

Realisierungsbericht

Status	In Prüfung
Projektname	Failover
Projektleiter	Fabian Haering
Auftraggeber	Daniel Schär
Autoren	Marc Binggeli, Abidin Vejseli, Fabian Haering, Siro Beck
Verteiler	Daniel Schär, Marc Binggeli, Abidin Vejseli, Fabian Haering, Siro Beck

Änderungskontrolle, Prüfung, Genehmigung

Version	Datum	Beschreibung, Bemerkung	Name oder Rolle

Definitionen und Abkürzungen

Begriff / Abkürzung	Bedeutung

Referenzen

Referenz	Titel, Quelle
[1]	
[2]	
[3]	

Inhaltsverzeichnis

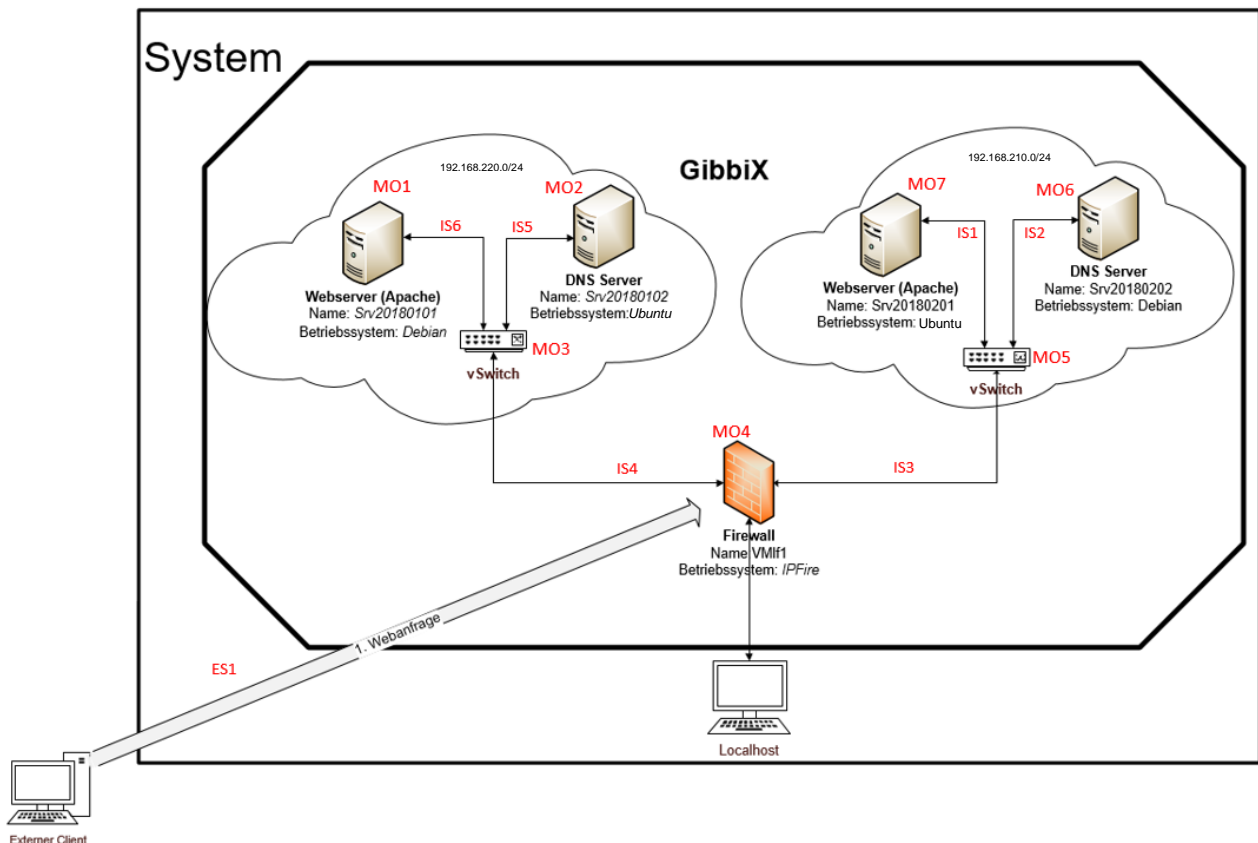
1	Technische Detailspezifikation	3
1.1	Systemdesign	3
1.1.1	Struktur	3
1.1.2	Beschreibung der Elemente	3
1.2	Schnittstellendefinitionen	4
1.3	Sicherheit (ISDS)	4
1.4	Anforderungszuordnung	4
2	Systemdokumentation	5
2.1	Konfigurations-Dokumentation	5
2.1.1	Konfiguration des Servers Srv20180101	5
2.1.1.1	Installation Apache2 Webserver	8
2.1.2	Konfiguration des Servers Srv20180102	9
2.1.2.1	Installation von Bind9 (DNS Dienst)	11
2.1.3	Konfiguration des Servers Srv20180201	15
2.1.4	Konfiguration des Servers Srv20180202	16
2.1.5	Konfiguration Firewall	17
2.2	Benutzerhandbuch	18
2.2.1	Systemübersicht	18
2.2.2	Anwenderfunktionalität	18
2.3	Supporthandbuch	20
2.3.1	Massnahmen bei Benutzerproblemen	20
2.3.2	Massnahmen bei technischen Problemen	21
2.3.3	Anhang zum Supporthandbuch	23
3	Systemtest	24
3.1	Testspezifikation	24
3.1.1	Kritikalität der Funktionseinheit	24
3.1.2	Testanforderungen	24
3.1.3	Testverfahren	24
3.1.4	Testkriterien	24
3.1.5	Testfälle	24
3.2	Testprozedur	26
3.2.1	Vorbereitung	26
3.2.2	Voraussetzungen:	26
3.2.3	Konfiguration:	26
3.2.4	Durchführung	27
3.2.5	Nachbearbeitung	28
3.3	Testprotokoll	29
3.3.1	Testobjekt	29
3.3.2	Testresultate	30
3.3.3	Testauswertung	30
4	Weiterführung der Projektplanung	31
4.1	Abgleich von Planung und tatsächlichem Verlauf der Phase Konzept	31
4.2	Aktualisierung der Risikosituation	32
4.3	Planung der nächsten Phase	33

1 Technische Detailspezifikation

1.1 Systemdesign

Durch unseren Änderungsantrag sind insgesamt ein Modul und eine Interne-, sowie Externe Schnittstelle weggefallen. Somit fehlen die zweite Firewall und die damit zusammenhängenden Schnittstellen. Zudem hat das Betriebssystem der Firewall auf IPFire und jenes der beiden DNS Server auf Ubuntu geändert. Der Rest vom System ist gleichgeblieben. Durch den Wegfall der zweiten Firewall kann zudem die Anforderung A2.3, welche im Konzeptbericht definiert wurde, nicht erfüllt werden.

1.1.1 Struktur



1.1.2 Beschreibung der Elemente

Module:

Webserver (Srv20180101):	OS: Debian,	IP: 192.168.220.50, Subnetz 255.255.255.0
DNS Server (Srv20180102):	OS: Ubuntu,	IP: 192.168.220.10, Subnetz 255.255.255.0
Firewall (VMIf1):	OS: IPFire,	IPs: 01Netz: 192.168.220.1 Subnetz 255.255.255.0 02Netz: 192.168.210.1 Subnetz 255.255.255.0 WAN: DHCP
Webserver (Srv20180201):	OS: Debian,	IP: 192.168.210.50, Subnetz 255.255.255.0
DNS Server (Srv20180202):	OS: Ubuntu,	IP: 192.168.210.10, Subnetz 255.255.255.0

1.2 Schnittstellendefinitionen

Externe Schnittstellen:

ES1: Firewall (Fw20180101) Port 80 und 443 für Webanfragen öffnen, 53 für DNS-Anfragen

Interne Schnittstellen:

IS1: Zuständig für Webanfragen/Webantworten (Ports: 80/443)

IS2: Zuständig für DNS-Anfragen/DNS-Antworten (Port: 53)

IS3: Zuständig für Webanfragen/Webantworten, DNS-Anfragen/DNS-Antworten (Ports: 53/80/443)

IS4: Zuständig für Webanfragen/Webantworten (Ports: 80/443)

IS5: Zuständig für DNS-Anfragen/DNS-Antworten (Port: 53)

IS6: Zuständig für Webanfragen/Webantworten, DNS-Anfragen/DNS-Antworten (Ports: 53/80/443)

1.3 Sicherheit (ISDS)

Da wir keine speziellen Datenschutz- und Sicherheitsanforderungen haben, mussten wir diese bei der Umsetzung nicht beachten.

1.4 Anforderungszuordnung

A Fo.- Nr.	Anforderung (Stichwort)	ES1	IS1	IS2	IS3	IS4	IS5	IS6	MO1	MO2	MO3	MO4	MO5	MO6	MO7
A1	Erreichbarkeit Webdienst		X	X	X	X	X	X	X	X	X	X	X	X	X
A1.1	Verfügbarkeit Webdienst			X	X	X	X		X	X				X	X
A2	System Redundant								X	X	X		X	X	X
A2.1	Hardware								X	X	X	X	X	X	X
A2.2	Ein produktives System		X	X	X				X	X	X	X	X	X	X
A2.3	Netzverkehr umleiten Firewall				X	X						X			
A2.4	Umleitung Webanfragen			X	X	X	X			X				X	
A3	Informieren über System	X	X	X	X	X	X	X	X	X	X	X	X	X	X
A3.1	Informieren über Firewalls											X			
A3.2	Schulung Konfiguration DNS									X				X	

2 Systemdokumentation

2.1 Konfigurations-Dokumentation

2.1.1 Konfiguration des Servers Srv20180101

In diesem Abschnitt beschreiben wir, wie wir den Server Srv20180101 erstellt und konfiguriert haben. Dieser Server dient in unserem System als Webserver. Wir haben den Webserver über den VMware Workstation Player 14 erstellt.

Das Debian ISO, welches wir bei der Installation verwenden, haben wir von der Webseite: <https://www.debian.org/distrib/> heruntergeladen. Dabei wählten wir das 64-Bit Netinst ISO.

Ein Installations-Image herunterladen

Abhängig von Ihrer Internet-Verbindung können Sie eines der folgenden Images herunterladen:

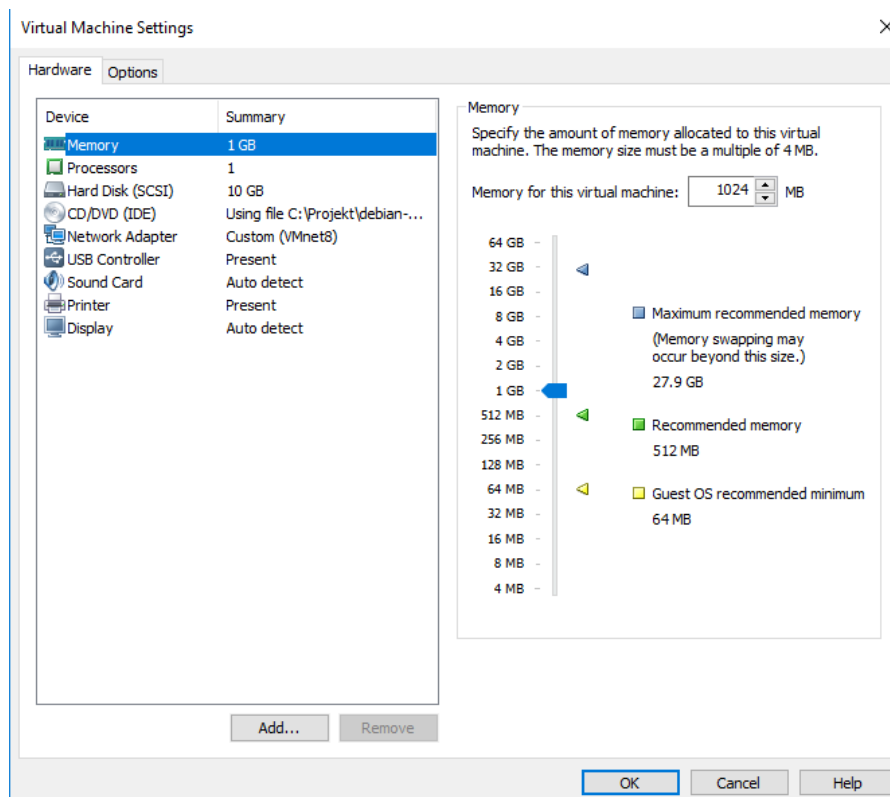
- Ein **kleines Installations-Image**: kann schnell heruntergeladen werden und sollte auf einen Wechseldatenträger aufgebracht werden. Um dies zu nutzen, benötigen Sie auf dem zu installierenden Rechner eine Internet-Verbindung.

 [64-Bit-PC Netinst-ISO](#), [32-Bit-PC Netinst-ISO](#)

- Ein größeres **vollständiges Installations-Image**: enthält mehr Pakete; dies macht es einfacher, einen Rechner ohne Internet-Verbindung zu installieren.

 [64-Bit-PC DVD-Torrents](#), [32-Bit-PC DVD-Torrents](#), [64-Bit-PC CD-Torrents](#), [32-Bit-PC CD-Torrents](#)

Beim Erstellen eines neuen Servers im VMware Workstation Player, klickten wir uns durch das Installationswizard. Nachdem wir den Servernamen auf Srv20180101 und den Standort des .ISO ausgewählt haben, haben wir folgende Hardwareeinstellungen vorgenommen.

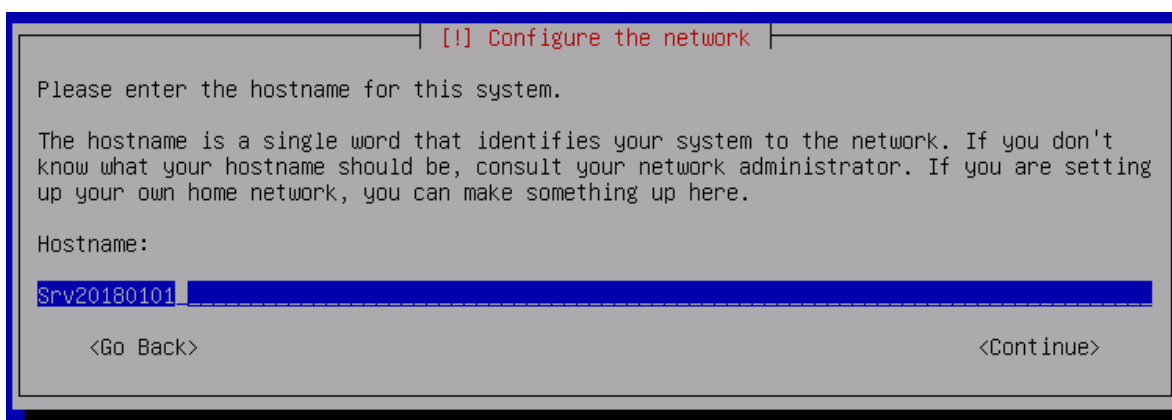


Danach kann man der Server starten und es erscheint die Startseite der Debian Installation. Wir wählten die normale Installationsmethode „Install“.



Bei der Installation haben wir folgende Einstellungen für die sprach- und regionalen Einstellungen vorgenommen.

Region/Tastatur	
Sprache	Englisch
Kontinent/Land	Europa/Schweiz
Tastaturlayout	Vereinigtes Königreich / Schweizerdeutsch



Als Hostnamen setzen wir Srv20180101.

Den Paketmanager und die IP Konfiguration haben wir folgendermassen eingestellt.

Paket Manager	
Land	Schweiz
Server	ftp.ch.debian.org
Proxy	Kein Proxy eingetragen
IP-Konfiguration	
IP-Adresse	192.168.220.50
Gateway	192.168.220.1
DNS-Server	192.168.220.10, 192.168.210.10
Subnetzmaske	255.255.255.0

2.1.1.1 Installation Apache2 Webserver

Bevor wir mit der Installation begonnen haben, haben wir die Paketlisten aktualisiert.

Dazu verwendeten wir folgende Befehle:

```
root@Srv20180101:~# apt update
```

```
root@Srv20180101:~# apt upgrade_
```

Danach haben wir als nächstes die «net-tools» heruntergeladen, damit wir den uns bekannten Linux Befehl ifconfig verwenden können.

```
root@Srv20180101:~# apt install net-tools
```

Danach installierten wir den apache Server.

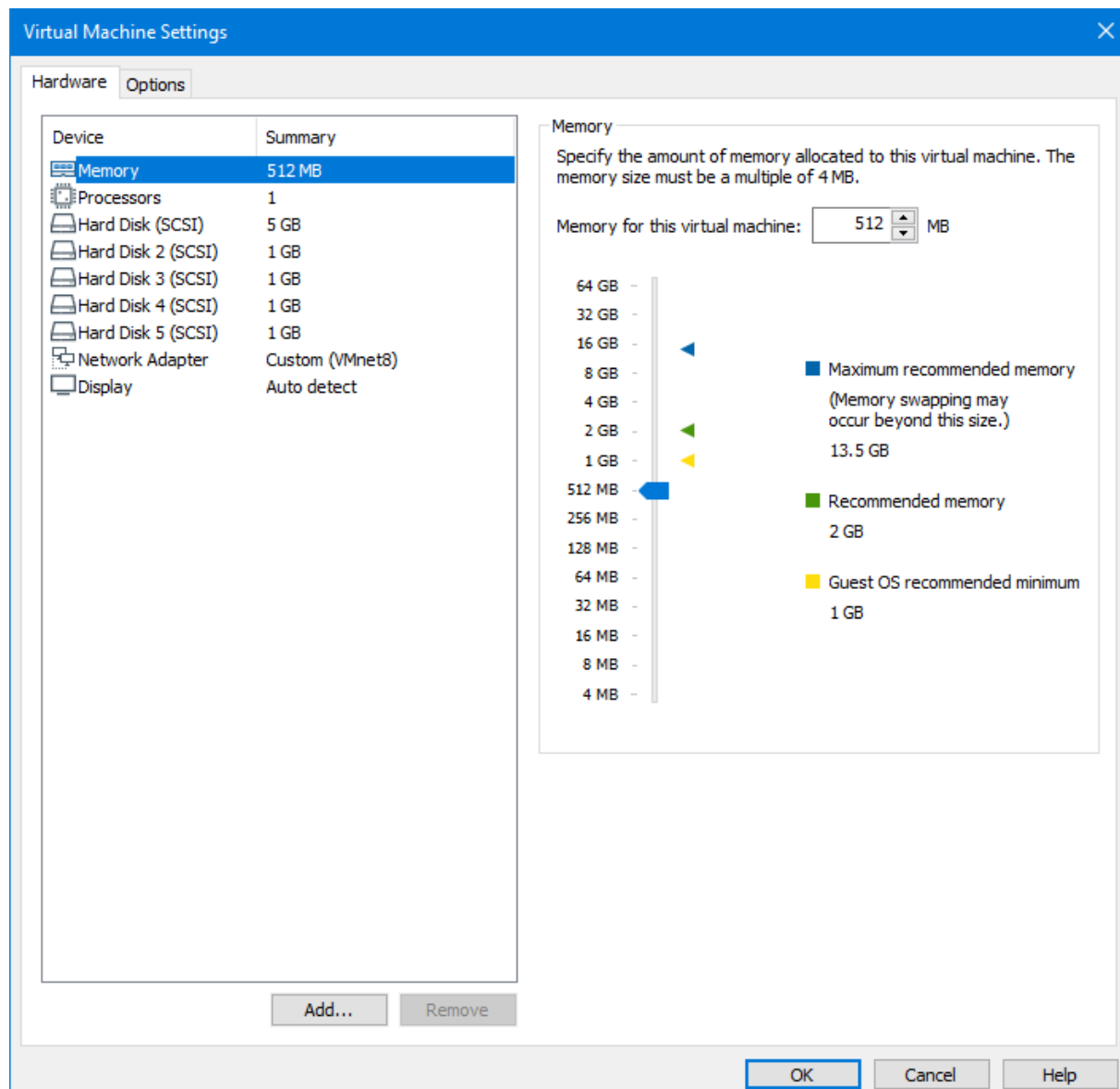
```
root@Srv20180101:~# apt install apache2
```

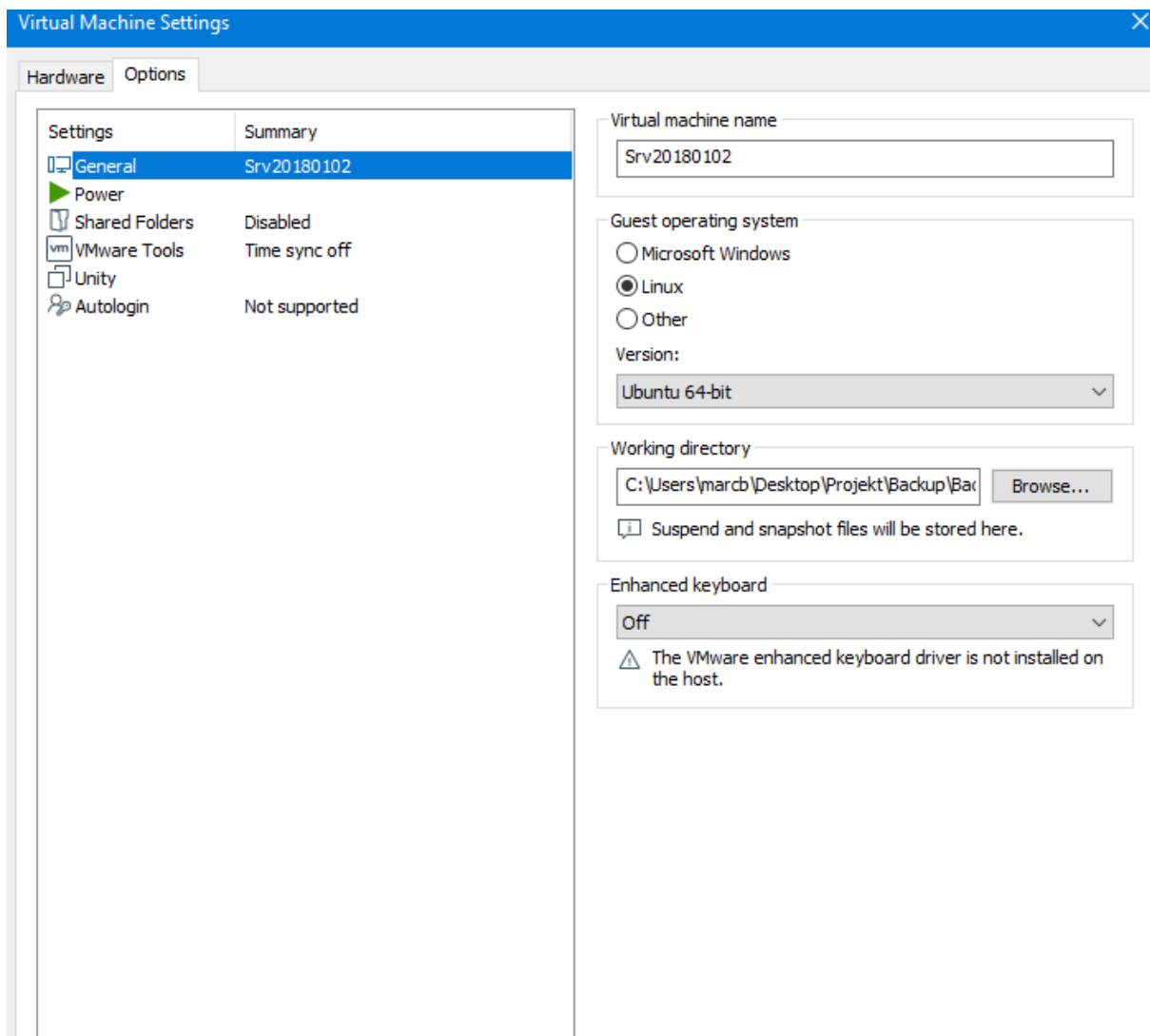
Damit ist die Konfiguration des Webserver abgeschlossen.

2.1.2 Konfiguration des Servers Srv20180102

Die Grundlage für diesen Server bietet die virtuelle Maschine vmls1, welche auch auf der Gibbix vorhanden ist. Damit wir nicht die Maschine auf der Gibbix verwenden, haben wir das ZIP File der virtuellen Maschine; „vmls1.7z.001“ vom Pfad /sh-smartlearn/3_archive geholt und entpackt.

Die genauen Einstellungen, welche wir im VMware Workstation Player vorgenommen haben, sind auf diesem Screenshot ersichtlich. Wichtig ist, dass sich dieser Server im VMnet 8 befindet und dass der Hostname geändert wird.





Den Hostnamen haben wir zudem in der Datei /etc/hostname auf Srv20180102 geändert.
Zudem haben wir folgende IP Einstellungen gesetzt:

IP-Konfiguration	
IP-Adresse	192.168.220.10
Gateway	192.168.220.1
DNS-Server	192.168.220.10, 192.168.210.10
Subnetzmaske	255.255.255.0

2.1.2.1 Installation von Bind9 (DNS Dienst)

Wir verwenden Bind9 als DNS Server. Mit diesem DNS Server haben wir bereits im Modul 239 gearbeitet. Bevor wir mit der Installation von Bind9 angefangen haben, haben wir die Paketlisten und alle dazugehörigen Pakete aktualisiert.

```
root@Srv20180102:~# apt update_  
root@Srv20180102:~# apt upgrade_
```

Wir installieren als Vorbereitung zur Installation von Bind9 ein Kompilierungsprogramm.

```
root@Srv20180102:~# sudo apt-get install build-essential checkinstall
```

Danach holen wir uns mit dem Befehl wget das Bind9 Paket von der Herstellerseite.

```
root@Srv20180102:~# wget --no-check-certificate \ https://www.isc.org/downloads/file/bind-9-11-0/?version=tar-gz -O BIND9.11.0.tar.gz
```

Nachdem wir es auf unsere virtuelle Maschine geholt haben, entpacken wir das Paket.

```
root@Srv20180102:~# tar -xvzf Bind9.11.0.tar.gz_
```

Bevor wir mit der Installation fortfahren, installieren wir fehlende Abhängigkeiten, welche von Bind benötigt werden, um das Paket zu Kompilieren und installieren.

```
root@Srv20180102:~# sudo apt-get install libssl-dev libxml2-dev
```

Mit folgendem Befehl haben wir den Installationsort von Bind festgelegt. Die Konfigurationsdateien werden alle in einem Unterverzeichnis von /etc abgelegt.

```
root@Srv20180102:~# ./configure --sysconfdir=/etc/bind9/_
```

Das eigentliche Kompilieren machen wir mir mit dem make Befehl.

```
root@Srv20180102:~# make_
```

Zum Abschluss der Installation führten wir den Checkinstall Befehl aus.

```
root@Srv20180102:~# sudo checkinstall
```

Nachdem dieser Befehl ausgeführt worden ist, ist Bind9 installiert. Damit der DNS Server schlussendlich auch funktioniert, haben wir Dateien für die Konfiguration angelegt.

Wir haben folgende Dateien im Verzeichnis /etc/bind9/ erstellt:

- db.192.168.210
- db.192.168.220
- db.com.failover.lan
- named.conf
- named.conf.local
- named.conf.options

Inhalt db.192.168.220

```
;
; Zonendatei fuer 220.168.192.in-addr.arpa.
;
$TTL      3600
@         IN      SOA      Srv20180102.lan.failover.com.  root.failover.com. (
                                1
                                1H
                                2H
                                1D
                                1H )

@         IN      NS       Srv20180102.lan.failover.com.
1         IN      PTR      vmlf1.lan.failover.com.
10        IN      PTR      Srv20180102.lan.failover.com.
50        IN      PTR      Srv20180101.lan.failover.com.
```

Zonendatei db.192.168.220

```
;
; Zonendatei fuer 210.168.192.in-addr.arpa.
;
$TTL      3600
@         IN      SOA      Srv20180202.lan.failover.com.  root.failover.com. (
                                1
                                1H
                                2H
                                1D
                                1H )

@         IN      NS       Srv20180202.lan.failover.com.
1         IN      PTR      vmlf1.lan.failover.com.
10        IN      PTR      Srv20180202.lan.failover.com.
50        IN      PTR      Srv20180201.lan.failover.com.
```

Zonendatei db.com.failover.lan

```
;  
;  
;  
$TTL      3600  
@         IN      SOA      Srv20180102.lan.failover.com.  root.failover.com (   
                          1  
                          1H  
                          2H  
                          1D  
                          1H )  
  
@         IN      NS       Srv20180102.lan.failover.com.  
vmlf1     IN      A        192.168.220.1  
vmlf1     IN      A        192.168.210.1  
Srv20180101 IN      A        192.168.220.50 ;Webserver1 1  
Srv20180102 IN      A        192.168.220.10 ; DNS1  
Srv20180101 IN      A        192.168.210.50 ; Webserver1 2  
Srv20180202 IN      A        192.168.210.10 ; DNS2  
Srv20180201 IN      A        192.168.210.50 ; Webserver2 1  
Srv20180201 IN      A        192.168.220.50 ; Webserver2 2
```

Inhalt named.conf Datei

```
// Konfigurationsdatei  
  
include "/etc/bind9/named.conf.options";  
include "/etc/bind9/named.conf.local";
```

Inhalt named.conf.options Datei

```
options {
    // IPv4
    listen-on port 53 {
        any;
    };

    // IPv6
    listen-on-v6 {
        none;
    };

    forwarders {
        8.8.8.8;
        8.8.4.4;
    };

    allow-query {
        any;
    };

    allow-recursion {
        127.0.0.1;
        192.168.210.0/24;
        192.168.220.0/24;
    };
};
```

Inhalt named.conf.local Datei

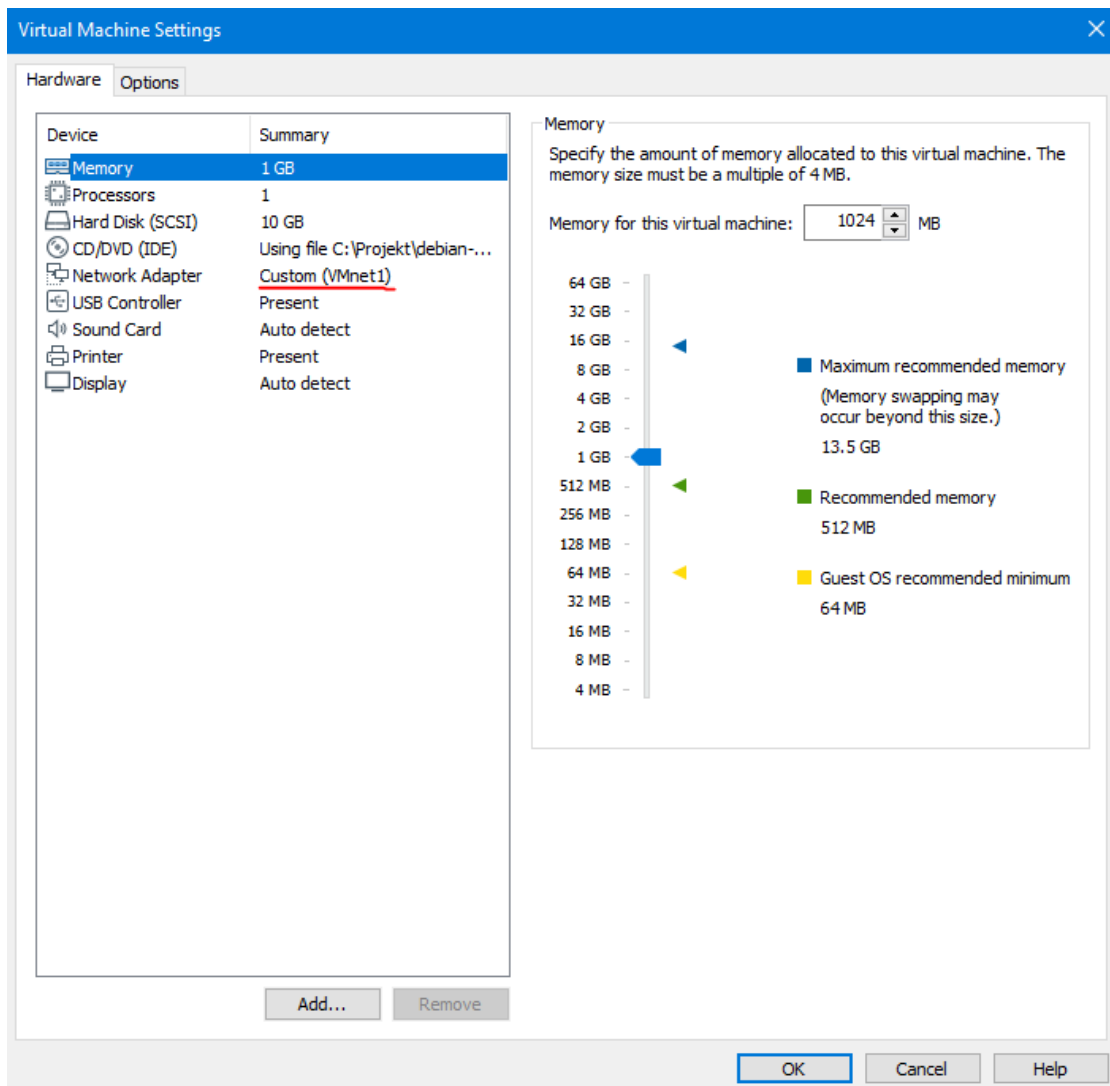
```
zone "lan.failover.com" {
    type master;
    notify no;
    file "/etc/bind9/db.com.failover.lan";
};

zone "220.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind9/db.192.168.220";
};

zone "210.168.192.in-addr.arpa" {
    type master;
    notify no;
    file "/etc/bind9/db.192.168.210";
};
```

2.1.3 Konfiguration des Servers Srv20180201

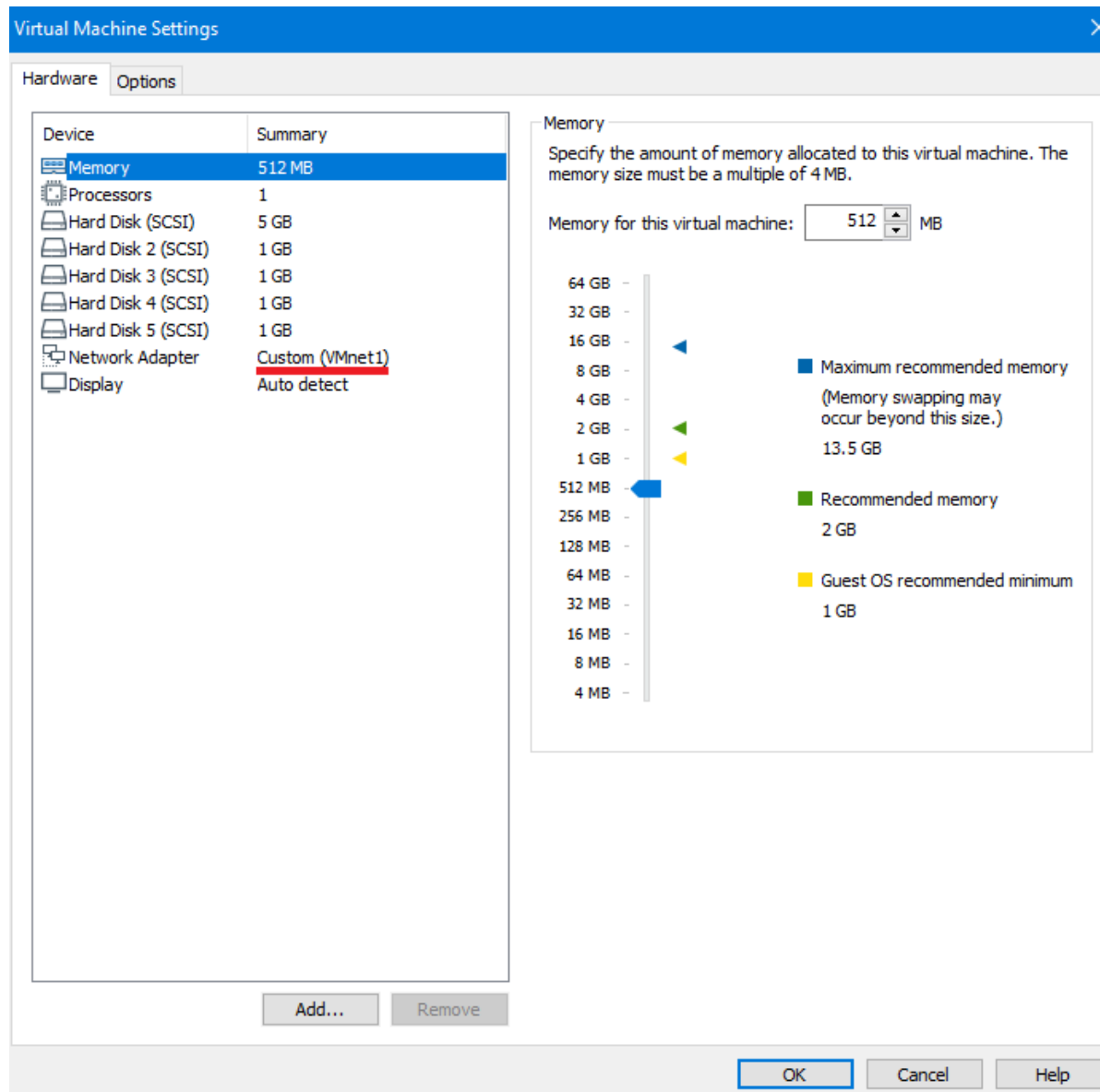
Dieser Server ist analog dem Server Srv20180201, dem anderen Webserver, konfiguriert, welche weiter oben im Dokument beschrieben ist. Die zwei Unterschiede zwischen den beiden Servern sind das VMnet und die IP Einstellungen.



IP-Konfiguration	
IP-Adresse	192.168.210.50
Gateway	192.168.210.1
DNS-Server	192.168.220.10, 192.168.210.10
Subnetzmaske	255.255.255.0

2.1.4 Konfiguration des Servers Srv20180202

Dieser Server wurde bis auf wenige Einstellungen analog dem Server Srv20180102, dem anderen DNS Server konfiguriert. Dieser Server befindet sich im VMnet 1 und hat deshalb eine andere Netzwerkkonfiguration.

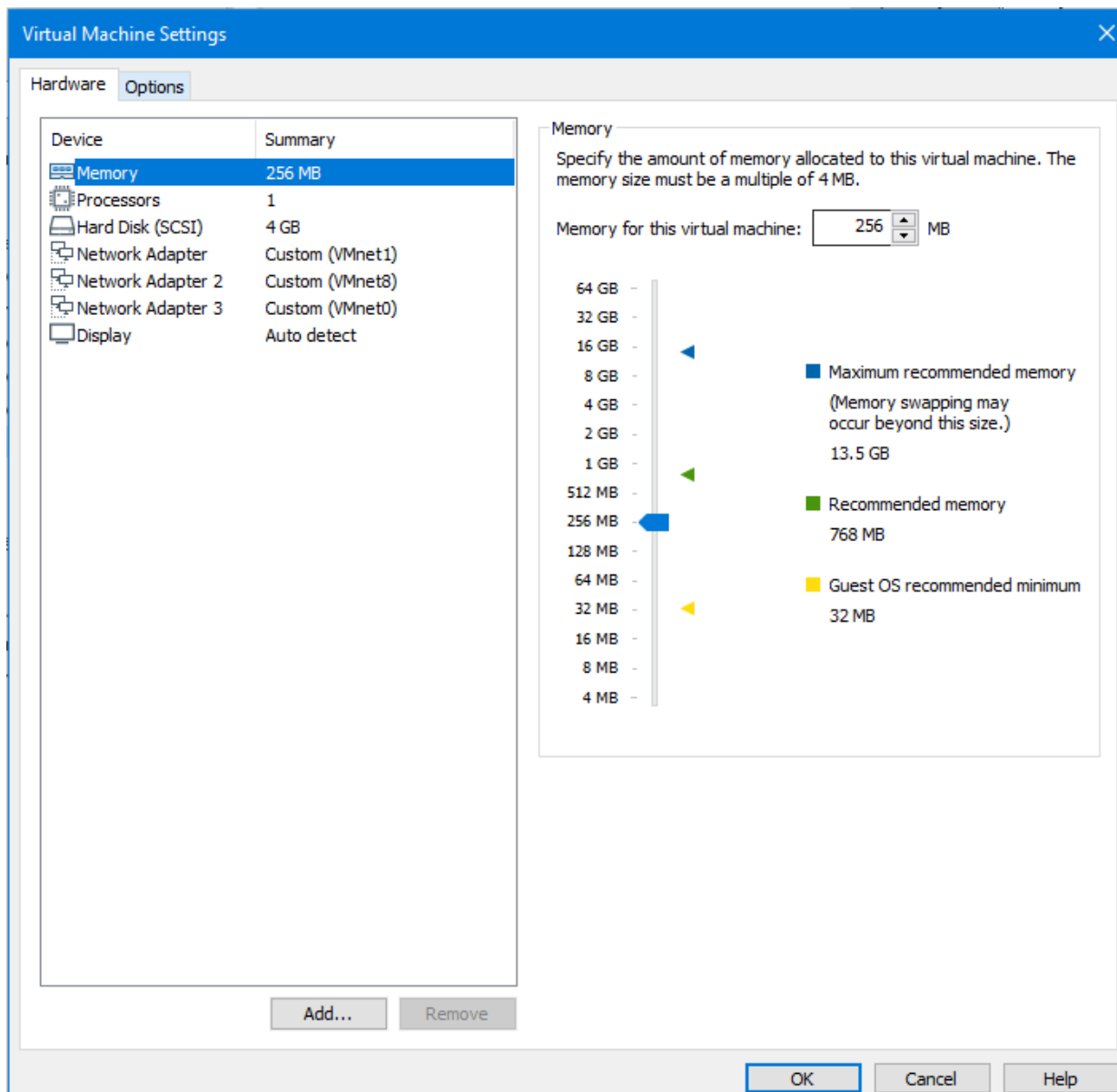


IP-Konfiguration	
IP-Adresse	192.168.210.10
Gateway	192.168.210.1
DNS-Server	192.168.220.10, 192.168.210.10
Subnetzmaske	255.255.255.0

Die Konfiguration der Zonendateien und die Installation von Bind 9 erfolgte wie beim anderen DNS Server.

2.1.5 Konfiguration Firewall

Das Grundgerüst der Firewall ist die virtuelle Maschine vmlf1, welche auch auf der Gibbix vorhanden ist. Wir haben das ZIP File vmlf1.7z.001 vom Pfad /sh-smartlearn/3_archive geholt und entpackt.



Die genaue Konfiguration mit den verschiedenen Netzwerkadaptern ist im Printscreen zu sehen.

An den Detailsinstellungen haben wir keine Änderung vorgenommen. Wir haben zum Beispiel der IP Konfiguration nicht verändert, da diese bereits unseren Vorstellungen entspricht.

2.2 Benutzerhandbuch

2.2.1 Systemübersicht

Das Ziel dieses Systems ist die Verfügbarkeit des Webservers und diese des DNS Servers zu erhöhen. Die Hauptfunktion dieses Systems besteht darin, dass ein DNS Server die Namensauflösung vom anderen DNS Server übernimmt, falls dieser ausfällt. Zudem werden die Anfragen auf den anderen Webserver umgeleitet, falls ein Webserver ausfällt.

Die Struktur unserer Systemumgebung, sowie allgemeine Informationen zur Sicherheit, dem Datenschutz und Anwenderrollen sind unter Punkt 1.1 Systemdesign zu finden.

2.2.2 Anwenderfunktionalität

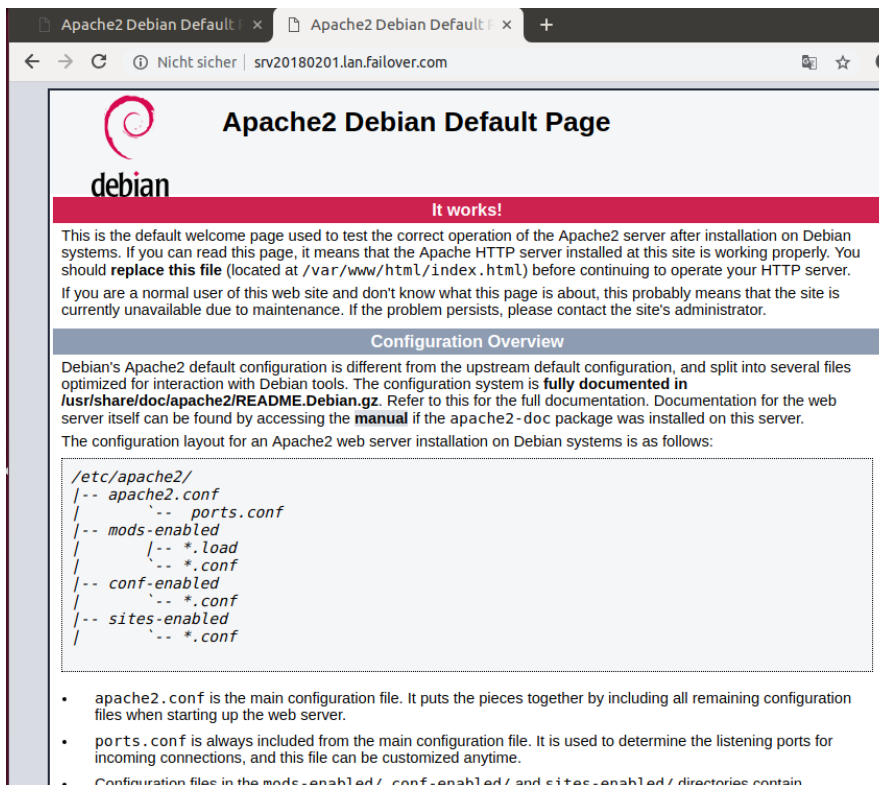
Der Benutzer kann den/die DNS Server starten, damit die Namensauflösung im System funktioniert. Dies kann er mit dem Befehl `named -g` tun.

```
root@Srv20180102:~# named -g_
```

Dieses Bild zeigt die erwartete Ausgabe beim Starten des DNS Servers

[illegible]

Zugriff auf Webserver



Sobald mindestens ein Web- und DNS-Server und die Firewall gestartet sind, ist es dem Benutzer möglich via einen Browser auf einen Webserver zuzugreifen. Im obigen Screenshot ist die erwartete Ausgabe beim Zugriff auf den Webserver zu sehen.

Neben dem Zugriff auf einen Webserver hat der Benutzer die Möglichkeit, eine IP-Adresse auf einen Namen aufzulösen, oder eine IP-Adresse auf einen Namen. Dazu muss mindestens ein DNS Server gestartet sein.

```
root@Srv20180102:~# nslookup 192.168.220.50
50.220.168.192.in-addr.arpa      name = Srv20180101.lan.failover.com.

root@Srv20180102:~# nslookup Srv20180101.lan.failover.com
Server:      127.0.0.1
Address:     127.0.0.1#53

Name:   Srv20180101.lan.failover.com
Address: 192.168.220.50
Name:   Srv20180101.lan.failover.com
Address: 192.168.210.50
```

Allfällige Massnahmen bei Technischen- und Benutzerproblemen sind unter Punkt 2.3 Supporthandbuch dokumentiert.

2.3 Supporthandbuch

2.3.1 Massnahmen bei Benutzerproblemen

Der DNS Server kann mit dem Befehl `named -g` gestartet werden. Es spielt keine Rolle, in welchem Verzeichnis der DNS Server gestartet wird, wichtig ist nur, dass er nur einmal gestartet wird.

```
root@Srv20180102:~# named -g_
```














Nachdem der DNS Server gestartet wurde, sollte folgendes Fenster erscheinen.

```

28-Nov-2018 14:53:19.193 automatic empty zone: 123.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 124.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 125.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 126.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 127.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 0.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 127.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 254.169.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 2.0.192.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 100.51.198.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 113.0.203.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 255.255.255.255.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: D.F.IP6.ARPA
28-Nov-2018 14:53:19.195 automatic empty zone: 8.E.F.IP6.ARPA
28-Nov-2018 14:53:19.195 automatic empty zone: 9.E.F.IP6.ARPA
28-Nov-2018 14:53:19.195 automatic empty zone: A.E.F.IP6.ARPA
28-Nov-2018 14:53:19.195 automatic empty zone: B.E.F.IP6.ARPA
28-Nov-2018 14:53:19.196 automatic empty zone: 8.B.D.0.1.0.0.2.IP6.ARPA
28-Nov-2018 14:53:19.196 automatic empty zone: EMPTY.AS112.ARPA
28-Nov-2018 14:53:19.196 'max-cache-size 90%' - setting to 423MB (out of 470MB)
28-Nov-2018 14:53:19.197 configuring command channel from '/etc/bind9/rndc.key'
28-Nov-2018 14:53:19.197 couldn't add command channel 127.0.0.1#953: file not found
28-Nov-2018 14:53:19.198 configuring command channel from '/etc/bind9/rndc.key'
28-Nov-2018 14:53:19.198 couldn't add command channel ::1#953: file not found
28-Nov-2018 14:53:19.198 not using config file logging statement for logging due to -g option
28-Nov-2018 14:53:19.199 managed-keys-zone: loaded serial 0
28-Nov-2018 14:53:19.202 zone lan2.failover.com/IN: loaded serial 1
28-Nov-2018 14:53:19.202 zone 220.168.192.in-addr.arpa/IN: loaded serial 1
28-Nov-2018 14:53:19.203 zone 210.168.192.in-addr.arpa/IN: loaded serial 1
28-Nov-2018 14:53:19.204 zone lan1.failover.com/IN: loaded serial 1
28-Nov-2018 14:53:19.204 zone staff.liftup.com/IN: loaded serial 1
28-Nov-2018 14:53:19.204 all zones loaded
28-Nov-2018 14:53:19.205 running

```

Falls der Benutzer eine Virtuelle Maschine nicht starten kann, kann er die Ordnerstruktur der Maschine anschauen gehen. Dort sollten sich jetzt diverse Ordner befinden, welche mit .lck enden. Diese Ordner können gelöscht werden. Danach sollte das Starten der virtuellen Maschinen wieder möglich sein.

 Srv20180101.vmx.lck	28.11.2018 14:38	Dateiordner	
 Srv20180101.nvram	27.11.2018 20:08	NVRAM-Datei	9 KB
 Srv20180101.vmdk	28.11.2018 12:42	VMware virtual dis...	1 KB
 Srv20180101.vmsd	31.10.2018 14:00	VMSD-Datei	0 KB
 Srv20180101.vmx	28.11.2018 13:27	VMware virtual m...	3 KB
 Srv20180101.vmx.f	31.10.2018 14:00	VMXF-Datei	1 KB
 Srv20180101-s001.vmdk	28.11.2018 13:27	VMware virtual dis...	1'852'480 KB
 Srv20180101-s002.vmdk	28.11.2018 13:27	VMware virtual dis...	6'912 KB
 Srv20180101-s003.vmdk	31.10.2018 14:28	VMware virtual dis...	448 KB
 vmware.log	28.11.2018 13:27	Textdokument	260 KB
 vmware-0.log	27.11.2018 22:00	Textdokument	240 KB
 vmware-1.log	27.11.2018 21:47	Textdokument	240 KB
 vmware-2.log	27.11.2018 21:33	Textdokument	241 KB

2.3.2 Massnahmen bei technischen Problemen

DNS Server:

Wenn beim Starten eines DNS Servers Fehler erscheinen, besteht die Möglichkeit den Sever mit der Tastenkombination CTRL und C abzuschalten.

Als nächstes können die Ausgaben des DNS Servers angeschaut werden. Diese sind normalerweise folgendermassen aufgebaut.

```

28-Nov-2018 14:53:19.193 automatic empty zone: 123.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 124.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 125.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 126.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 127.100.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 0.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 127.IN-ADDR.ARPA
28-Nov-2018 14:53:19.193 automatic empty zone: 254.169.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 2.0.192.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 100.51.198.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 113.0.203.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 255.255.255.255.IN-ADDR.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IPv6.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IPv6.ARPA
28-Nov-2018 14:53:19.194 automatic empty zone: D.F.IPv6.ARPA
28-Nov-2018 14:53:19.195 automatic empty zone: 8.E.F.IPv6.ARPA
28-Nov-2018 14:53:19.195 automatic empty zone: 9.E.F.IPv6.ARPA
28-Nov-2018 14:53:19.195 automatic empty zone: A.E.F.IPv6.ARPA
28-Nov-2018 14:53:19.195 automatic empty zone: B.E.F.IPv6.ARPA
28-Nov-2018 14:53:19.196 automatic empty zone: 8.B.D.0.1.0.0.2.IPv6.ARPA
28-Nov-2018 14:53:19.196 automatic empty zone: EMPTY.AS112.ARPA
28-Nov-2018 14:53:19.196 'max-cache-size 90%' - setting to 423MB (out of 470MB)
28-Nov-2018 14:53:19.197 configuring command channel from '/etc/bind9/rndc.key'
28-Nov-2018 14:53:19.197 couldn't add command channel 127.0.0.1#953: file not found
28-Nov-2018 14:53:19.198 configuring command channel from '/etc/bind9/rndc.key'
28-Nov-2018 14:53:19.198 couldn't add command channel ::1#953: file not found
28-Nov-2018 14:53:19.198 not using config file logging statement for logging due to -g option
28-Nov-2018 14:53:19.199 managed-keys-zone: loaded serial 0
28-Nov-2018 14:53:19.202 zone lan2.failover.com/IN: loaded serial 1
28-Nov-2018 14:53:19.202 zone 220.168.192.in-addr.arpa/IN: loaded serial 1
28-Nov-2018 14:53:19.203 zone 210.168.192.in-addr.arpa/IN: loaded serial 1
28-Nov-2018 14:53:19.204 zone lan1.failover.com/IN: loaded serial 1
28-Nov-2018 14:53:19.204 zone staff.liftup.com/IN: loaded serial 1
28-Nov-2018 14:53:19.204 all zones loaded
28-Nov-2018 14:53:19.205 running

```

In den Ausgaben des DNS Servers sollten eine oder mehrere Fehlermeldungen sichtbar sein, falls der Server nicht funktioniert. Meistens sind die Dateien, unter anderem die Zonendateien, welche der DNS Server beim Starten lädt, die Fehlerursache.

Diese Dateien befinden sich im Verzeichnis `/etc/bind9/`. Der Wechsel in dieses Verzeichnis ist via `cd /etc/bind9/` möglich.

```
root@Srv20180102:~#  
root@Srv20180102:~# cd /etc/bind9/  
root@Srv20180102:/etc/bind9#
```

Mit dem Befehl `ls` sind alle Dateien in diesem Verzeichnis sichtbar.

```
root@srv20100102:/etc/bind9# ls
bind.keys          db.192.168.220     db.com.failover.lan2  db.root            named.conf.local
db.192.168.210     db.com.failover.lan1  db.com.liftup.lan.save  named.conf          named.conf.options
```

Aus der Fehlermeldung des DNS Servers ist der Name des Dokumentes ersichtlich. Um das Dokument zu öffnen und den Fehler zu korrigieren kann man das Dokument mit dem Befehl `sudo nano «Dokumentname»` öffnen.

```
root@Srv20180102:/etc/bind9# nano db.192.168.220
```

Webserver:

Falls Probleme beim Webserver auftreten, besteht die Möglichkeit die IP-Adresse des Webserver zu überprüfen. Dies sollte im ersten Schritt gemacht werden.

Um die Überprüfung zu machen, dient der Befehl `ifconfig`. Nachdem dieser Befehl eingegeben wurde, sollte folgende Konsolenausgabe erscheinen.

```
root@Srv20180101:~# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.220.50 netmask 255.255.255.0 broadcast 192.168.220.255
    inet6 fe80::20c:29ff:fe3d:34a7 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:cd:34:a7 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 293 bytes 17788 (17.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 186 bytes 18130 (17.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 186 bytes 18130 (17.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Falls die IP-Adresse übereinstimmt, mit der IP-Adresse, welche im Browser eingegeben wurde, kann man als nächstes überprüfen, ob der Webserver via PING erreichbar ist. Dazu öffnet man auf Windows ein CMD Fenster. Auf Linux kann man den Befehl auf der Konsole eingeben.

ping IP-Webserver, beispielsweise ping 192.168.220.50

```
root@Srv20180102:/etc/bind9# ping 192.168.220.50
PING 192.168.220.50 (192.168.220.50) 56(84) bytes of data:
64 bytes from 192.168.220.50: icmp_seq=1 ttl=64 time=0.501 ms
64 bytes from 192.168.220.50: icmp_seq=2 ttl=64 time=0.283 ms
```

Wenn die IP-Adresse im Browser anders ist, als diese, welche mit dem Befehl `ifconfig` angezeigt wird, muss die IP-Adresse im Browserfeld geändert werden und danach sollte das Problem gelöst sein.

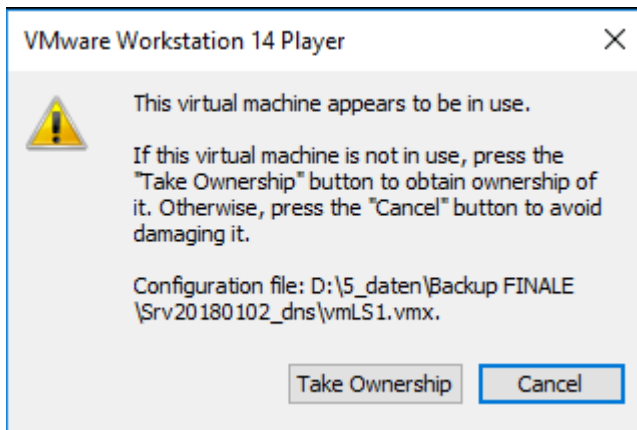
Neben dem PING Befehl auch den `Nslookup` Befehl, um die Namensauflösung des DNS Servers zu testen. `Nslookup` IP-Adresse des Servers, beispielsweise `nslookup 192.168.220.50`

Falls die `Nslookup` Anfrage fehlschlägt, besteht das Problem nicht beim Web-, sondern beim DNS Server.

```
root@Srv20180102:/etc/bind9# nslookup 192.168.220.50
50.220.168.192.in-addr.arpa      name = Srv20180101.lan.failover.com.
```

2.3.3 Anhang zum Suppothandbuch

Fehlermeldungen



Folgendes Bild zeigt eine mögliche Fehlermeldung, welche erscheinen kann, falls der Benutzer die virtuelle Maschine starten will. Die Ursache ist, dass die virtuelle Maschine nicht korrekt heruntergefahren wurde. Lösungsmassnahmen sind unter Punkt 1.3.1 Massnahmen bei Benutzerproblemen beschrieben.

```
root@Srv20180102:/etc/bind9# nslookup 192.168.220.50
;; connection timed out; no servers could be reached
```

Dieses Bild zeigt eine Fehlermeldung beim Versuch den Befehl nslookup auszuführen. Die Ursache ist, dass kein DNS Server gestartet ist oder ein falscher DNS Server eingetragen ist. Die erste Lösungsmassnahme ist, den DNS Server zu starten, falls keiner gestartet ist. Zudem kann man überprüfen, ob der richtige DNS Server hinterlegt ist. Dazu öffnet man in Linux die Interfaces Datei. nano /etc/network/interfaces.

3 Systemtest

3.1 Testspezifikation

3.1.1 Kritikalität der Funktionseinheit

Wir haben mehrere Testfälle, bei denen die Kritikalität bestimmt ist. Funktioniert ein Testfall nicht, wird anhand der Kritikalität entschieden, ob eine Abnahme trotz Fehlfunktion stattfinden kann oder nicht. Testfälle, die mit einer hohen Kritikalität definiert sind, müssen zwingend einwandfrei funktionieren.

3.1.2 Testanforderungen

Die Tests werden unter normalen Laufbedingungen getestet. Jedoch werden in vereinzelt Fällen Komponenten vom Netz genommen, um einen Ausfall zu simulieren. Dies hat bei uns den Vorteil, dass wir den Failover Prozess prüfen können.

3.1.3 Testverfahren

Jeder Test durchläuft 3 Abschnitte (Vorbereitung, Durchführung und Auswertung). Die Testfälle sind daher in 3 Teile gegliedert. Die Schritte werden in den einzelnen Testfällen genauer beschrieben.

3.1.4 Testkriterien

Abdeckungsgrad:

Die Testfälle sind darauf abgestimmt alle Anforderungen auf ihre Funktionalität zu testen. Es wird festgelegt, wie breit zu testen ist, um die Tauglichkeit des Testobjekts sicherzustellen.

Checklisten:

Die dazugehörigen Checklisten befinden sich direkt in den Testfällen falls benötigt. Hier wird auf die für den Test nötigen Checklisten hingewiesen.

Ende-Kriterien:

Sobald alle Checklistenpunkte das erwünschte Resultat ergeben, gilt der Testfall als erfüllt. Der Testfall muss genau nach den Vorgaben abgearbeitet werden, ansonsten kann man den Fall nicht nachvollziehen.

3.1.5 Testfälle

Wichtig: Die Tests funktionieren nur mit einem Windows Betriebssystem. Will man die Tests mit Linux machen, muss man anstelle von CMD einen Terminal oder die Shell benutzen.

Durch unsere Änderungen am System entsprechen die Testfälle nicht mehr dem Testkonzept, das wir in der Phase Konzeptionierung definiert haben.

NR	1
Kritikalität	Hoch
Anwendungsfall	Alle Server sind erreichbar (srv20180101, srv20180102, srv20180201, srv20180202)
Ausgangssituation	Ein Testgerät innerhalb des Netzes führt ein Ping auf alle Server unserer Umgebung durch. Dies wird jeweils aus dem Lan1 und dem Lan2 gemacht.
Erwartetes Ergebnis	Alle Server (srv20180101, srv20180102, srv20180201, srv20180202) werden antworten
Benötigte Tools/Apps	<ul style="list-style-type: none">- CMD- ping

NR	2
Kritikalität	Hoch
Anwendungsfall	DNS Server (srv20180102, srv20180202) gibt den Namen des Servers zurück.
Ausgangssituation	Ein Testgerät innerhalb des Netzes macht eine Nslookup-Anfrage auf die Webserver (srv20180101, srv20180201). Dies wird jeweils aus dem Lan1 und dem Lan2 gemacht.
Erwartetes Ergebnis	Die Anfrage wird den Namen der Server zurückgeben.
Benötigte Tools/Apps	<ul style="list-style-type: none">- CMD- Nslookup

NR	3
Kritikalität	Hoch
Anwendungsfall	Webserver(srv20180101, srv20180201) sind per IP erreichbar.
Ausgangssituation	Ein Testgerät innerhalb des Netzes wird mit einem Internet Browser (Chrome) die IP des Webserver (srv20180101, srv20180201) aufrufen. Dies wird jeweils aus dem Lan1 und dem Lan2 gemacht.
Erwartetes Ergebnis	Die Webseite des Webserver wird angezeigt.
Benötigte Tools/Apps	<ul style="list-style-type: none">- Chrome

NR	4
Kritikalität	Hoch
Anwendungsfall	Webserver (srv20180101, srv20180201) sind per DNS Name erreichbar.
Ausgangssituation	Ein Testgerät innerhalb des Netzes wird mit einem Internet Browser (Chrome) DNS Name des Webserver (srv20180101, srv20180201) aufrufen. Jeweils aus dem Lan1 und aus dem Lan2.
Erwartetes Ergebnis	Die Webseite des Webserver wird angezeigt.
Benötigte Tools/Apps	<ul style="list-style-type: none">- Chrome

NR	5
Kritikalität	Hoch
Anwendungsfall	Webserver (srv20180101, srv20180201) ist per DNS Name erreichbar trotz Ausfall einer der Webserver (srv20180101, srv20180201).
Ausgangssituation	Ein Testgerät innerhalb des Netzes wird mit einem Internet Browser (Chrome) DNS Name des Webserver (srv20180101, srv20180201) aufrufen. Jeweils aus dem Lan1 und aus dem Lan2. Einer der beiden Webserver (srv20180101, srv20180201) wird ausgeschaltet. Der Test beinhaltet zwei Durchläufe. Da beide einmal ausgeschaltet sein müssen.
Erwartetes Ergebnis	Die Webseite des Webserver wird angezeigt.
Benötigte Tools/Apps	<ul style="list-style-type: none">- Chrome

NR	6
Kritikalität	Hoch
Anwendungsfall	Webserver (srv20180101, srv20180201) ist per DNS Name erreichbar trotz Ausfall einer der DNS Server (srv20180102, srv20180202).
Ausgangssituation	Ein Testgerät innerhalb des Netzes wird mit einem Internet Browser (Chrome) DNS Name des Webserver (srv20180101, srv20180201) aufrufen. Jeweils aus dem Lan1 und aus dem Lan2. Einer der beiden DNS Server (srv20180102, srv20180202) wird ausgeschaltet. Der Test beinhaltet 2 Durchläufe. Da beide einmal ausgeschaltet sein müssen.
Erwartetes Ergebnis	Die Website des Webserver wird Angezeigt.
Benötigte Tools/Apps	- Chrome

3.2 Testprozedur

Die Nummer referenziert auf die Testfälle vom Punkt 4.1.5.

Die Tests sind der Reihe nach von Nummer eins bis sechs abzuarbeiten. Funktioniert der erste Testfall nicht, funktionieren auch die nachfolgenden Testfälle nicht korrekt.

3.2.1 Vorbereitung

Nr.	Ausgangszustand der Testfälle
1	Alle Server (srv20180101, srv20180102, srv20180201, srv20180202) inklusive VMLF1 sind gestartet.
2	Alle Server (srv20180101, srv20180102, srv20180201, srv20180202) inklusive VMLF1 sind gestartet.
3	Alle Server (srv20180101, srv20180102, srv20180201, srv20180202) inklusive VMLF1 sind gestartet. Chrome ist auf dem Testgerät installiert.
4	Alle Server (srv20180101, srv20180102, srv20180201, srv20180202) inklusive VMLF1 sind gestartet. Chrome ist auf dem Testgerät installiert.
5	Alle Server (srv20180101, srv20180102, srv20180201, srv20180202) inklusive VMLF1 sind gestartet. Chrome ist auf dem Testgerät installiert.
6	Alle Server (srv20180101, srv20180102, srv20180201, srv20180202) inklusive VMLF1 sind gestartet. Chrome ist auf dem Testgerät installiert.

3.2.2 Voraussetzungen:

Die einzelnen Server, welche für den jeweiligen Testfall benötigt werden, müssen gestartet werden. Zudem muss auf den DNS Servern der DNS Dienst Bind9 gestartet werden, falls der Test einen Zusammenhang mit dem DNS hat.

Nachdem die einzelnen Server gestartet sind, befinden sich diese im korrekten Aggregatzustand.

3.2.3 Konfiguration:

Für alle Tests ist vorausgesetzt das alle betroffenen Testobjekte wie vorgegeben im 3.1 Konfiguriert sind. Keine Abweichung unserer Standard Konfiguration.

3.2.4 Durchführung

Nr.	Interaktion der Testfälle
1	<p>Auf dem Testgerät (Windows 10 VM) wird die CMD Konsole geöffnet. Das Testgerät wird im Lan1 angebunden.</p> <ul style="list-style-type: none">○ Vom LAN1: Ping srv20180101○ Vom LAN1: Ping srv20180102○ Vom LAN1: Ping srv20180201○ Vom LAN1: Ping srv20180202 <p>Das Testgerät wird in das Lan2 Gebunden.</p> <ul style="list-style-type: none">○ Vom LAN2: Ping srv20180101○ Vom LAN2: Ping srv20180102○ Vom LAN2: Ping srv20180201○ Vom LAN2: Ping srv20180202
2	<p>Auf dem Testgerät (Windows 10 VM) wird die CMD Konsole geöffnet. Das Testgerät wird im Lan1 angebunden.</p> <ul style="list-style-type: none">○ Vom Lan1: nslookup srv20180101○ Vom Lan1: nslookup srv20180201 <p>Das Testgerät wird in das Lan2 Gebunden.</p> <ul style="list-style-type: none">○ Vom Lan2: nslookup srv20180101○ Vom Lan2: nslookup srv20180201
3	<p>Auf dem Testgerät (Windows 10 VM) wird Chrome geöffnet. Das Testgerät wird im Lan1 angebunden.</p> <ul style="list-style-type: none">○ Vom Lan1: IP vom srv20180101 in das Domain Feld eingeben○ Vom Lan1: IP vom srv20180201 in das Domain Feld eingeben <p>Das Testgerät wird in das Lan2 Gebunden.</p> <ul style="list-style-type: none">○ Vom Lan2: IP vom srv20180101 in das Domain Feld eingeben○ Vom Lan2: IP vom srv20180201 in das Domain Feld eingeben
4	<p>Auf dem Testgerät (Windows 10 VM) wird Chrome geöffnet. Das Testgerät wird im Lan1 angebunden.</p> <ul style="list-style-type: none">○ Vom Lan1: DNS Name des Webserver eingeben. <p>Das Testgerät wird in das Lan2 Gebunden.</p> <ul style="list-style-type: none">○ Vom Lan2: DNS Name des Webserver eingeben.

5	<p>Auf dem Testgerät (Windows 10 VM) wird Chrome geöffnet. Das Testgerät wird im Lan1 angebunden. Der Webserver(srv20180101) wird ausgeschaltet.</p> <ul style="list-style-type: none"> Vom Lan1: DNS Name des Webserver eingeben. <p>Das Testgerät wird in das Lan2 Gebunden.</p> <ul style="list-style-type: none"> Vom Lan2: DNS Name des Webserver eingeben. <p>Das Testgerät wird im Lan1 angebunden. Der Webserver(srv20180101) wird eingeschalten. Der Webserver (srv20180201) wird ausgeschaltet.</p> <ul style="list-style-type: none"> Vom Lan1: DNS Name des Webserver eingeben. <p>Das Testgerät wird in das Lan2 Gebunden.</p> <ul style="list-style-type: none"> Vom Lan2: DNS Name des Webserver eingeben.
6	<p>Auf dem Testgerät (Windows 10 VM) wird Chrome geöffnet. Das Testgerät wird im Lan1 angebunden. Der DNS Server(srv20180102) wird ausgeschaltet.</p> <ul style="list-style-type: none"> Vom Lan1: DNS Name des Webserver eingeben. <p>Das Testgerät wird in das Lan2 Gebunden.</p> <ul style="list-style-type: none"> Vom Lan2: DNS Name des Webserver eingeben. <p>Das Testgerät wird im Lan1 angebunden. Der DNS Server (srv20180102) wird eingeschalten. Der DNS Server (srv20180202) wird ausgeschaltet.</p> <ul style="list-style-type: none"> Vom Lan1: DNS Name des Webserver eingeben. <p>Das Testgerät wird in das Lan2 Gebunden.</p> <ul style="list-style-type: none"> Vom Lan2: DNS Name des Webserver eingeben.

3.2.5 Nachbearbeitung

Alle Testresultate werden nach dem folgenden Konzept festgehalten

NR	Die Nummer des jeweiligen Tests
Erwartetes Resultat	Genaue Beschreibung des Resultates, welches zu erwarten ist, nach dem der Test ausgeführt wurde
Tatsächliches Resultat	Genaue Beschreibung des Resultates, welches nach der Ausführung des Tests, entstanden ist.
Abweichungen	Festhalten welche Abweichungen entstanden sind nach dem Vergleichen des erwarteten Resultats und des tatsächlichen Resultats.

Die Testauswertung wird nach dem dokumentieren aller Testresultate erfasst. Die Auswertung variiert je nach dem wie viele der Test erfolgreich waren. Wichtig ist, dass deklariert wird, ob das Projekt abgeschlossen werden kann. Bestimmt wird das, durch die Analyse der erfolgreichen und fehlgeschlagen Tests. Zudem müssen die weiteren Massnahmen definiert werden, falls dies nötig ist.

3.3 Testprotokoll

3.3.1 Testobjekt

NR	1
Testobjekte	srv20180101, srv20180102, srv20180201, srv20180202, vmlf1 und der Windows 10 Testclient
Tester	Marc Binggeli
Ort	Zimmer IET 201 in der GIBB Bern
Datum	05.12.2018 um 14:20

NR	2
Testobjekte	srv20180101, srv20180201, vmlf1 und der Windows 10 Testclient
Tester	Marc Binggeli
Ort	Zimmer IET 201 in der GIBB Bern
Datum	05.12.2018 um 14:25

NR	3
Testobjekte	srv20180101, srv20180102, srv20180201, srv20180202, vmlf1 und der Windows 10 Testclient
Tester	Marc Binggeli
Ort	Zimmer IET 201 in der GIBB Bern
Datum	05.12.2018 um 14:30

NR	4
Testobjekte	srv20180101, srv20180201, vmlf1 und Windows 10 Testclient
Tester	Marc Binggeli
Ort	Zimmer IET 201 in der GIBB Bern
Datum	05.12.2018 um 14:40

NR	5
Testobjekte	srv20180101, srv20180201, vmlf1 und der Windows 10 Testclient
Tester	Marc Binggeli
Ort	Zimmer IET 201 in der GIBB Bern
Datum	05.12.2018 um 14:45

NR	6
Testobjekte	srv20180101, srv20180201, vmlf1 und der Windows 10 Testclient
Tester	Marc Binggeli
Ort	Zimmer IET 201 in der GIBB Bern
Datum	05.12.2018 um 14:50

Versionen der einzelnen Server:

Server	Version
Srv20180101	Debian 4.9.130-2 x86_64
Srv20180102	Ubuntu 16.04.4 LTS – 4.4.0-81-generic
Srv20180201	Debian 4.9.130-2 x86_64
Srv20180202	Ubuntu 16.04.4 LTS – 4.4.0-81-generic
Vmlf1	IPFire 2.19 (x86_x64)
Testclient	Windows 10

3.3.2 Testresultate

NR	1
Erwartetes Resultat	Alle Server (srv20180101, srv20180102, srv20180201, srv20180202) werden antworten
Tatsächliches Resultat	Die Server sind per Ping auf die IP erreichbar.
Abweichungen	Keine

NR	2
Erwartetes Resultat	Die Anfrage wird den Namen der Server zurückgeben.
Tatsächliches Resultat	Der Domain Name des Servers wurde zurückgegeben.
Abweichungen	Keine

NR	3
Erwartetes Resultat	Webserver (srv20180101, srv20180201) sind per IP erreichbar.
Tatsächliches Resultat	Die Webseite wurde im Browser angezeigt.
Abweichungen	Keine

NR	4
Erwartetes Resultat	Die Website des Webserver wird angezeigt.
Tatsächliches Resultat	Die Webseite wurde im Browser angezeigt.
Abweichungen	Keine

NR	5
Erwartetes Resultat	Die Website des Webserver wird angezeigt.
Tatsächliches Resultat	Die Webseite wurde im Browser angezeigt.
Abweichungen	Keine

NR	6
Erwartetes Resultat	Der Ping auf alle beteiligten Testobjekte funktioniert sowohl vom LAN1, als auch vom LAN2.
Tatsächliches Resultat	Die Webseite wurde im Browser angezeigt.
Abweichungen	Keine

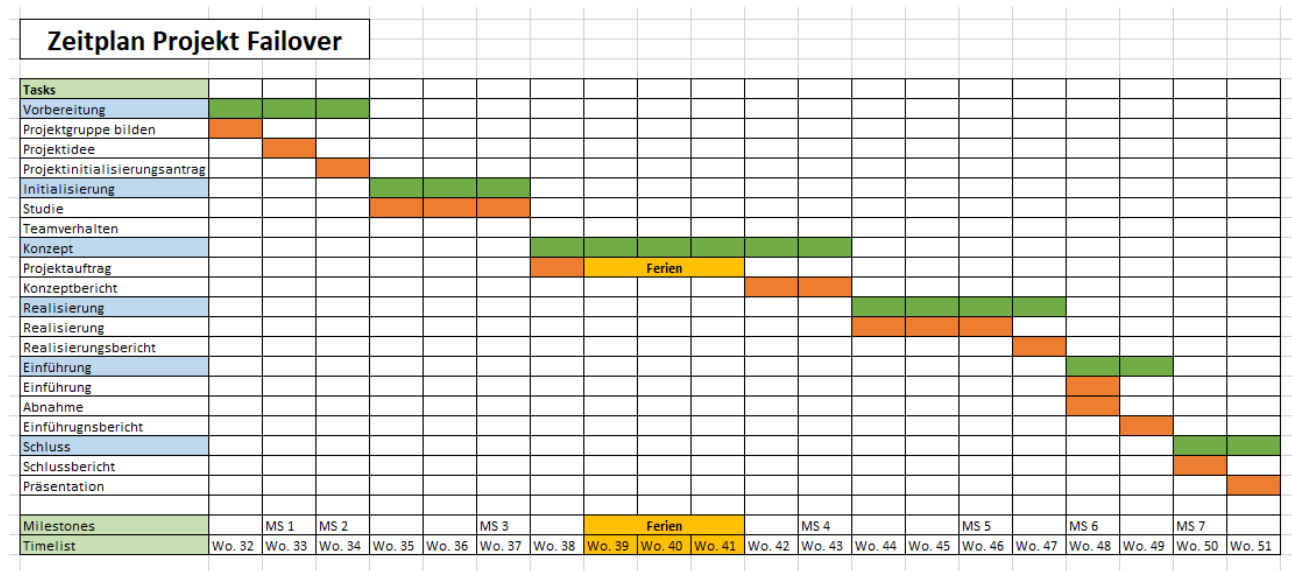
3.3.3 Testauswertung

Unsere Testfälle wurden erfolgreich und ohne Abweichungen zu dem erwarteten Ergebnis durchgeführt. Das gebaute System funktioniert einwandfrei. Für die Anforderungen, die wegen des Änderungsantrages nicht mehr getestet werden können, wurde kein Test durchgeführt.

4 Weiterführung der Projektplanung

4.1 Abgleich von Planung und tatsächlichem Verlauf der Phase Konzept

In Hinblick auf die Zeitplanung sind wir ein bisschen in Rückstand geraten. Die Realisierungsphase hat insbesondere mit der Problematik in Zusammenhang mit der Firewall mehr Zeit in Anspruch genommen, als wir eigentlich geplant haben. Jedoch werden wir die Einführung sowie der Schlussbericht ein wenig kürzen können, da dieser im Modul extrem lange geplant ist.



In der Realisierungsphase bestanden die Risiken vor allem bei der Umsetzung der Umgebung. Da wir mit virtuellen Maschinen gearbeitet haben, konnten wir die Umgebung nicht so umsetzen wie sie eigentlich geplant war.

Dadurch müssen wir auf eine zweite Firewall verzichten, da wir die Umleitung von den beiden Firewalls und das Portforwarding nicht konfigurieren konnten. Wir beschäftigten uns intensiv mit diesem Thema, aber wir konnten keine Lösung finden. Deshalb entschieden wir, dass wir die zweite Firewall weglassen und uns stattdessen auf die Dokumentation der bestehenden Umgebung konzentrieren.

Für diese Änderung haben wir einen Änderungsantrag ausgefüllt. In diesem ist eine Änderung des Sollzustandes beschrieben. Neu wird nur noch eine virtuelle Firewall eingesetzt und nicht wie anfangs geplant zwei. Hinter der Firewall befinden sich 2 Netze, die redundant sind. Wenn nun ein Netz ausfällt, wechselt die Firewall das Netz und der Dienst, also in unserem Fall der Webserver, ist für die User wieder erreichbar.

Das Risiko, dass wir an der Konfiguration der Firewall scheitern werden war uns in der Konzeptphase bewusst. Wir dachten jedoch, dass wir dies mit Hilfe des Internets lösen können.

Die Konsequenzen daraus sind, dass wir ungefähr 1 bis 2 Wochen an Zeit verloren haben. Jedoch können wir diese wieder in den nächsten Phasen einholen. Die Anforderung A 2.3 kann mit der neuen, angepassten Umgebung nicht erfüllt werden.

4.2 Aktualisierung der Risikosituation

Die Risiken wurden in der Konzeptphase bereits aktualisiert. Die Risiken, die wir in der Phase Konzept definiert haben sind folgende:

Risikobeschrieb	Eintrittswahr-scheinlichkeit	Auswirkung	Massnahme
Zeitplan nicht einhaltbar	3	Gross	Puffer einplanen Zeitplan gut einteilen und planen
Krankheit	2	Klein	Absprache mit dem Projektleiter sowie mit dem Projektteam
Fehlende Ressourcen	2	Mittel	Ressourcen frühzeitig verifizieren und bereitstellen
Konfigurationsfehler	2	Gross	Konfigurationen überprüfen, von einem Kollegen Zweitmeinung einholen
Falsche Kommunikation zwischen den Teammitgliedern	3	Gross	Absprache miteinander halten, Abschlussmeeting nach den Lektionen.

Während der Phase Realisierung gab es wieder verschiedene Änderungen an der Risikosituation. Einerseits konnten wir bei manchen Situationen die Auswirkung und die Eintrittswahrscheinlichkeit entschärfen. Ausserdem konnten wir einige Risiken streichen, da diese in den nächsten Phasen nicht mehr relevant sein werden. Jedoch wurde ein neues Risiko erkannt und erfasst. Unten ist die aktualisierte Tabelle der Risikosituationen:

Risikobeschrieb	Eintrittswahr-scheinlichkeit	Auswirkung	Massnahme
Zeitplan nicht einhaltbar	2	Mittel	Puffer einplanen Zeitplan gut einteilen und planen
Krankheit	1	Klein	Absprache mit dem Projektleiter sowie mit dem Projektteam
Falsche Kommunikation zwischen den Teammitgliedern	2	Gross	Absprache miteinander halten, Abschlussmeeting nach den Lektionen.
Verlust der Systemumgebung	2	Gross	Backup der Umgebung erstellen, Aufbewahrung auf verschiedenen Hosts

4.3 Planung der nächsten Phase

Der aktualisierte Projektplan sieht nun folgendermassen aus:

Zeitplan Projekt Failover																										
Tasks																										
Vorbereitung																										
Projektgruppe bilden																										
Projektidee																										
Projektinitialisierungsantrag																										
Initialisierung																										
Studie																										
Teamverhalten																										
Konzept																										
Projektauftrag																										
Konzeptbericht																										
Realisierung																										
Realisierungsbericht																										
Einführung																										
Einführung																										
Einführungsbericht																										
Schluss																										
Schlussbericht																										
Präsentation																										
Milestones																										
Timelist																										

Wie bereits erwähnt, werden die Phasen Einführung und Schluss ein wenig gekürzt. Trotz der Kürzung sollte es für uns immer noch möglich sein, diese Phasen erfolgreich und im Zeitraum abzuschliessen. Für die Phasen Einführung und Schluss werden im Modul vier Wochen als Vorbereitung eingeplant. Daher werden wir diesen Teil auf zwei bis drei Wochen kürzen.

Die Präsentation wird vor den Ferien fertiggestellt, damit die Präsentation von unserem Projekt nach den Weihnachtsferien in den Wochen zwei und drei gehalten werden kann.