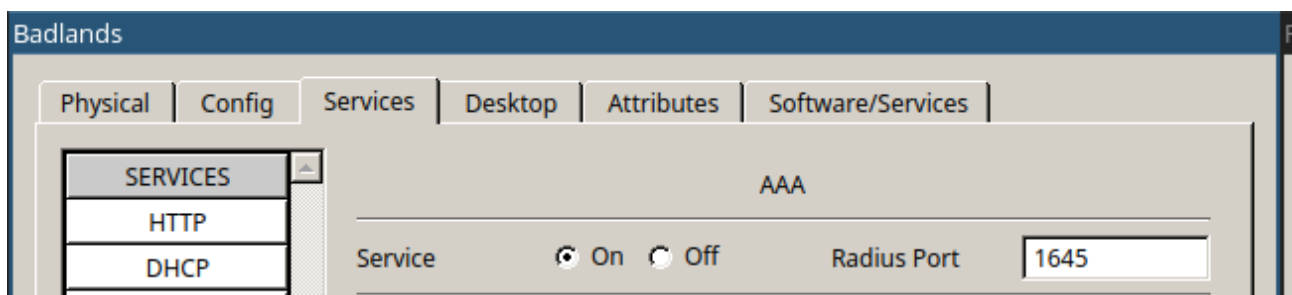
```

[Connection to 10.0.0.1 closed by foreign host]
C:\>ssh -l cisco 10.0.0.1
Open
Password:
Password:
unauthorized access prohibited
R0#

```

Radius

Als erstes wird der Radius service am Badlands Server aktiviert



- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoE
- VM Management

Network Configuration

Client Name Client IP
 Secret ServerType

	Client Name	Client IP	Server Type	Key
1	R0	10.0.0.1	Radius	ciscoclass
2	SW0	10.0.0.2	Radius	ciscoclass

Add

Save

Remove

User Setup

Username Password

	Username	Password
1	cisco	ciscoclass

Add

Save

Remove

Top

Danach wird AAA auf den Intermediate Devices aktiviert

```

aaa new-model
radius-server host 10.0.20.2 key ciscoclass
aaa authentication login default group radius local
login block-for 120 attempts 5 within 60
  
```

```
login on-success log
login on-failure log
```

Der Switch unterstützt im Packet Tracer kein AAA, daher wird diese Konfiguration am Switch in der Testumgebung ausgelassen. Die Obere Konfiguration kann allerdings 1 zu 1 für den Switch übernommen werden, um AAA zu aktivieren.

Running-config Files

R0

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
security passwords min-length 10
!
hostname R0
!
login block-for 120 attempts 5 within 60
login on-failure log
login on-success log
!
!
enable secret 5 $1$mERr$UBS6AqpcFjkupAnmSUCGG.
!
!
ip dhcp excluded-address 10.0.40.1 10.0.40.100
!
ip dhcp pool Staff
network 10.0.40.0 255.255.255.0
default-router 10.0.40.1
dns-server 10.0.20.2
!
!
aaa new-model
!
aaa authentication login default group radius local
!
!
!
!
!
!
!
ip cef
no ipv6 cef
!
!
!
username cisco privilege 15 secret 5 $1$mERr$UBS6AqpcFjkupAnmSUCGG.
!
!
license udi pid CISCO1941/K9 sn FTX1524813R
!
!
```



```
interface GigabitEthernet0/1.50
 encapsulation dot1Q 50
 ip address 10.0.50.1 255.255.255.0
 ip nat inside
 !
interface Vlan1
 no ip address
 shutdown
 !
ip nat pool NAT 10.0.0.1 10.0.50.255 netmask 255.255.0.0
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip classless
 !
ip flow-export version 9
 !
 !
access-list 1 permit 10.0.0.0 0.0.255.255
ip access-list extended sl_def_acl
 deny tcp any any eq telnet
 deny tcp any any eq www
 deny tcp any any eq 22
 permit tcp any any eq 22
 !
banner motd ^Cunauthorized access prohibited^C
 !
radius-server host 10.0.20.2 auth-port 1645 key ciscoclass
 !
 !
 !
line con 0
 transport output ssh
 exec-timeout 20 0
 !
line aux 0
 !
line vty 0 4
 exec-timeout 20 0
 transport input ssh
 transport output ssh
line vty 5 15
 exec-timeout 20 0
 transport input ssh
 transport output ssh
 !
 !
 !
end
```

SW0

```
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
 !
hostname SW0
 !
```

```
enable secret 5 $1$mERr$UBS6AqpcFjkupAnmSUCGG.
!
!
!
ip ssh version 2
ip ssh authentication-retries 2
ip ssh time-out 90
ip domain-name schreib.at
!
username cisco secret 5 $1$mERr$UBS6AqpcFjkupAnmSUCGG.
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
switchport mode trunk
switchport port-security mac-address sticky
!
interface FastEthernet0/2
switchport access vlan 10
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/3
switchport access vlan 20
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/4
switchport access vlan 40
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/5
switchport access vlan 50
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/6
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/7
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/8
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/9
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/10
switchport access vlan 40
```

```
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/11
switchport access vlan 40
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/12
switchport access vlan 40
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/13
switchport access vlan 40
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/14
switchport access vlan 40
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/15
switchport access vlan 30
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/16
switchport access vlan 30
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/17
switchport access vlan 30
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/18
switchport access vlan 30
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/19
switchport access vlan 30
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/20
switchport access vlan 30
switchport mode access
switchport port-security mac-address sticky
!
interface FastEthernet0/21
switchport mode access
switchport port-security mac-address sticky
```

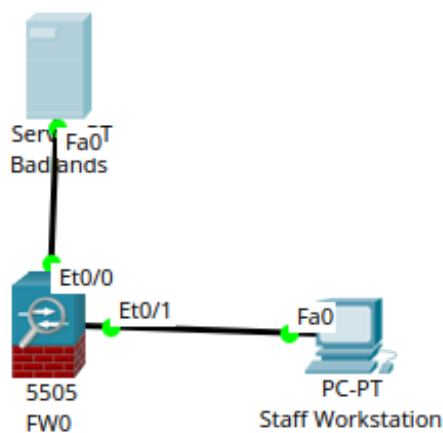
```
shutdown
!
interface FastEthernet0/22
switchport mode access
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/23
switchport mode access
switchport port-security mac-address sticky
shutdown
!
interface FastEthernet0/24
switchport mode access
switchport port-security mac-address sticky
shutdown
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 10.0.0.2 255.255.255.0
!
interface Vlan10
mac-address 00d0.ff1b.ee01
no ip address
!
interface Vlan20
mac-address 00d0.ff1b.ee02
no ip address
!
interface Vlan30
mac-address 00d0.ff1b.ee03
no ip address
!
interface Vlan40
mac-address 00d0.ff1b.ee04
no ip address
!
interface Vlan50
mac-address 00d0.ff1b.ee05
no ip address
!
ip default-gateway 10.0.0.1
!
banner motd ^Cunauthorized access prohibited^C
!
!
!
line con 0
login local
exec-timeout 20 0
!
line vty 0 4
exec-timeout 20 0
```

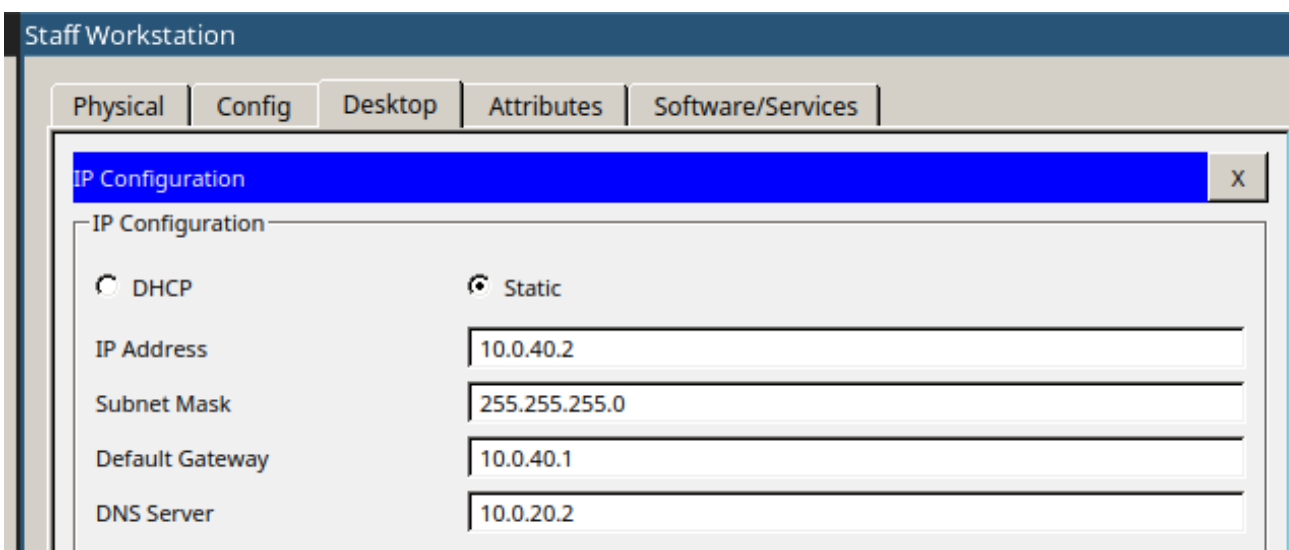
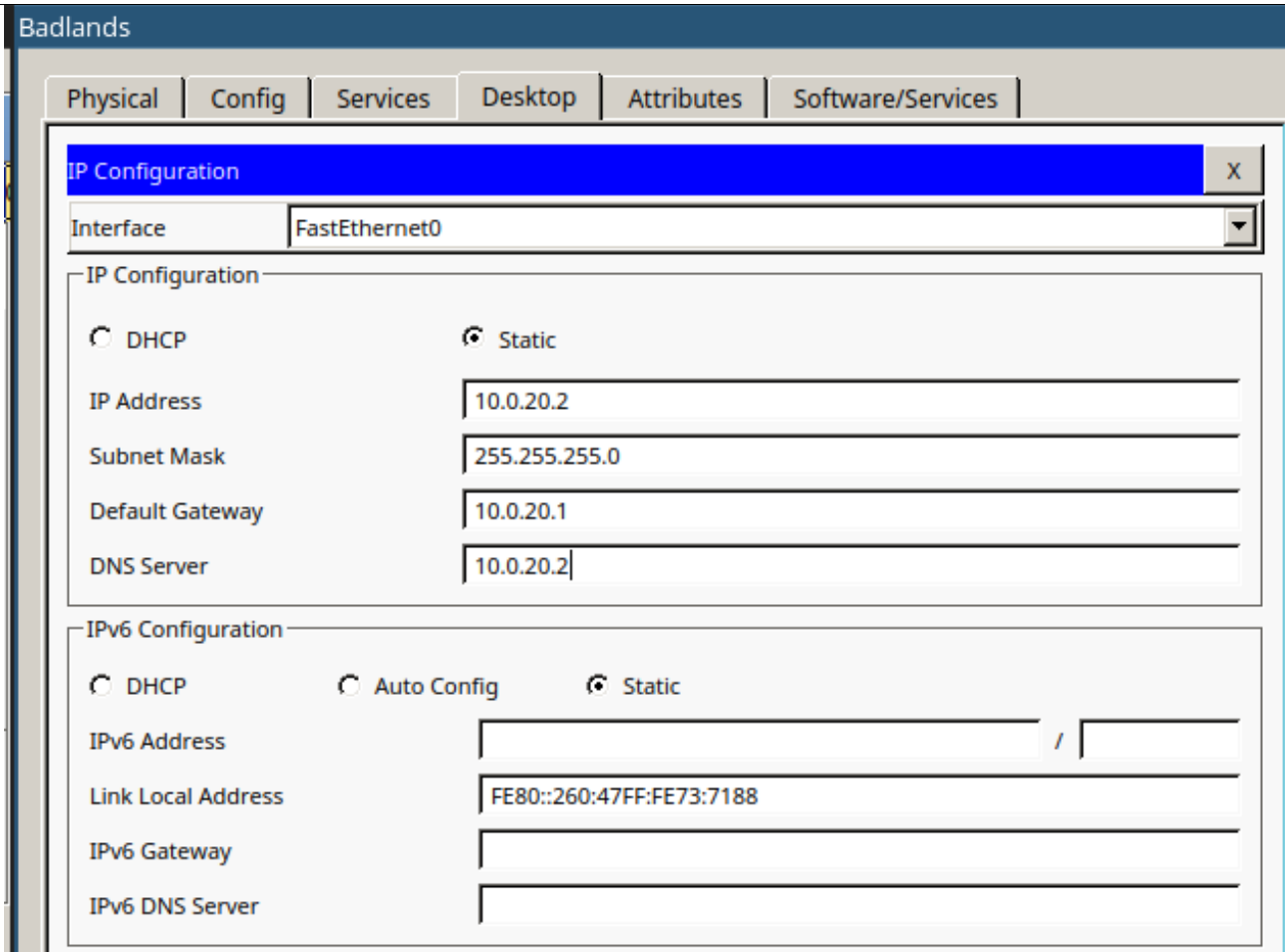


```
login local
transport input ssh
transport output ssh
line vty 5 15
exec-timeout 20 0
login local
transport input ssh
transport output ssh
!
!
!
end
```

ASA Konfiguration

DA die ASA im Packettracer nicht sonderlich gut simuliert wird, wird ein kleineres Netzwerk aufgebaut, um die Konfiguration der ASA durchzuführen. In diesem mini-netzwerk werden nur die Geräte FW0, Staff Workstation und Badlands simuliert, da mehr als 2 VLANs nicht unterstützt werden.





Die Vlans sollten auf der echten ASA mit folgenden Security levels konfiguriert werden:

ID	Name	Security-Level
1	Management	100
2	Outside	0
10	DMZ	0
20	Intranet	40
30	VOIP	60
40	Staff	80

ID	Group	Security-Level
----	-------	----------------

Alle konfigurierten access listen werden als inbound definiert. Die Access Listen werden auf der konfiguration der ASA noch mit keinem Interface in verbindung gebracht, da diese vom Testnetzwerk und vom realen Netzwerk abweichen.

Um die DMZ nutzen zu können muss folgendes Kommando zusätzlich an der ASA ausgeführt werden:

```
route outside 0.0.0.0 0.0.0.0 10.0.20.1
```

Um die Outside Access-List einem Interface zuzuweisen, muss folgendes Kommando angegeben werden:

```
access-group outside in interface outside
```

Da es in der Testumgebung das Outside interface nicht existiert, ist es nicht möglich, diese Befehle auszuführen.

Running-config der ASA

```
hostname FW0
names
!
interface Ethernet0/0
  switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
  nameif intranet
  security-level 50
  ip address 10.0.20.1 255.255.255.0
!
interface Vlan2
  nameif staff
  security-level 100
  ip address 10.0.40.1 255.255.255.0
!
interface Vlan20
  no nameif
  no security-level
  no ip address
```

```
!
object network acadia
 host 10.0.20.1
!
!
access-list outside extended permit tcp any object acadia
access-list outside extended permit tcp any object acadia eq smtp
access-list outside extended permit tcp any object acadia eq pop3
access-list outside extended permit tcp any object acadia eq www
access-list outside extended permit tcp any object acadia eq 22
access-list outside extended permit tcp any object acadia eq 25565
access-list outside extended permit tcp any object acadia eq 1194
access-list outside extended permit tcp any object acadia eq 8001
access-list outside extended permit tcp any object acadia eq 27900
access-list outside extended permit udp any 10.0.30.0 255.255.255.0 eq 5060
!
!
!
!
!
!
!
!
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
```

Virtuelle Maschinen erstellen

Anwendungen auf Acadia installieren und verfügbar machen.

OpenSSH kann bereits bei der installation von Ubuntu installiert wird und muss nicht mehr mehr manuell aufgesetzt werden.

Vor der Installation wird das System mit `apt-get update; apt-get upgrade` auf den aktuellsten Stand gebracht

Installation von Docker und Docker-Compose

Docker wird [nach der Anleitung der Docker Website](#) installiert.

Docker-Compose wird ebenfalls [nach der Anleitung](#) installiert.

Um zu testen ob die Anwendungen installiert sind, wird zum testendocker `-v` und `docker-compose -v` verwendet.

```
root@kmu-Acadia:~# chmod +x /usr/local/bin/docker-compose
root@kmu-Acadia:~# docker -v
Docker version 17.03.0-ce, build 3a232c8
root@kmu-Acadia:~# docker-compose -v
docker-compose version 1.11.2, build dfed245
root@kmu-Acadia:~#
```

Nach der Vollständigen Installation von Docker-Compose kann nun mit der Installation der einzelnen Komponenten begonnen werden

Installation von Webmin

Webmin wird <http://www.debianadmin.com/install-webmin-on-debian-7-6-wheezy.html> unter Debian installiert.

Die Verschlüsselung des Webmin Miniserv wird deaktiviert, da die Verschlüsselung von Nginx übernommen wird.

nano /etc/webmin/miniserv.conf Der Parameter `ssl=1` wird auf `ssl=0` gesetzt. Danach wird Webmin neu gestartet.

```
-bash: systemctl: command not found
root@kmu-Acadia:~# service webmin status
Webmin (pid 17756) is running
root@kmu-Acadia:~#
```

Installation von NGINX

Webmin wird ebenfalls direkt auf dem Host installiert

```
apt-get install -y nginx
```

```
root@kmu-Acadia:~# service nginx status
[ ok ] nginx is running.
```

Welcome to nginx on Debian!

If you see this page, the nginx web server is successfully installed and working on Debian. Further configuration is required.

For online documentation and support please refer to nginx.org

Please use the `reportbug` tool to report bugs in the nginx package with Debian. However, check [existing bug reports](#) before reporting a new bug.

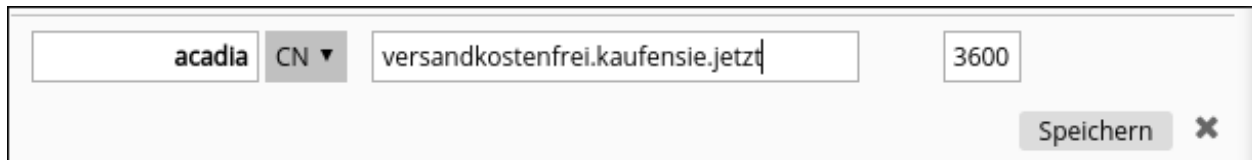
Thank you for using debian and nginx.

Die Installation von NGINX war erfolgreich.

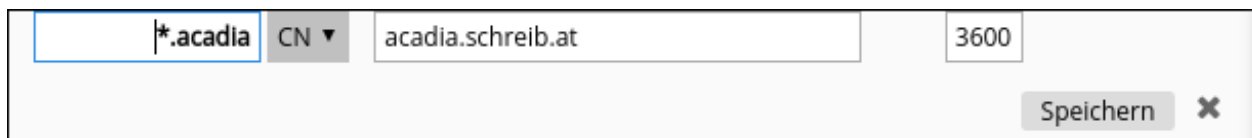
Subdomäne erstellen

Dafür wird als erstes eine eigene Subdomain für den Server erstellt

Dazu wird beim DNS Server ein neuer CNAME Record erstellt



Der Einfachheit halber wird die Wildcard Domain `*acadia.schreib.at` erstellt, um auf alle Dienste des Servers zugreifen zu können.



NextCloud (Nativ)

Als erstes wird NextCloud heruntergeladen und in das richtige Verzeichnis verschoben:

```
cd ~
wget https://download.nextcloud.com/server/releases/nextcloud-11.0.2.zip
unzip nextcloud-11.0.2.zip
mkdir /var/www/
mv nextcloud /var/www/
rm nextcloud-11.0.2.zip
chown -R www-data: /var/www/nextcloud
```

Um Nginx verwenden zu können wird auch noch ein MySQL kompatibler Server benötigt. Dafür wird MariaDB gewählt und installiert

```
sudo apt-get install -y mariadb-server
```

Das Administratorpassword der Datenbank wird auf `ciscoclass` gesetzt.

GitLab

Gitlab wird [nach der Anleitung auf der GitLab Seite](#) installiert.

Der externe Port wird von 80 auf 8080 verändert, indem die `external_url` konfigurationsparameter in `/etc/gitlab/gitlab.rb` auf `external_url http://127.0.0.1:8080/` gesetzt wird. Danach wird gitlab mit dem Befehl `gitlab-ctl reconfigure` neugestartet.

NGINX konfigurieren

Damit NextCloud richtig funktioniert muss erstmal php für NGINX installiert werden. Dafür werden die Pakete php5, php5-cgi, php5-gd, php5-curl, php5-mysql und php5-fpm benötigt

NGINX wird dazu genutzt, auf die einzelnen Webanwendungen mithilfe von subdomänen zugreifen zu können (sprich webmin.acadia.schreib.at für webmin, git.acaida.schreib.at für gitlab und acadia.schreib.at für NextCloud)

Nginx Konfigurationsdatei:

```
# Webmin
server {
    server_name webmin.acadia.schreib.at;
    listen 80;
    location / {
        proxy_redirect http://127.0.0.1:10000/ http://webmin.acadia.schreib.at/;
        proxy_pass http://127.0.0.1:10000/;
        proxy_set_header    Host    $host;
    }
}

# GitLab
server {
    server_name git.acadia.schreib.at;
    listen 80;
    location / {
        proxy_redirect http://127.0.0.1:8080/ http://git.acadia.schreib.at/;
        proxy_pass http://127.0.0.1:8080/;
        proxy_set_header    Host    $host;
    }
}

# NextCloud
server {
    listen 80;
    server_name cloud.acadia.schreib.at;

    #ssl_certificate /etc/ssl/nginx/cloud.example.com.crt;
    #ssl_certificate_key /etc/ssl/nginx/cloud.example.com.key;

    root /var/www/;

    # set max upload size
    client_max_body_size 10G;

    # Disable gzip to avoid the removal of the ETag header
    gzip off;

    # Uncomment if your server is build with the ngx_pagespeed module
    # This module is currently not supported.
    #pagespeed off;

    index index.html index.php;
    error_page 403 /core/templates/403.php;
    error_page 404 /core/templates/404.php;
```

```

rewrite ^/.well-known/carddav /remote.php/dav/ permanent;
rewrite ^/.well-known/caldav /remote.php/dav/ permanent;

# The following 2 rules are only needed for the user_webfinger app.
# Uncomment it if you're planning to use this app.
#rewrite ^/.well-known/host-meta /public.php?service=host-meta last;
#rewrite ^/.well-known/host-meta.json /public.php?service=host-meta-json last;

location = /robots.txt {
allow all;
log_not_found off;
access_log off;
}

location ~ ^/(build|tests|config|lib|3rdparty|templates|data)/ {
deny all;
}

location ~ ^/(?!\.|autotest|occ|issue|indie|db_|console) {
deny all;
}

location / {

rewrite ^/remote/(.*) /remote.php last;

rewrite ^(/core/doc/[^\/]+/)$ $1/index.html;

try_files $uri $uri/ =404;
}

location ~ \.php(?:$|/) {
fastcgi_param HTTP_PROXY "";

fastcgi_pass unix:/var/run/php5-fpm.sock;
fastcgi_index index.php;
include fastcgi_params;
}

# Adding the cache control header for js and css files
# Make sure it is BELOW the location ~ \.php(?:$|/) { block
location ~* \.(?:css|js)$ {
add_header Cache-Control "public, max-age=7200";
# Add headers to serve security related headers
add_header Strict-Transport-Security "max-age=15768000; includeSubDomains;
preload;";
add_header X-Content-Type-Options nosniff;
add_header X-Frame-Options "SAMEORIGIN";
add_header X-XSS-Protection "1; mode=block";
add_header X-Robots-Tag none;
add_header X-Download-Options noopen;
add_header X-Permitted-Cross-Domain-Policies none;
# Optional: Don't log access to assets
access_log off;
}

```



```
# Optional: Don't log access to other assets
location ~* \.(?:jpg|jpeg|gif|bmp|ico|png|swf)$ {
    access_log off;
}
}
```

Besagte Konfigurationsdatei mit dem namen proxy-config wird im folgenden Verzeichnis abgelegt:

/etc/nginx/sites-available

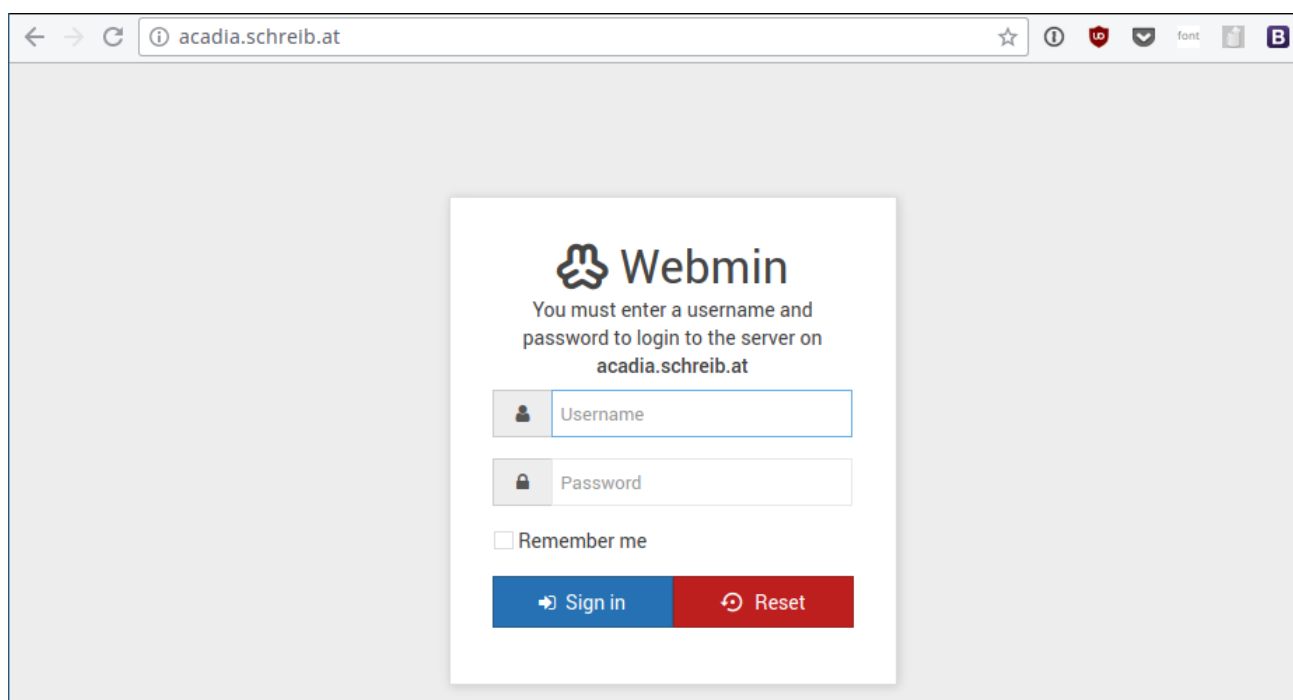
```
:/etc/nginx/sites-available# touch proxy-config
:/etc/nginx/sites-available# nano proxy-config
:/etc/nginx/sites-available# █
```

Um diese zu aktivieren muss die aktuelle konfiguration aus dem sites-enabled Ordner gelöscht und durch die neue ersetzt werden:

```
root@kmu-Acadia:/etc/nginx/sites-available# rm ../sites-enabled/default
root@kmu-Acadia:/etc/nginx/sites-available# ln -s ../sites-enabled/proxy-config proxy-config
ln: failed to create symbolic link 'proxy-config': File exists
root@kmu-Acadia:/etc/nginx/sites-available# ln -s proxy-config ../sites-enabled/proxy-config
root@kmu-Acadia:/etc/nginx/sites-available# ls -la ../sites-enabled/
total 8
drwxr-xr-x 2 root root 4096 Mar 21 11:30 .
drwxr-xr-x 6 root root 4096 Mar 21 11:02 ..
lrwxrwxrwx 1 root root   12 Mar 21 11:30 proxy-config -> proxy-config
root@kmu-Acadia:/etc/nginx/sites-available# █
```

Danach wird der NGINX Service neugestartet.

Jetzt sind die einzelnen Webdienste erreichbar.



Einrichten von NextCloud



Create an admin account

root

cisoclass



So-so password

Storage & database ▾

Data folder

/var/www/nextcloud/data

Configure the database

Only MySQL/MariaDB is available. Install and activate additional PHP modules to choose other database types.

For more details check out the [documentation](#). ↗

root

cisoclass



nextcloud

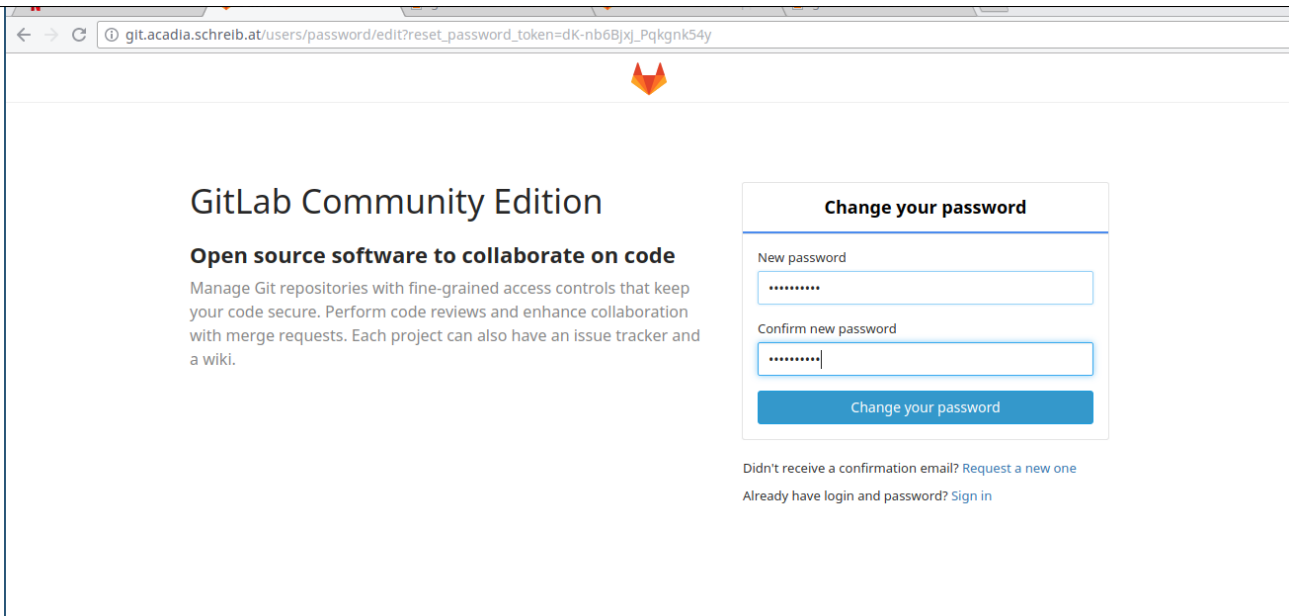
localhost

Finish setup

Need help? See the [documentation](#) ↗

Einrichten von GitLab

Das Passwort wird auf cisoclass gesetzt.



Aufsetzen von Badlands

Um den Server im Unterricht demonstrieren zu können wird Badlands innerhalb einer Virtuellen Maschine erstellt.

Das root password wird auf ciscoclass gesetzt. Der SSH Server wird automatisch mit installiert.

Danach wird die Installation voollständig ausgeführt.

Zur einfacheren konfiguration wird auf dem Gerät Webmin installiert

ssh

SSH wurde bereits bei der Installation vorkonfiguriert. In den Konfigurationsdateien wird der root login aktiviert

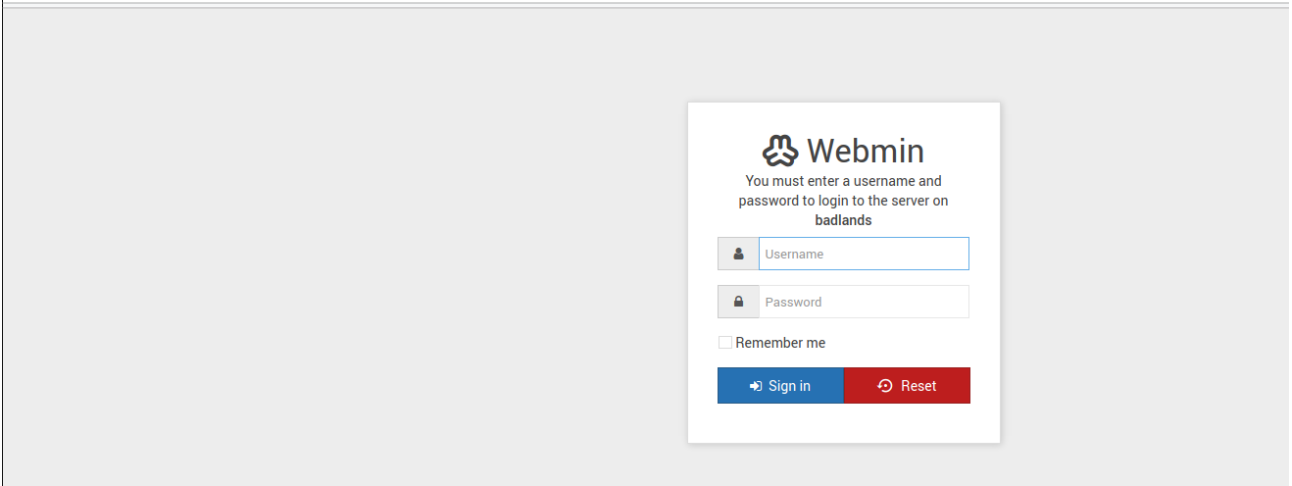
```
bujuhu ~ ssh root@192.168.43.212
root@192.168.43.212's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 23 14:25:46 2017
root@badlands:~#
```

Webmin

Damit der Server einfacher verwaltet werden kann, wird nach dem selben Prozess der letzten Übung Webmin auf dem Server installiert.



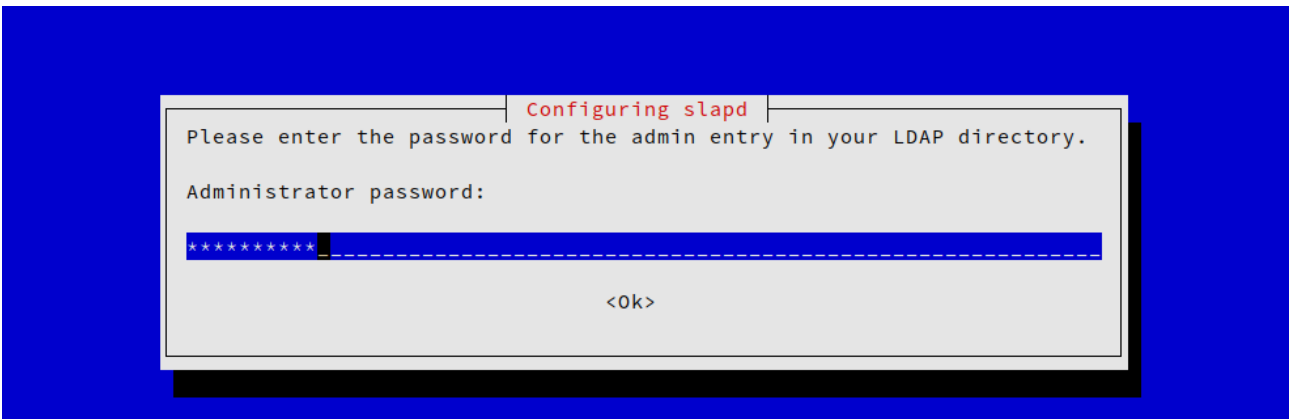
phpldapadmin

PHPldap wird mit dem befehl apt-get install phpldapadmin installiert.

LDAP

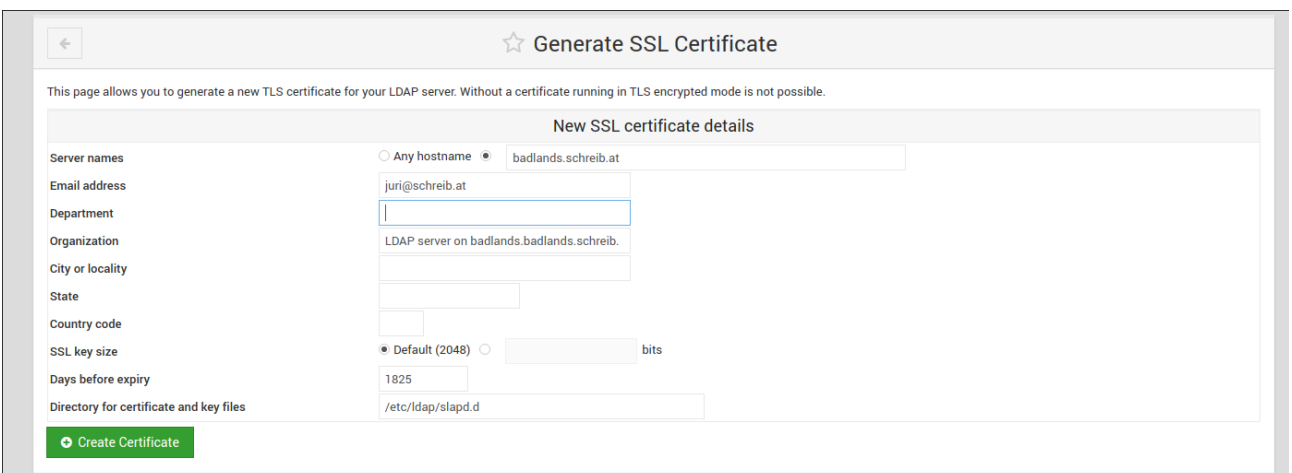
Die Pakete slapd ldap-utils ldapscripts werden installiert.

Das Administrator Passwort wird auf ciscoclass gesetzt



Konfiguration

Es wird ein SSL Zertifikat für LDAP generiert



Administratordokumentation

SSH und SFTP

Nutzen sie ihren Administratoraccount und greifen sie auf den Server mit dem SSh oder SFTP Applikation ihrer wahl darauf zu:

```
bujuhu ~/Sync/Projects/nvs gh-pages ssh bujuhu@ldap.kmu.schreib.at
bujuhu@ldap.kmu.schreib.at's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-71-generic x86_64)

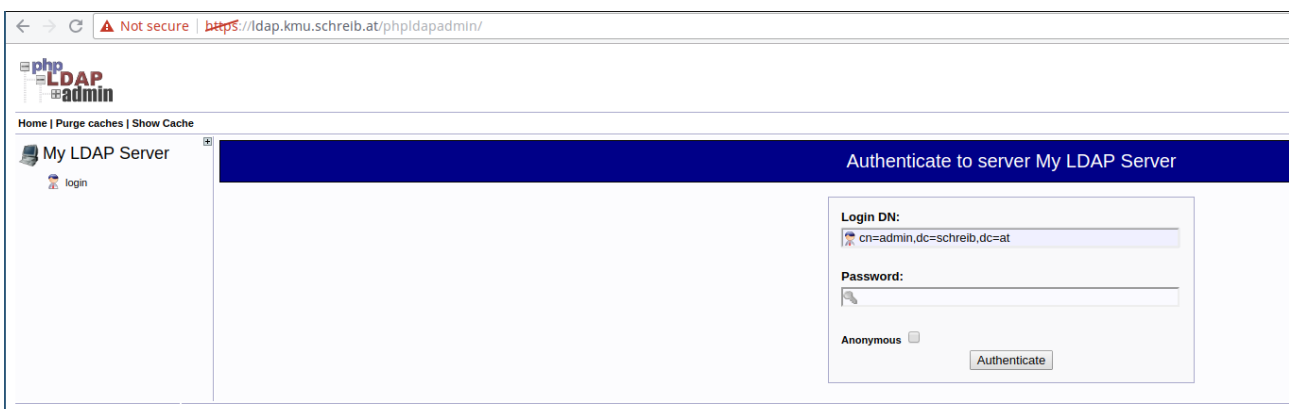
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

13 packages can be updated.
0 updates are security updates.

Last login: Mon Apr  3 20:59:15 2017 from 10.0.0.242
```

LDAP

Rufen sie die Administrationsoberfläche phpldapadmin über die URL <https://ldap.kmu.schreib.at/phpldapadmin/> auf.



Geben sie den DN ihres Administratoraccounts, sowie ihr Passwort an um sich anzumelden

Erstellen eines Benutzers

Kopieren sie den max.muster benutzer und passen sie die Werte auf den neuen Benutzer an

The screenshot shows the 'My LDAP Server' web interface. On the left is a tree view of the LDAP directory structure, including 'dc=schreib, dc=at', 'cn=admin', 'ou=groups', and 'cn=users'. The main area displays the configuration for the user 'uniqueIdentifier=max.muster'. The configuration includes fields for 'cn' (Max Muster), 'Email' (max.muster@kmu.schreib.at), 'gidNumber' (501), 'givenName' (Max), 'homeDirectory' (/home/max.muster), 'mailEnabled' (true), 'mailGidNumber' (5000), and 'mailHomeDirectory'. A list of actions is visible on the left, such as 'Refresh', 'Switch Template', 'Copy or move this entry', 'Rename', 'Create a child entry', 'Export', 'Delete this entry', 'Compare with another entry', and 'Add new attribute'.

Webimn (Acadia)

Melden sie sich mit ihrem Benutzernamen und Passwort auf <http://webmin.acadia.schreib.at> an

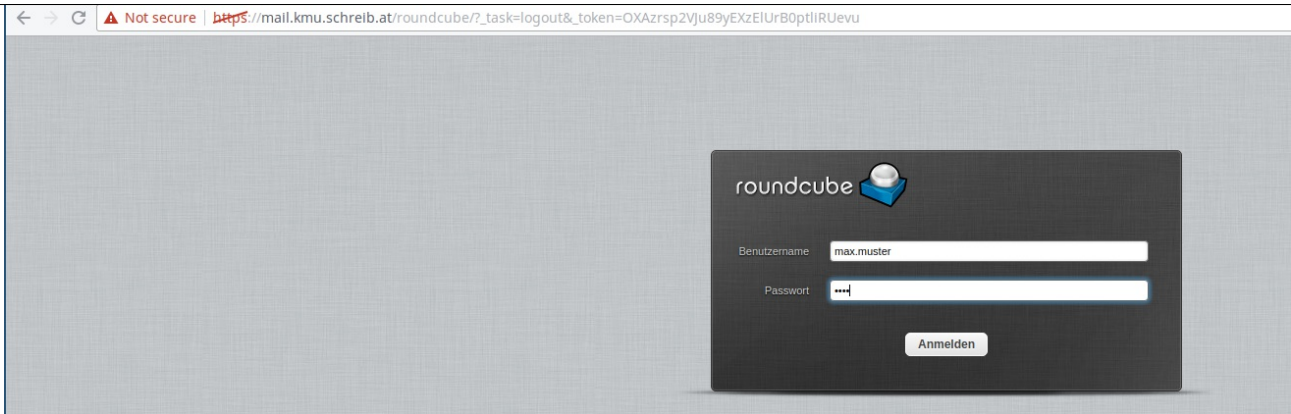
The screenshot shows the login page for 'webmin.acadia.schreib.at'. It features the Webmin logo and a message: 'You must enter a username and password to login to the server on webmin.acadia.schreib.at'. There are input fields for the username (root) and password (masked with dots). A 'Remember me' checkbox is present. At the bottom, there are 'Sign in' and 'Reset' buttons.

Benutzerdokumentation

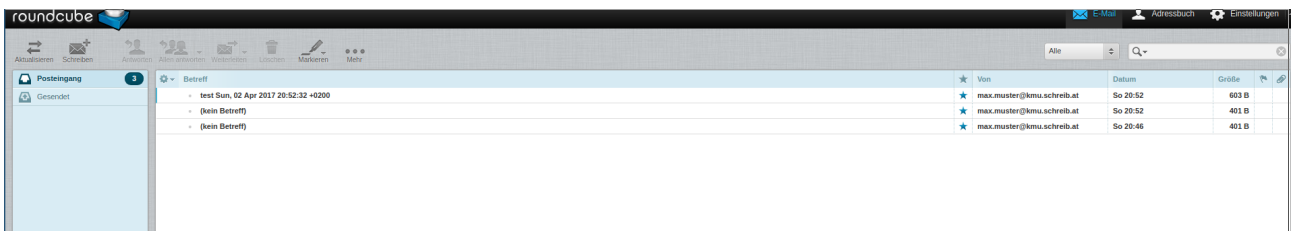
E-Mail

Wenn sich der Computer, welcher E-Mails nutzen möchte sich innerhalb des Unternehmensnetzwerkes befindet, kann ganz einfach mit einen Aufruf auf (<https://mail.kmu.schreib.at/roundcube>)[<https://mail.kmu.schreib.at>] geschehen.

Melden Sie sich mit ihrem Benutzernamen und Passwort an:



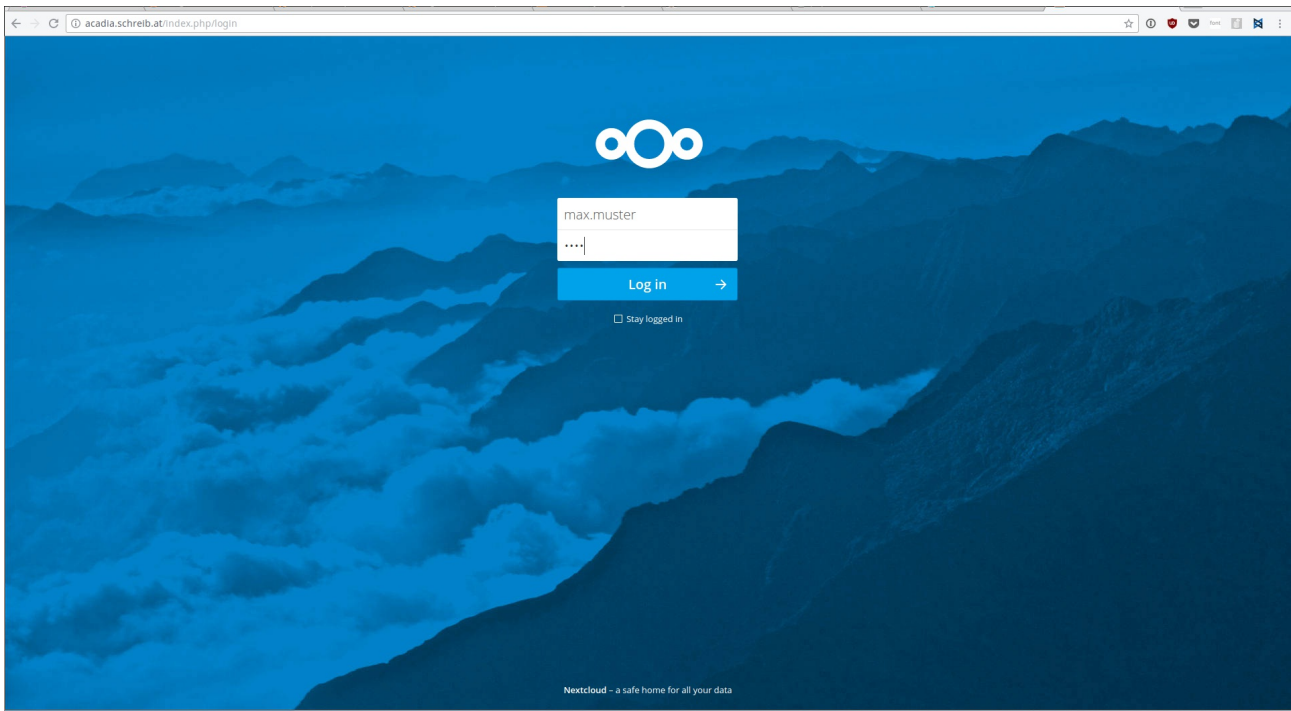
Danach haben Sie Zugriff auf Ihre E-Mails sowie die Möglichkeit neue E-Mails zu verfassen.



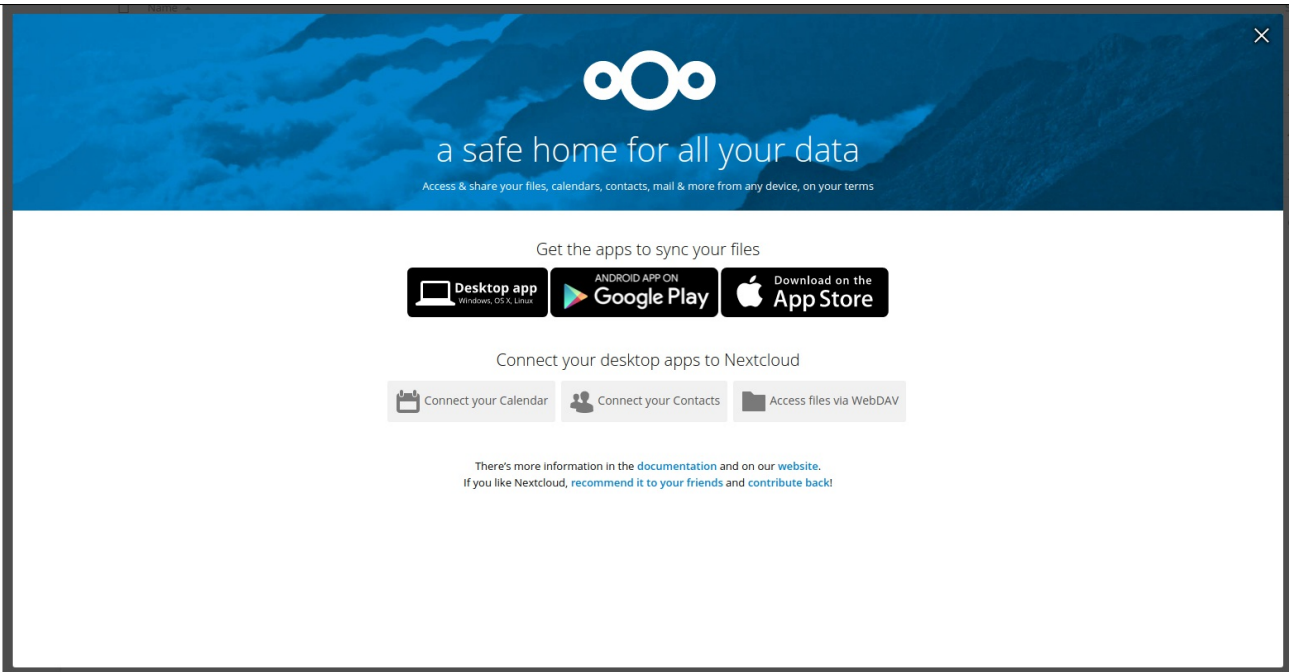
Kontakte, Kalender, Dateien

Um auf diese Dienste zugreifen zu können Nutzen sie folgenden Link:
(<https://acadia.kmu.schreib.at/>)[<http://acadia.kmu.schreib.at/>]

Melden sie sich auf dieser Seite mit ihren Informaitonen an



Danach werden sie von NextCloud durch eine installationsanleitung geführt:



Git

Rufen sie Gitlab über

(<https://git.acadia.kmu.schreib.at/>)[<http://git.acadia.kmu.schreib.at/>] auf. Geben sie ihre Benutzerdaten ein und Melden sie sich an:

Sign in

Register

Username or email

Password

Remember me [Forgot your password?](#)

Auf folgender Seite können sie nun Projekte und Gruppen erstellen, in welchen sie ihre Code-Repositories ablegen können:

Welcome to GitLab

Code, test, and deploy together



You can create a group for several dependent projects.
Groups are the best way to manage projects and members.

New group



You don't have access to any projects right now
You can create up to **10** projects.

New project

Sandstorm

Falls die passende Anwendung für sie noch nicht vorinstalliert ist, können Sie Sandstorm nutzen:

rufen sie dazu die domäne <https://bujuhu.sandcats.io:6080/> auf.

Melden sie sich mit ihrem LDAP Konto an:



Sign in

with LDAP

username ⓘ

password ⓘ

LOG IN











troubleshooting

Darauf hin können sie eigene Cloudanwendungen über ein Installationsmenü hinzufügen:










Apps Upload app

search

Most used

 Hacker CMS Markdown CMS	 Roundcube Email client	 GitLab Git hosting	 Rocket.Chat Chat app	 Collections Grain list sharing	 Wekan Kanban board	 Etherpad Document editor	 Davros File storage
---	--	--	--	--	--	---	---

All apps

 Install... from app market	 Collections Grain list sharing	 Davros File storage	 Etherpad Document editor	 GitLab Git hosting	 Hacker CMS Markdown CMS	 Rocket.Chat Chat app	 Roundcube Email client	 Wekan Kanban board
--	--	---	--	--	---	---	--	--

VoIP: Teamspeak

Um sich mit dem Unternehmens-Teamspeak server verbinden zu können, öffnen sie ihren teamspeak client und geben eine neue Verbindung zum Server **teamspeak.schreib.at** an.

Connect

Server Address:
teamspeak.schreib.at

Nickname: Server Password:
Juri

▼ More Connect In New Tab Cancel

Aufrufen der öffentlichen Unternehmenswebsite

Dazu muss einfach die öffentlich erreichbare URL <https://kmu.schreib.at> aufgerufen werden.

http://localhost:4000/NVS/5CHIF_20170403_Schreib/