

Dokumentation SWITCHengines

Erstellt im Modul IP-316bb 2015 / 2016

Adrian Schulz

Brugg, 18.09.2016

Versions Nr.	Datum	Änderung	Autor
1.0	18.09.2016	Erstellung	A.Schulz

Inhaltsverzeichnis

1	SWITCHengines	3
1.1	Registrierung.....	3
1.2	Zugriff & Sicherheit.....	3
1.2.1	Sicherheitsgruppen	3
1.2.1.1	Sicherheitsgruppe erstellen	4
1.2.1.2	Benötigte Sicherheitsgruppen und Regeln.....	6
1.2.2	Schlüsselpaare.....	6
1.2.2.1	Schlüsselpaare	7
1.2.2.2	Name für das Schlüsselpaar	8
1.2.3	Floating IPs	8
1.2.3.1	Floating IP dem Projekt zuweisen	8
1.3	Instanz erstellen	9
1.3.1	Log prüfen	11
1.4	Instanz steuern.....	11
1.4.1	Privater Schlüssel in Putty-Schlüssel umwandeln.....	11
1.4.2	Instanz ansprechen	12
1.4.3	Dateien auf den Server laden	14
2	Anhang.....	17
2.1	Download-Links.....	17

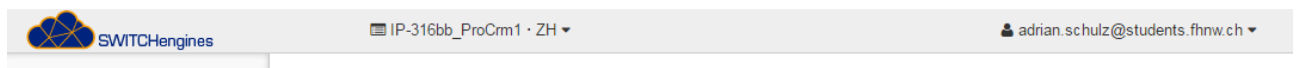
1 SWITCHengines

In diesem Dokument ist eine Anleitung wie eine virtuelle Maschine bei SWITCHengines eingerichtet wird. Bei SWITCHengines wird eine virtuelle Maschine Instanz genannt.

1.1 Registrierung

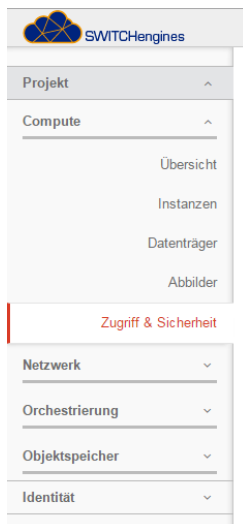
Um sich zu registrieren braucht es einen Voucher, welcher von switchengines.services@fhnw.ch angefordert werden kann. Der Voucher enthält einen Link, welcher zur Registrierungsseite von SWITCHengines zeigt.

Eine Instanz bei SWITCHengines zu betreiben ist nicht gratis und wird daher von der FHNW finanziert. Aus diesem Grund muss jeder Account eines Projektmitglieds von switchengines.services@fhnw.ch zu einem Projekt hinzugefügt werden. Wenn dieser Punkt durchgeführt wurde, kann man oben in der Toolbar auf das Projekt wechseln.



1.2 Zugriff & Sicherheit

Bei diesem Punkt können diverse Einstellungen betreffend dem Zugriff auf eine Instanz angepasst werden.



1.2.1 Sicherheitsgruppen

Eine Sicherheitsgruppe ersetzt die Firewall auf einer Instanz. Vorteil dadurch ist, dass man die Einstellungen immer noch verändern kann wenn man sich aus Versehen aus der Instanz ausge-

geschlossen hat. Einer Instanz können mehrere Sicherheitsgruppen zugewiesen werden, wobei eine Sicherheitsgruppe mehrere Regeln enthält. Zu Beginn ist bereits eine Default-Sicherheitsgruppe definiert.

Für unsere Instanz braucht es aber 2 neue Sicherheitsgruppen.

1.2.1.1 Sicherheitsgruppe erstellen

Zuerst klickt man unter 'Zugriff & Sicherheit' auf 'Sicherheitsgruppen' und danach auf „Sicherheitsgruppe erstellen“.

<input type="checkbox"/>	Name	Beschreibung	Actions
<input type="checkbox"/>	Access		Regeln verwalten
<input type="checkbox"/>	Web		Regeln verwalten
<input type="checkbox"/>	default	Default security group	Regeln verwalten

Displaying 3 items

Anschliessend gibt man den Namen und allenfalls eine Beschreibung ein und klickt dann auf „Sicherheitsgruppe erstellen“.

Sicherheitsgruppe erstellen

Name *

Beschreibung

Sicherheitsgruppen sind Sets von IP Filterregeln, die für die Netzwerkeinstellungen der VM gelten. Nachdem die Sicherheitsgruppe erzeugt wurde, können Regeln hinzugefügt werden.

Abbrechen Sicherheitsgruppe erstellen

Nachher klickt man Rechts auf „Regeln verwalten“.

Projekt

Compute

Übersicht

Instanzen

Datenträger

Abbilder

Zugriff & Sicherheit

Netzwerk

Orchestrierung

Zugriff & Sicherheit

Sicherheitsgruppen

Schlüsselpaare

Floating IPs

API Zugriff

Filter

+ Sicherheitsgruppe erstellen

✕ Sicherheitsgruppen löschen

<input type="checkbox"/>	Name	Beschreibung	Actions
<input type="checkbox"/>	Access		Regeln verwalten
<input type="checkbox"/>	Web		Regeln verwalten
<input type="checkbox"/>	default	Default security group	Regeln verwalten

Displaying 3 items

In der folgenden Ansicht sieht man alle Regeln einer Sicherheitsgruppe. Als Default sind bereits 2 Ausgangsregeln definiert, diese bitte nicht löschen. Anschliessend erstellt man alle eigenen Regeln per Klick auf ‚Regel hinzufügen‘.

Projekt

Compute

Übersicht

Instanzen

Datenträger

Abbilder

Zugriff & Sicherheit

Netzwerk

Sicherheitsgruppenregeln verwalten: Access (46c7662a-4669-4ed3-9a2f-df8b8348be41)

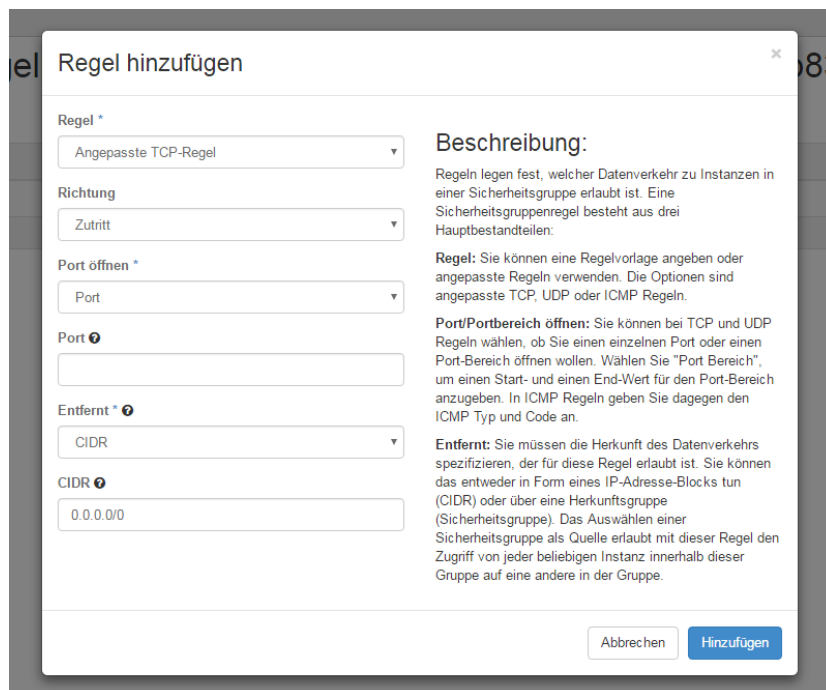
+ Regel hinzufügen

✕ Regeln löschen

<input type="checkbox"/>	Richtung	Netzwerktyp	IP-Protokoll	Port-Bereich	Entfernte IP Präfix	Entfernte Sicherheitsgruppe	Actions
<input type="checkbox"/>	Zutritt	IPv4	ICMP	Jede(s)	0.0.0.0/0	-	Regel löschen
<input type="checkbox"/>	Zutritt	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	Regel löschen

Displaying 2 items

Danach muss man die Regel genau definieren und klickt dann auf ‚Hinzufügen‘.



Regel hinzufügen

Regel *
Angepasste TCP-Regel

Richtung
Zutritt

Port öffnen *
Port

Port
[]

Entfernt *
CIDR

CIDR
0.0.0.0/0

Beschreibung:
Regeln legen fest, welcher Datenverkehr zu Instanzen in einer Sicherheitsgruppe erlaubt ist. Eine Sicherheitsgruppenregel besteht aus drei Hauptbestandteilen:
Regel: Sie können eine Regelvorlage angeben oder angepasste Regeln verwenden. Die Optionen sind angepasste TCP, UDP oder ICMP Regeln.
Port/Portbereich öffnen: Sie können bei TCP und UDP Regeln wählen, ob Sie einen einzelnen Port oder einen Port-Bereich öffnen wollen. Wählen Sie "Port Bereich", um einen Start- und einen End-Wert für den Port-Bereich anzugeben. In ICMP Regeln geben Sie dagegen den ICMP Typ und Code an.
Entfernt: Sie müssen die Herkunft des Datenverkehrs spezifizieren, der für diese Regel erlaubt ist. Sie können das entweder in Form eines IP-Adresse-Blocks tun (CIDR) oder über eine Herkunftsgruppe (Sicherheitsgruppe). Das Auswählen einer Sicherheitsgruppe als Quelle erlaubt mit dieser Regel den Zugriff von jeder beliebigen Instanz innerhalb dieser Gruppe auf eine andere in der Gruppe.

Abbrechen Hinzufügen

1.2.1.2 Benötigte Sicherheitsgruppen und Regeln

Neben den Default-Ausgangsregeln müssen, noch folgende Regeln definiert werden:

SICHERHEITSGRUPPE	REGEL	FELD	WERT
ACCESS	SSH	Regel	SSH
		Entfernt	CIDR
		CIDR	147.86.0.0/16
	ICMP	Regel	ALL ICMP
		Richtung	Zutritt
		Entfernt	CIDR
		CIDR	147.86.0.0/16

Anmerkung: Diese Regeln bewirken, dass die Instanz nur aus dem FHNW-Netz erreichbar ist.

1.2.2 Schlüsselpaare

Bei SWITCHengines sind die Instanzen nicht per Passwort gesichert. Grund dafür sind die Images, welche öffentlich zur Verfügung gestellt werden. Der Username und das Passwort wären bei allen laufenden Instanzen das gleiche. Deshalb werden SSH-Keys benutzt.

SSH-Keys bestehen aus einem privaten und einem öffentlichen Schlüssel. Der öffentliche Schlüssel wird in der Instanz gespeichert und der private in der Session. Die SSH-Keys werden bei SWITCHengines 'Schlüsselpaare' genannt.

1.2.2.1 Schlüsselpaare

Falls noch kein Schlüsselpaar vorhanden ist, muss eines erstellt werden. Dazu geht man unter 'Zugriff & Sicherheit' in den Reiter 'Schlüsselpaare' und klickt anschliessend auf 'Schlüsselpaar erzeugen'.

Zugriff & Sicherheit

Sicherheitsgruppen | Schlüsselpaare | Floating IPs | API Zugriff

Filter

<input type="checkbox"/>	Schlüsselpaar-Name	Fingerabdruck	Actions
<input type="checkbox"/>	ProCrm1Key	70:c7:d5:c5:51:e7:9a:42:91:02:b6:20:7d:9f:b6:5d	<input type="button" value="Schlüsselpaar löschen"/>

Displaying 1 item

Danach gibt man den Namen für das Schlüsselpaar ein und klickt auf 'Schlüsselpaar erzeugen'.

Schlüsselpaar erzeugen

Schlüsselpaar-Name *

Beschreibung:

Schlüsselpaare sind ssh Authentifizierungsdetails, die während des Starts eines Abbildes injiziert werden. Beim Erzeugen eines neuen Schlüsselpaares wird der öffentliche Schlüssel registriert und der private Schlüssel (eine .pem Datei) heruntergeladen.

Schützen und benutzen Sie den Schlüssel wie jeden anderen privaten ssh-Schlüssel.

Normalerweise wird anschliessend automatisch der private Schlüssel heruntergeladen. Falls dies nicht der Fall ist, kann man auf den angezeigten Link klicken um den privaten Schlüssel herunterzuladen.

Schlüsselpaar herunterladen

Das Schlüsselpaar "ProCrm1Key" wird automatisch heruntergeladen. Wenn nicht, verwenden Sie den unten stehenden Link.

[Schlüsselpaar "ProCrm1Key" herunterladen](#)

Was mit diesem privaten Schlüssel gemacht werden muss, wird in Kapitel ‚Zugang per SSH‘ erklärt. Es ist aber wichtig, dass der private Schlüssel nicht verloren geht.

1.2.2.2 Name für das Schlüsselpaar

Der Name für das verwendete Schlüsselpaar ist ‚ProCrm1Key‘.

1.2.3 Floating IPs

Damit eine Instanz auch über eine öffentliche IP-Adresse angesteuert werden kann, muss eine Floating IP dem Projekt zugewiesen werden. Über diese IP-Adresse ist die VM von überall erreichbar.

1.2.3.1 Floating IP dem Projekt zuweisen

Um eine Floating IP dem Projekt zuzuweisen, klickt man auf ‚IP zu Projekt zuweisen‘ unter dem Reiter ‚Floating IPs‘ in ‚Zugriff & Sicherheit‘.



IP-Adresse	Zugewiesene feste IP-Adresse	Pool	Status	Actions
86.119.35.58	-	public	Runter	Zuweisen

Danach muss das Netzwerk gewählt. Man hat normalerweise keine andere Wahl als ‚public‘. Danach klickt man auf ‚IP belegen‘.

Floating IP belegen

Pool *

public

Beschreibung:

Floating IP aus einem angegebenen Pool belegen.

Projektkontingente

Floating IP (0)

10 Verfügbar

Abbrechen

IP belegen

Anm: Man kann die Floating IP nicht auswählen. Sie wird einem von SWITCHengines zugewiesen.

1.3 Instanz erstellen

Um eine Instanz zu erstellen geht man unter ‚Compute‘ in ‚Instanzen‘. Hier klickt man dann auf ‚Instanz starten‘.

Projekt

Compute

Übersicht

Instanzen

Datenträger

Abbilder

Zugriff & Sicherheit

Instanzen

Instanzname

Filter

Filter

Instanz starten

Instanzname	Abbildname	IP-Adresse	Größe	Schlüsselpaar	Status	Verfügbarkeitszone	Aufgabe	Zustand	Zeit seit Erzeugung	Actions
No items to display.										
Displaying 0 items										

Nachher muss man diverse Einstellungen vornehmen und klickt anschliessend auf ‚Start‘. Unter anderem werden die Sicherheitsgruppen ausgewählt und der Public-Key des Schlüsselpaars auf der Instanz abgespeichert.

Instanz starten

Details *

Zugriff & Sicherheit

Netzwerk *

Nach Erstellung

Weitergehende Optionen

Verfügbarkeitszone

nova

Instanzname *

ProCrm1-VM

Variante * ?

c1.large

Instanzenanzahl * ?

1

Boot-Quelle der Instanz * ?

Von Abbild starten (erzeugt neuen Datenträger)

Abbildname *

Ubuntu Trusty 14.04 (SWITCHengines) (1,6 GB)

Gerätegröße (GB) * ?

30

Gerätename ?

vda

☐ Löschen beim Beenden ?

Geben Sie die Details zum Start einer Instanz an.

Das Diagramm unten zeigt die von diesem Projekt verwendeten Ressourcen im Verhältnis zu den Projektkontingenten.

Varianten-Details

Name	c1.large
VCPUs	4
Root-Festplatte	20 GB
Flüchtige Festplatte	0 GB
Festplatte gesamt	20 GB
RAM	4,096 MB

Projekt-Begrenzungen

Anzahl der Instanzen

0 von 5 verwendet

Anzahl der VCPUs

0 von 10 verwendet

RAM gesamt

0 von 16.384 MB verwendet

Abbrechen

Start

Anschliessend muss man einige Augenblicke warten bis die Instanz erstellt ist und auch läuft. Danach muss noch die Floating IP zugewiesen werden. Dazu klickt man rechts auf den Pfeil und wählt ‚Floating IP zuweisen‘.

Instanzen

<div> <div>Instanzname</div> <div>Filter</div> <div>Filter</div> <div>Instanz starten</div> <div>Instanzen löschen</div> <div>More Actions</div> </div>											
<input type="checkbox"/>	Instanzname	Abbildname	IP-Adresse	Größe	Schlüsselpaar	Status	Verfügbarkeitszone	Aufgabe	Zustand	Zeit seit Erzeugung	Actions
<input type="checkbox"/>	ProCrm1-VM	-	10.0.233.244 2001:620:5ca1:1f0:f816:3eff:fee8:3bec	c1.large	ProCrm1Key	Aktiv	nova	Keine	Läuft	1 Stunde, 2 Minuten	<div>Schattenkopie erstellen</div> <div>Floating IP zuweisen</div> <div>Schnittstelle hinzufügen</div> <div>Schnittstelle abtrennen</div> <div>Instanz bearbeiten</div>

Danach wählt man die vorher reservierte Floating IP aus (Feld ‚IP-Adresse‘). Das Protokoll kann auf dem Default-Wert gelassen werden. Dann klickt man auf ‚Zuweisen‘.

Floating IP Zuweisungen verwalten

IP-Adresse *

IP-Adresse *

86.119.35.58

Wählen Sie die IP-Adresse, die Sie der ausgewählten Instanz oder dem Port zuweisen wollen.

Protokoll wird verknüpft *

ProCrm1-VM: 10.0.233.244

Abbrechen Zuweisen

1.3.1 Log prüfen

Es ist wichtig, dass nach dem Erstellen das Log geprüft wird. Findet man bspw. im Log eine Meldung, dass der SSH-Key nicht verifiziert werden konnte, so kann man sich später auch mit dem richtigen privaten Schlüssel nicht anmelden. In diesem Fall sind meistens falsche Firewall-Regeln der Grund für die Meldung.

Um das Log einer Instanz zu prüfen klickt man unter ‚Instanzen‘ auf die betroffene Instanz und geht anschliessend in den Reiter ‚Log‘.

1.4 Instanz steuern

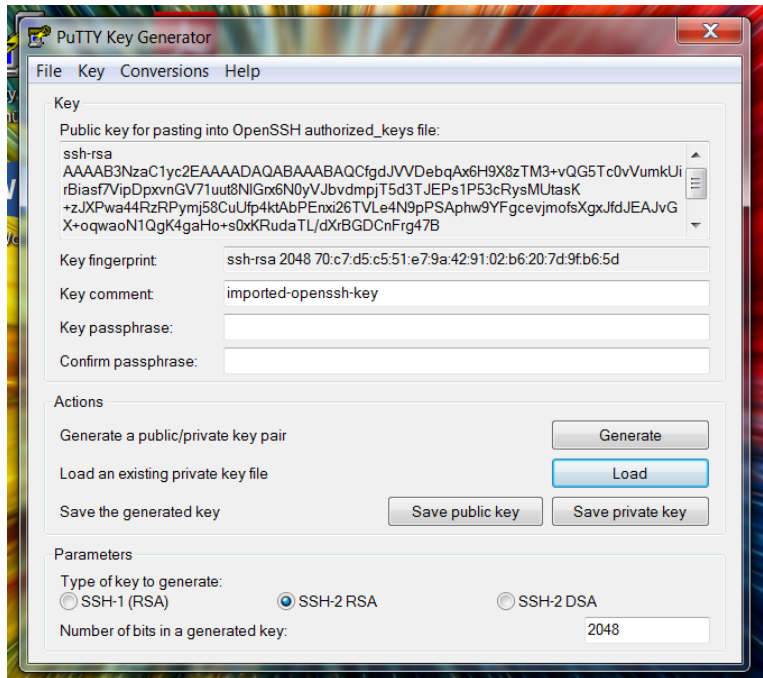
Die Instanz kann in Windows via Putty bedient werden.

1.4.1 Privater Schlüssel in Putty-Schlüssel umwandeln

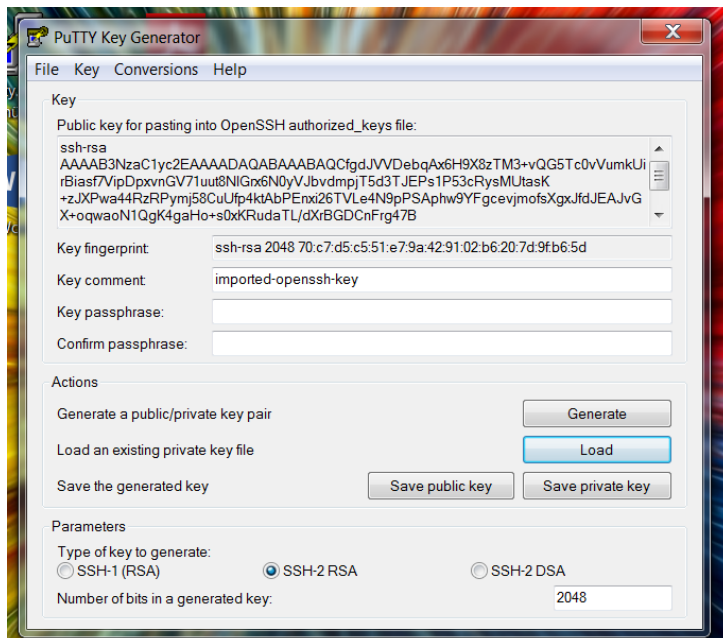
Da die Instanz nicht mit einem Passwort sondern mit einem SSH-Key geschützt ist, muss der vorher heruntergeladene Schlüssel in der Putty-Session gespeichert werden. Da Putty das SSH-Key-Format von SWITCHengines nicht versteht muss der Key erst in einen Putty-Schlüssel umgewandelt werden.

Dazu braucht es noch das Tool ‚PuTTYgen‘. Der Download-Link steht im Anhang.

Wenn man es startet, wird man zuerst gefragt ob man es wirklich ausführen will. Anschliessend öffnet sich das Programm. Um den Schlüsseln nun umzuwandeln, klickt man auf ‚Load‘ und wählt den vorher heruntergeladenen Schlüssel aus.



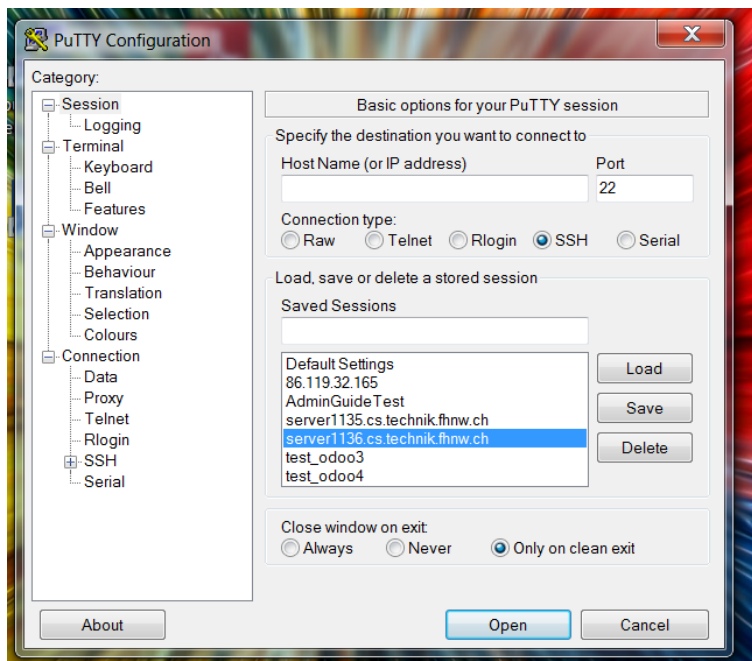
Anschließend kommt normalerweise eine Meldung, dass der Schlüssel erfolgreich importiert worden ist. Dann klickt man unten rechts auf ‚Save private key‘ und gibt dem neu generierten Putty-Key einen Namen. Ein Passwort muss nicht zwingend vergeben werden.



1.4.2 Instanz ansprechen

Um die Instanz anzusprechen braucht es Putty. Der Download-Link steht im Anhang.

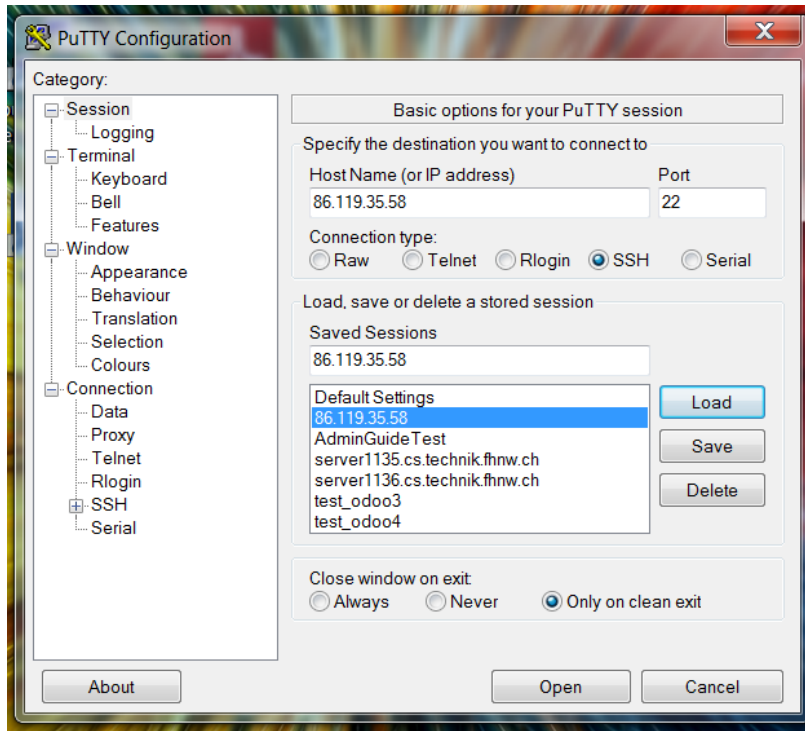
Nach dem Starten von Putty speichert man am besten eine Session für die Instanz. Dazu gibt man alle Einstellungen an und klickt anschliessend auf ‚Save‘.



Folgende Einstellungen müssen vorgenommen werden.

REITER	FELD	WERT
SESSION	Host Name (or IP address)	Vorher zugewiesene Floating IP
	Port	22
	Connection Type	SSH
	Saved Session	Beliebig. Floating IP empfohlen.
CONNECTION / SSH / AUTH	Private key file for authentication	Voher erstelltes Putty-Key-File auswählen.

Dann klickt man auf ‚Open‘.



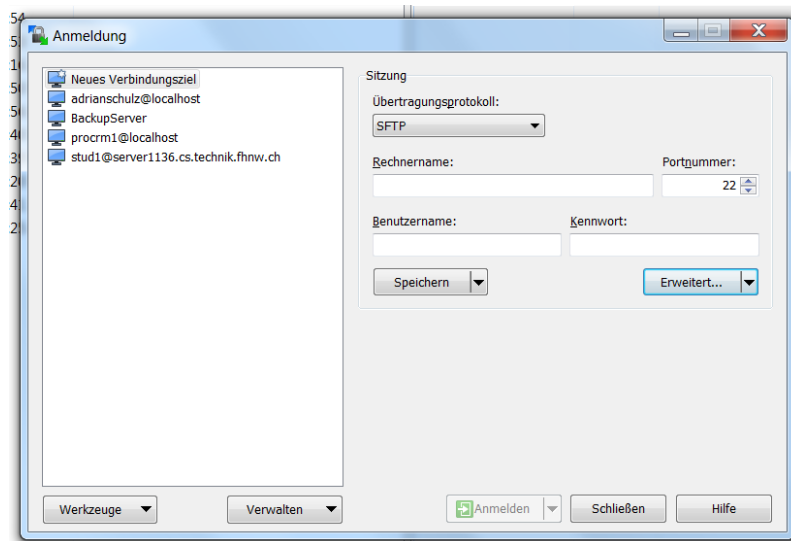
Falls alles richtig durchgeführt wurde, konnte die Verbindung zur Instanz hergestellt werden. Putty fragt man ersten Aufrufen einer Instanz, ob man dem Geräte vertraut. Hier kann man ‚Yes‘ klicken.

Auf der Instanz wird man dann als erstes nach dem Usernamen gefragt. Dieser ist ‚ubuntu‘.

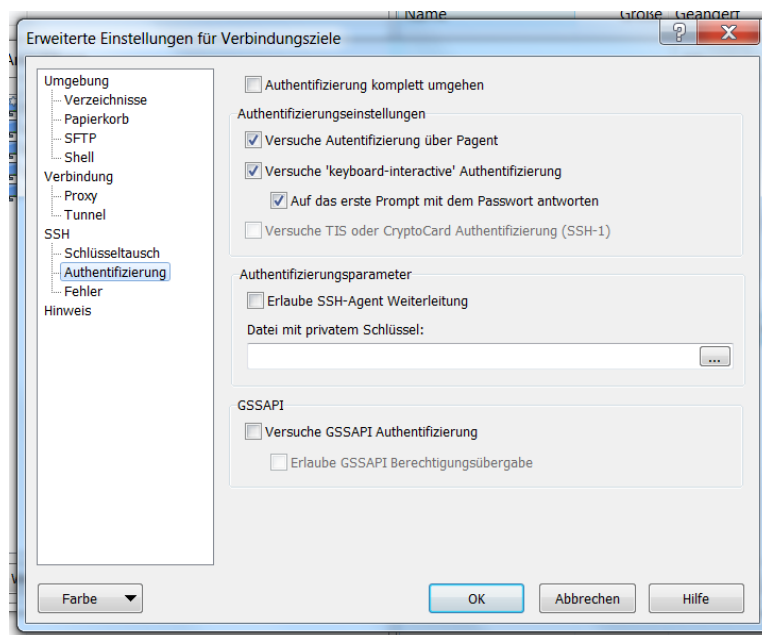
1.4.3 Dateien auf den Server laden

Unter bestimmten Umständen ist es notwendig, dass eine Datei vom lokalen Rechner auf den Server geladen werden muss. Dies kann in Windows mit WinSCP via SFTP erreicht werden.

Wenn man es startet, öffnet sich ein Fenster, in welchem man die Session-Einstellungen vornehmen kann.



Neben Standard-Einstellungen müssen noch erweiterte Einstellungen vorgenommen werden. Dazu klickt man auf ‚Erweitert‘.

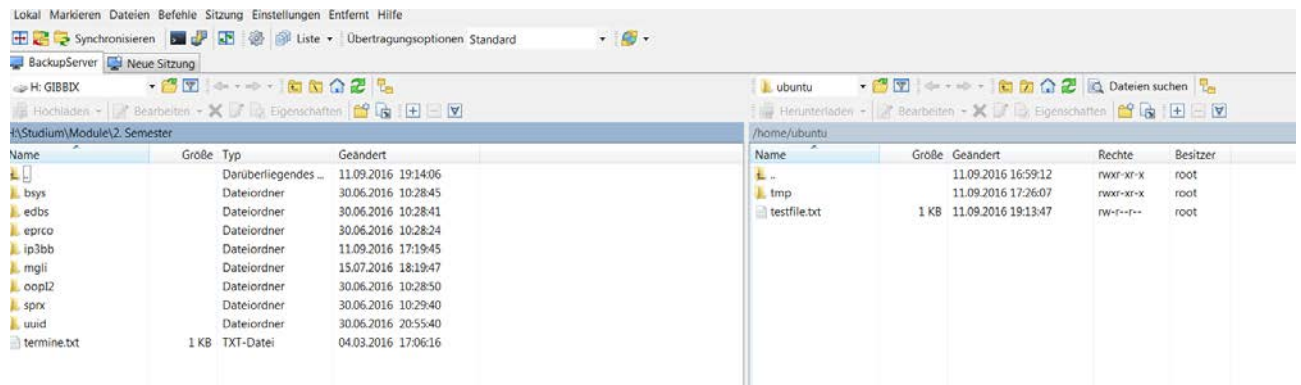


MENU	FELD	WERT
SITZUNG	Übertragungsprotokoll	SFTP
	Rechnername	Floating IP
	Portnummer	22
ERWEITERT / SSH / AU-	Daten mit privaten Schlüssel	Voher erstelltes Putty-Key-File

IDENTIFIZIERUNG

auswählen.

Danach klickt man auf ‚Anmelden‘. Das Fenster wird grösser und nun sieht man auf der linken Seite die Dateien auf dem eigenen Computer und rechts sind die Files des Servers. Per ‚Drag & Drop‘ können Dateien verschoben werden.



2 Anhang

2.1 Download-Links

TOOL	LINK
PUTTY	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
PUTTYGEN	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
WINSCP	https://winscp.net/eng/download.php .