

Ausarbeitung OS-Management

Ausgewähltes Linux Distro: Ubuntu Server 20.04.

Ablauf der Installation des Ubuntu Server

1. Tastatur konfigurieren
 - a. Layout auswählen: Deutsch
 - b. Variante auswählen: Deutsch
2. Netzwerkverbindungen einrichten (Auswahl des NI)
 - a. Default gelassen
3. Konfiguration eines Proxys
 - a. Default gelassen
4. Spiegelserver verwenden
 - a. Default
5. „Guided storage layout“ konfigurieren
 - a. Default
6. Speicher konfigurieren
 - a. Default
7. Benutzer setup
 - a. Eingabe name
 - b. Server name
 - c. Username
 - d. Password
8. SSH Setup
 - a. Installation des SSH-Daemon ,OpenSSH
9. Featured Server Snaps
 - a. Default
10. Installation

Nach der Installation und den Neustart des OS starten wir mit der Konfiguration des SSH-Daemons (OpenSSH).

Konfiguration von OpenSSH:

1. Öffnen des config files:
 - a. Command: `$ sudo vim /etc/ssh/ssh_config`
2. Ändern des Ports für die SSH-Verbindung (Default 22)
 - a. Feld für den SSH-Port auskommentieren und Port angeben
 - i. In meinen Fall: Port 65100
3. Verbindung von non root User autorisieren
 - a. Hierzu müssen sie wieder das Feld PermitRootLogin auskommentieren
 - i. Dann müssen sie nur noch dem Feld PermitRootLogin „no“ anfügen
4. Nun geht es darum in ihren Netzwerkeinstellungen für die VM das Port Forwarding zu aktivieren
 - a. Bei VirtualBox sehen sie einen Tab Maschine. Von hier aus müssen sie auf Ändern->Netzwerk->Erweitert->Port-Weiterleitung gehen
 - b. Das nun folgende Bild zeigt meine persönlichen Einstellungen

Name	Protokoll	Host-IP	Host-Port	Gast-IP	Gast-Port
Rule 1	TCP	127.0.0.1	44444	10.0.2.15	65100

- c. Die Host-IP wäre in meinen Fall die Loopback Adresse
- d. Der Host-Port kann frei gewählt werden
- e. Die lokale IP-Adresse von der VM wird bei der Gast-IP eingetragen
 - i. Falls sie diese nicht wissen geben sie das Command: `$ Ip addr` auf Ihrer VM ein
 1. In meinen Fall ist die IP: 10.0.2.15
- f. Nun bei dem Gast-Port ist es wichtig, dass sie den Port eingabe über den ihre SSH-Service erreichbar ist. Dies haben vorhin in der config Datei für den SSH-Service definiert (in meinem Fall war dies 65100)
 - i. Host-IP = Loopback (127.0.0.1)
 - ii. Host-Port= Beispielweise 44444
 - iii. Lokale IP von VM: 10.0.2.15
 - iv. Der im config file definierte Port: 65100

Nun ist es Ihnen möglich sich zu ihrem Server mittels SSH von ihrer Hostmaschine zu verbinden.

Verbindung zu der VM herstellen mittels SSH

Dazu müssen folgende Schritte beachtet werden:

- 1) Zuerst einmal muss auf ihrer Hostmaschine ein SSH Public Key file generiert werden
 - a) Das Command hierfür: `$ ssh-keygen -t rsa`
 - b) Anschließend werden sie nach dem Speicherort gefragt
 - i) Mit „Enter“ speichern sie den Key Default-Ordner (`/root/.ssh/id_rsa`)
 - c) Ebenso können sie Passphrase definieren
 - i) Falls sie keine haben wollen einfach leer lassen und mit „Enter“ bestätigen
- 2) Nun müssen sie den Public Key von der Hostmaschine an die VM schicken
 - a) Das Command hierfür: `$ scp -P 44444 ~/.ssh/id_rsa.pub tom@127.0.0.1:/home/tom`
 - i) Bei -P: der Host-Port der in den Netzwerkeinstellungen der VM für das Port-Forwarding definiert wurde (in meinem Fall 44444)
 - ii) Dann kommt das Verzeichnis in welcher der SSH Public Key gespeichert wurde
 - iii) Am Schluss führen sie ihren Username an begleitet von ihrer Host-IP Adresse und das Verzeichnis, in dem der Key auf der VM gespeichert werden soll
- 3) Nun müssen sie das Public Key File auf ihrer VM zu den `.ssh/authorized_keys` hinzufügen
 - a) Hierzu geben sie das Command: `cat id_rsa.pub >> .ssh/authorized_keys`
- 4) Nun gehen sie wieder auf ihr SSH Config file, öffnen es `$ sudo vim /etc/ssh/sshd_config` und nehmen folgende Änderungen vor:
 - a) Kommentieren sie „PasswordAuthentication“ aus und ergänzen mit:
`PasswordAuthentication no`
 - b) Kommentieren sie „PubKeyAuthentication“ aus und ergänzen mit: `PubKeyAuthentication yes`
- 5) Nun können sie vom Host aus mittels SSH auf Server verbinden:
 - a) Command: `$ ssh -p 44444 tom@127.0.0.1`

Firewall konfigurieren

1. Zuerst alle Verbindungen zu den Ports unterbinden
 - a. Command: `$ ufw default deny`
2. Nun müssen sie den Port für die einkommenden SSH Verbindungen öffnen
 - a. Hierzu müssen sie den Port, auf den ihr SSH-Service läuft, zulassen
 - b. Command: `$ sudo allow 65100` (Port von SSH auf VM)
3. Um die Firewall dann zu aktivieren
 - a. Command: `$ sudo ufw enable`