

http://ovm-kassel.de Lernjob	
Lernjob IT-BS-VM-LJ-3.3 SSH-Client und -Server	
Code	IT-BS-VM-LJ-3.3
Autor	André Bauer <a(dot)bauer(at)ovm-kassel(dot)de>
Datum	22. Mai 2018
Links	<ul style="list-style-type: none"> • ssh(1) - Linux man page • PUTTY • PuTTY User Manual
Verwandte Literatur	<ul style="list-style-type: none"> • IT-BS-VM-LJ-3.1 Dokumentieren mit Script und AsciiDoc • IT-BS-VM-LJ-3.2 Netzwerke mit Virtualbox
Lizenz	 <p>Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz.</p>

SSH-Client und -Server

1. Was ist SSH?

SSH ist die Abkürzung für **Secure Shell** und wird als Begriff sowohl für das Netzwerkprotokoll als auch für die zugehörigen Dienstprogramme verwendet. SSH bietet eine kryptographisch abgesicherte Verbindung zwischen zwei Systemen und kann mit dem Programm `ssh` als interaktive Shell zum Zugriff und zur Administration entfernter und/oder virtueller Systeme sowie auch zum Datentransfer mit `sftp`, `scp` und `sshfs` verwendet werden.

2. Voraussetzungen

Im Folgenden wird vorausgesetzt, dass Sie bereits eine Virtuelle Maschine mit einem Linux-System, wie z. B. Ubuntu, als Gastsystem eingerichtet haben. Die folgenden Beispiele sollten aber auch auf andere Distributionen, die auf Debian basieren, übertragbar sein. Bei Linux-Distributionen, die z. B. auf Redhat basieren, müssen die Befehle, die zur Installation neuer Pakete dienen, angepasst werden, so muss unter Redhat `yum` statt `apt` verwendet werden. Die Namen der Pakete können ggf. abweichen.

3. Einen SSH-Server unter Linux einrichten

Um einen SSH-Server unter Ubuntu einzurichten, genügt es, diesen mit **apt** zu installieren:

Quellcode 1. Auf dem Gastsystem

```
$ sudo apt update
$ sudo apt install openssh-server ①
```

① Installation und Start des SSH-Servers.

Ob bereits ein SSH-Server-Prozess auf einem System läuft, kann mit **ps** überprüft werden:

Quellcode 2. Auf dem Gastsystem

```
$ ps xa | grep /usr/sbin/sshd
19851 ?        Ss        0:00 /usr/sbin/sshd -D ①
20419 pts/18   S+        0:00 grep --color=auto /usr/sbin/sshd
```

① Der SSH-Server ist in Betrieb.

4. Einen SSH-Server von einem Linux-Client verwenden

Da bei den meisten Linux-Distributionen bereits ein SSH-Client vorinstalliert ist, kann der SSH-Server über das **Loopback-Netzwerk** getestet werden:

Beispiel 1. Auf dem Gastsystem

```
$ ssh user@127.0.0.1 ①
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:x0amQ1jaC09SJmZjL0jPQuEB4mPEcr67ItNtgVib8po. ②
Are you sure you want to continue connecting (yes/no)? yes ③
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
user@127.0.0.1's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-36-generic x86_64)

Last login: Sat May  5 10:05:16 2018 from 127.0.0.1
```

- ① Statt der IP-Adresse **127.0.0.1** für die Loopback-Schnittstelle, kann auch der Name **localhost** verwendet werden.
- ② Beim ersten Login eines Clients auf einem unbekannten SSH-Server wird zur Kontrolle der ECDSA-Key-Fingerprint ausgegeben.
- ③ Der Vorgang wird aus Sicherheitsgründen nur nach einer Bestätigung fortgesetzt. Bei einer bereits genutzten Verbindung kann ein geänderter ECDSA-Key-Fingerprint auf einen **Man-in-the-Middle-Angriff** hindeuten.

Anstatt sich über die Loopback-Schnittstelle auf demselben System per **ssh** anzumelden, ist es

natürlich auch möglich, sich remote über ein Netzwerk auf einem anderen System anzumelden.

Für das folgende Beispiel müssen zwei VMs miteinander vernetzt (siehe Lernjob [IT-BS-VM-LJ-3.2 Netzwerke mit Virtualbox](#)) und auf dem System mit der IP-Adresse **10.0.3.10/24** ein SSH-Server eingerichtet sein.

Beispiel 2. SSH-Verbindung zwischen Linux-VMs

```
$ ssh user@10.0.3.10
user@10.0.3.10's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-39-generic x86_64)

...

Last login: Thu May 10 22:55:06 2018 from 10.0.3.11
user@Linux-VirtualBox:~$
```

Aufgabe 1



Dokumentieren Sie Ihr Vorgehen mit Script und AsciiDoc und stellen Sie das Ergebnis als PDF-Datei in Ihrem E-Portfolio zur Verfügung.

- Richten Sie zwei Linux-VMs in einem NAT-Netzwerk ein und installieren und starten Sie in einer VM einen SSH-Server. Wählen Sie dazu IP-Adressen, die von den Beispielen und anderen Quellen abweichen.
- Testen Sie wie in [Beispiel 1](#) den SSH-Server über die Loopback-Schnittstelle.
- Testen Sie wie in [Beispiel 2](#) den SSH-Server von der zweiten VM.

5. Einen SSH-Server von einem Hostsystem verwenden

Für den Zugriff vom Hostsystem auf das Linux-Gastsystem verwenden wir im Folgenden zunächst eine Portweiterleitung. Dazu richten wir eine Portweiterleitung auf den Port 22 des Gastsystems ein, z. B. von Port 8022 auf dem Hostsystem.

Unix-artige Hostsysteme

Auf unixartigen Hostsystemen, wie z. B. Linux oder Mac OS X, kann **ssh** direkt von einem Terminal aus verwendet werden. Im Unterschied zu [Beispiel 2](#) wird dem SSH-Befehl mit der Option **-p 8022** eine Portnummer, die für die Verbindung mit dem SSH-Server verwendet werden soll, übergeben. Ohne eine solche Angabe wird der SSH-Standard-Port 22 verwendet.

Beispiel 3. Auf dem Hostsystem

```
$ ssh user@localhost -p 8022 ①
The authenticity of host '[localhost]:8022 ([127.0.0.1]:8022)' can't be
established.
ECDSA key fingerprint is SHA256:x0amQ1jaC09SJmZjL0jPQuEB4mPEcr67ItNtgVib8po.
Are you sure you want to continue connecting (yes/no)? yes ②
Warning: Permanently added '[localhost]:8022' (ECDSA) to the list of known hosts.
user@localhost's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-36-generic x86_64)
```

① Verwendung von **ssh** mit Port 8022.

② Falls vom Hostsystem noch keine SSH-Verbindung zu dem Linux-Gastsystem aufgebaut worden ist, muss auch hier der ECDSA-Key-Fingerprint bestätigt werden.

Windows-Hostsysteme

Unter Windows kann SSH mit dem SSH-Client **PuTTY** und den zu gehörigen Programmen **PSCP**, **PSFTP** usw. verwendet werden. Eine [Anleitung für PuTTY unter Windows](#) zeigt die notwendigen Schritte.

Aufgabe 2



Dokumentieren Sie Ihr Vorgehen mit Script und AsciiDoc und stellen Sie das Ergebnis als PDF-Datei in Ihrem E-Portfolio zur Verfügung.

- Richten Sie eine Linux-VM mit SSH-Server, NAT und einer Port-Weiterleitung ein. Wählen Sie dazu eine Port-Nummer, die von dem Beispiel und anderen Quellen abweicht. Testen Sie wie in [Beispiel 3](#) den SSH-Server über die Port-Weiterleitung.
- Richten Sie eine Linux-VM mit SSH-Server und einem Host-only-Adapter ein. Wählen Sie dazu IP-Adressen, die von den Beispielen und anderen Quellen abweichen. Testen Sie wie in [Beispiel 2](#) den SSH-Server
 - vom Hostsystem sowie
 - von einer zweiten Linux-VM.
- Richten Sie eine Linux-VM mit SSH-Server und einer Netzwerkbrücke ein. Testen Sie wie zuvor den SSH-Server
 - vom Hostsystem sowie
 - von einer zweiten Linux-VM.

6. Secure Copy (scp)

Mit Secure Copy (scp) können Dateien über ein Netzwerk verschlüsselt kopiert werden. Für das folgenden Beispiel müssen zwei VMs miteinander vernetzt (siehe Lernjob [IT-BS-VM-LJ-3.2 Netzwerke mit Virtualbox](#)) und auf dem System mit der IP-Adresse **10.0.3.10** ein SSH-Server eingerichtet sein.

Beispiel 4. Von einer zweiten Linux-VM

```
$ scp srv/index.adoc user@10.0.3.10:srv/ ①
user@10.0.3.10's password:
index.adoc                               100%  95    0.1KB/s   00:00
```

① Kopiert die Datei **srv/index.adoc** in den Ordner **~/srv** auf den SSH-Server mit der IP-Adresse **10.0.3.10**.

Beispiel 5. Von einer zweiten Linux-VM

```
$ scp user@10.0.3.10:srv/index.adoc srv/ ①
user@10.0.3.10's password:
index.adoc                               100%  95    0.1KB/s   00:00
```

① Kopiert die Datei **~/srv/index.adoc** vom SSH-Server mit der IP-Adresse **10.0.3.10** in den Ordner **srv/**.

Aufgabe 3



Dokumentieren Sie Ihr Vorgehen mit Script und AsciiDoc und stellen Sie das Ergebnis als PDF-Datei in Ihrem E-Portfolio zur Verfügung.

- a. Richten Sie eine Linux-VM mit SSH-Server, NAT-Netzwerk und Port-Weiterleitung ein. Wählen Sie dazu eine Port-Nummer und IP-Adressen, die von den Beispielen und anderen Quellen abweichen.
- b. Kopieren Sie Dateien zwischen
 - zwei Linux-VM sowie
 - einer Linux-VM und dem Host über die Port-Weiterleitung.

Kopieren Sie Dateien sowohl zum als auch vom SSH-Server wie in [Beispiel 4](#) und [Beispiel 5](#).