

DNS Server installieren

In dieser Übung werden Sie einen DNS-Server installieren und konfigurieren. Hierzu werden Sie auf der AWS Academy Lab-Umgebung einen virtuellen Server (EC2 Instanz) starten. Auf diesem virtuellen Server werden Sie den weitverbreiteten Open-Source DNS Server [Bind](#) installieren.

Sicherheitsgruppe erstellen

Als erstes muss in AWS eine Sicherheitsgruppe erstellt werden. Mit dieser Sicherheitsgruppe wird die Firewall des Servers konfiguriert. Hierbei ist es wichtig, dass wir den eingehenden Datenverkehr für DNS-Pakete zulassen.

1. Starten Sie die [AWS Academy Lab-Umgebung](#).
2. Klicken Sie auf **Services** -> **Datenverarbeitung** um die EC2 Übersicht zu öffnen.
3. Klicken Sie in der Gruppe **Ressourcen** auf **Sicherheitsgruppen** um zur Übersicht mit den Sicherheitsgruppen zu gelangen.

Ressourcen [Info](#) Globale Ansicht von EC2 ↗ ↻ ⚙️

Sie verwenden die folgenden Amazon EC2-Ressourcen in der Region USA Ost (Nord-Virginia):

🔍 Ressourcen nach Tag(s) filtern

Instances (ausgeführt)	0	Dedicated Hosts	0	Elastic IP-Adressen	2
Instances	0	Load Balancers	0	Platzierungsgruppen	0
Schlüsselpaare	4	Sicherheitsgruppen	1	Snapshots	0
Volumes	0				

- Klicken Sie auf den orangenen Button **Sicherheitsgruppe erstellen**.
- Wählen Sie einen passenden Namen wie z. B. DNS-Server. Diese Sicherheitsgruppe können Sie dann für alle DNS-Server verwenden, welche Sie in der AWS-Umgebung erstellen. Setzen Sie ebenfalls eine aussagekräftige Beschreibung wie "Gewahrt den Zugriff fuer DNS-Dienste von extern" (Sonderzeichen sind nicht erlaubt)
- Klicken Sie nun unter **Regeln für eingehenden Datenverkehr** auf **Regel hinzufügen**.
- Fügen Sie nun drei Regeln hinzu. Jeweils eine für **DNS (TCP)**, **DNS (UDP)**, und **SSH**. Setzen Sie bei allen drei Regeln die erlaubte Quelle auf **Anywhere IPv4**:

Regeln für eingehenden Datenverkehr [Info](#)

Typ	Protokoll	Portbereich	Quelle	Beschreibung – optional	
DNS (UDP)	UDP	53	Anywhere... 0.0.0.0/0		Lösche n
DNS (TCP)	TCP	53	Anywhere... 0.0.0.0/0		Lösche n
SSH	TCP	22	Anywhere... 0.0.0.0/0		Lösche n

Regel hinzufügen

- Bei Regeln für ausgehenden Datenverkehr sollte bereits eine Regel existieren für den gesamten Datenverkehr. Diese können Sie so belassen:

Regeln für ausgehenden Datenverkehr [Info](#)

Typ	Protokoll	Portbereich	Ziel	Beschreibung – optional	
Gesamter Datenverkehr	Alle	Alle	Benutz... 0.0.0.0/0		Lösche n

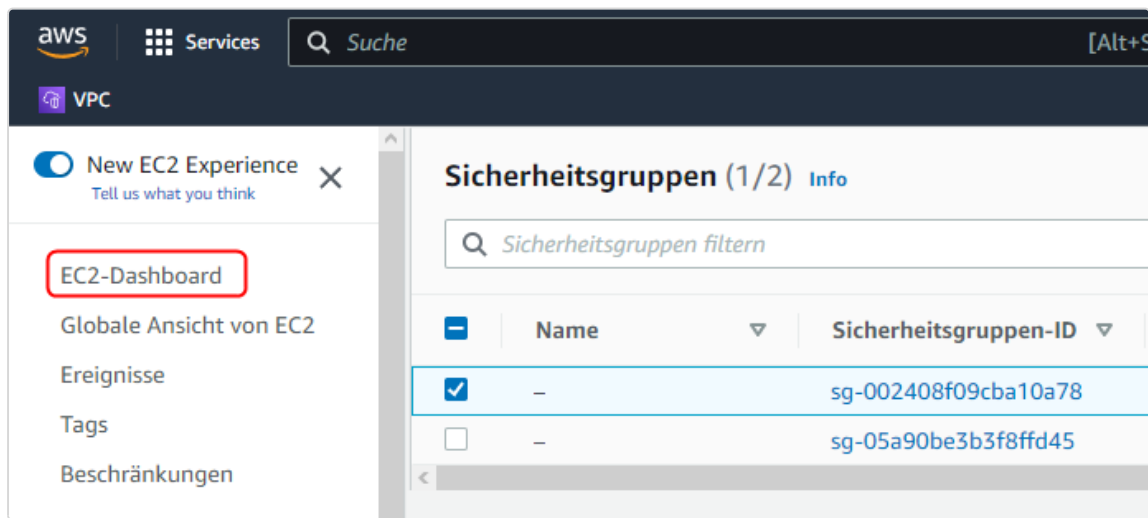
Regel hinzufügen

- Bestätigen Sie nun mit dem orangen Button **Sicherheitsgruppe erstellen**

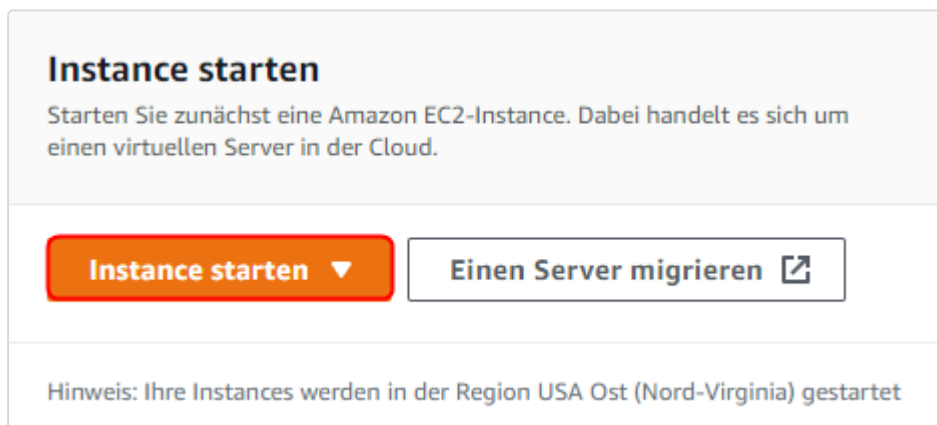
VM anlegen

Nun können Sie als nächsten Schritt eine neue Virtuelle Maschine (EC2 Instanz) anlegen:

- Wechseln Sie wieder in das EC2-Dashboard. Alternativ können Sie im Menü aber auch direkt zu Instances wechseln:



- Klicken Sie nun auf den Button Instance starten:

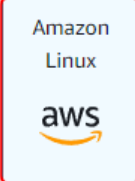


- Wählen Sie einen passenden Namen für Ihren DNS Server.
- Wählen Sie nun Amazon Linux als Server Image aus:

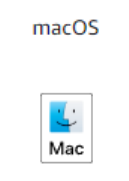
▼ Anwendungs- und Betriebssystemabbilder (Amazon Machine Image) [Info](#)

Ein AMI ist eine Vorlage, die die Softwarekonfiguration (Betriebssystem, Anwendungsserver und Anwendungen) enthält, die zum Starten Ihrer Instance benötigt wird. Suchen Sie nach AMIs, wenn Sie unten nicht sehen, wonach Sie suchen

Schnellstart



Amazon Linux



macOS



Ubuntu



Windows



Red Hat



S

[Weitere AMIs durchsuchen](#)

Einschließlich von AMIs aus AWS, Marketplace und der Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-0b0dcb5067f052a63 (64-Bit (x86)) / ami-01b5ec3ed8678d8b7 (64-Bit (Arm))
Virtualisierung: hvm ENA-aktiviert: true Root-Gerätetyp: ebs

Zur kostenlosen Nutzung berechtigt ▼

Beschreibung

Amazon Linux 2 Kernel 5.10 AMI 2.0.20221103.3 x86_64 HVM gp2

Architektur	AMI-ID	
64-Bit (x86) ▼	ami-0b0dcb5067f052a63	Verifizierter Anbieter

- Wählen Sie den Instanz-Typ **t2.medium** aus.
- Wählen Sie Ihren vorgängig erstellten Gruppen-SSH-Key aus, damit dieser bei der EC2-Instanz hinterlegt wird.

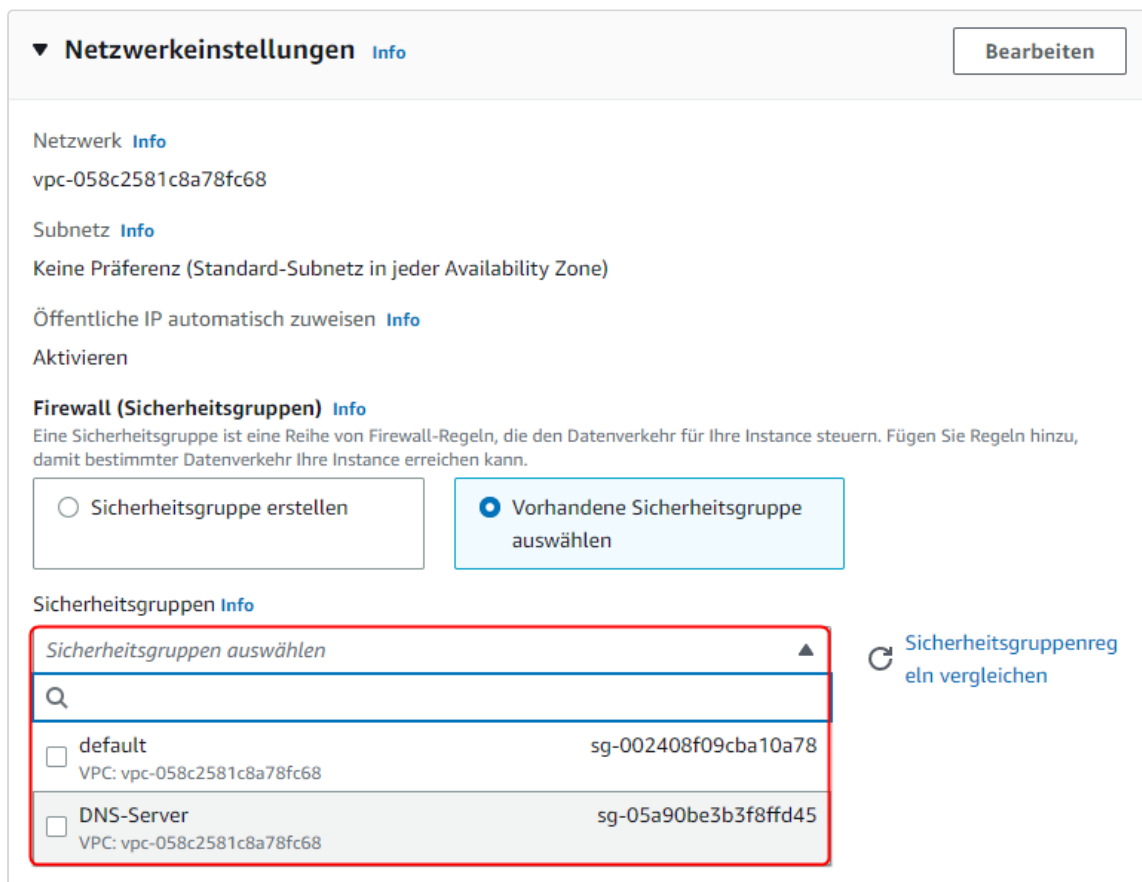
▼ Schlüsselpaar (Anmeldung) [Info](#)

Sie können ein Schlüsselpaar verwenden, um eine sichere Verbindung zu Ihrer Instance herzustellen. Stellen Sie sicher, dass Sie Zugriff auf das ausgewählte Schlüsselpaar haben, bevor Sie die Instance starten.

Schlüsselpaarname - Pflichtfeld

[Neues Schlüsselpaar erstellen](#)

7. Nun können Sie im Abschnitt Netzwerk-Einstellungen die zuvor erstellte Sicherheitsgruppe hinzufügen.



▼ **Netzwerkeinstellungen** [Info](#) Bearbeiten

Netzwerk [Info](#)
vpc-058c2581c8a78fc68

Subnetz [Info](#)
Keine Präferenz (Standard-Subnetz in jeder Availability Zone)

Öffentliche IP automatisch zuweisen [Info](#)
Aktivieren

Firewall (Sicherheitsgruppen) [Info](#)
Eine Sicherheitsgruppe ist eine Reihe von Firewall-Regeln, die den Datenverkehr für Ihre Instance steuern. Fügen Sie Regeln hinzu, damit bestimmter Datenverkehr Ihre Instance erreichen kann.

☐ Sicherheitsgruppe erstellen ☒ Vorhandene Sicherheitsgruppe auswählen

Sicherheitsgruppen [Info](#)

Sicherheitsgruppen auswählen

☐ default sg-002408f09cba10a78
VPC: vpc-058c2581c8a78fc68

☐ DNS-Server sg-05a90be3b3f8ffd45
VPC: vpc-058c2581c8a78fc68

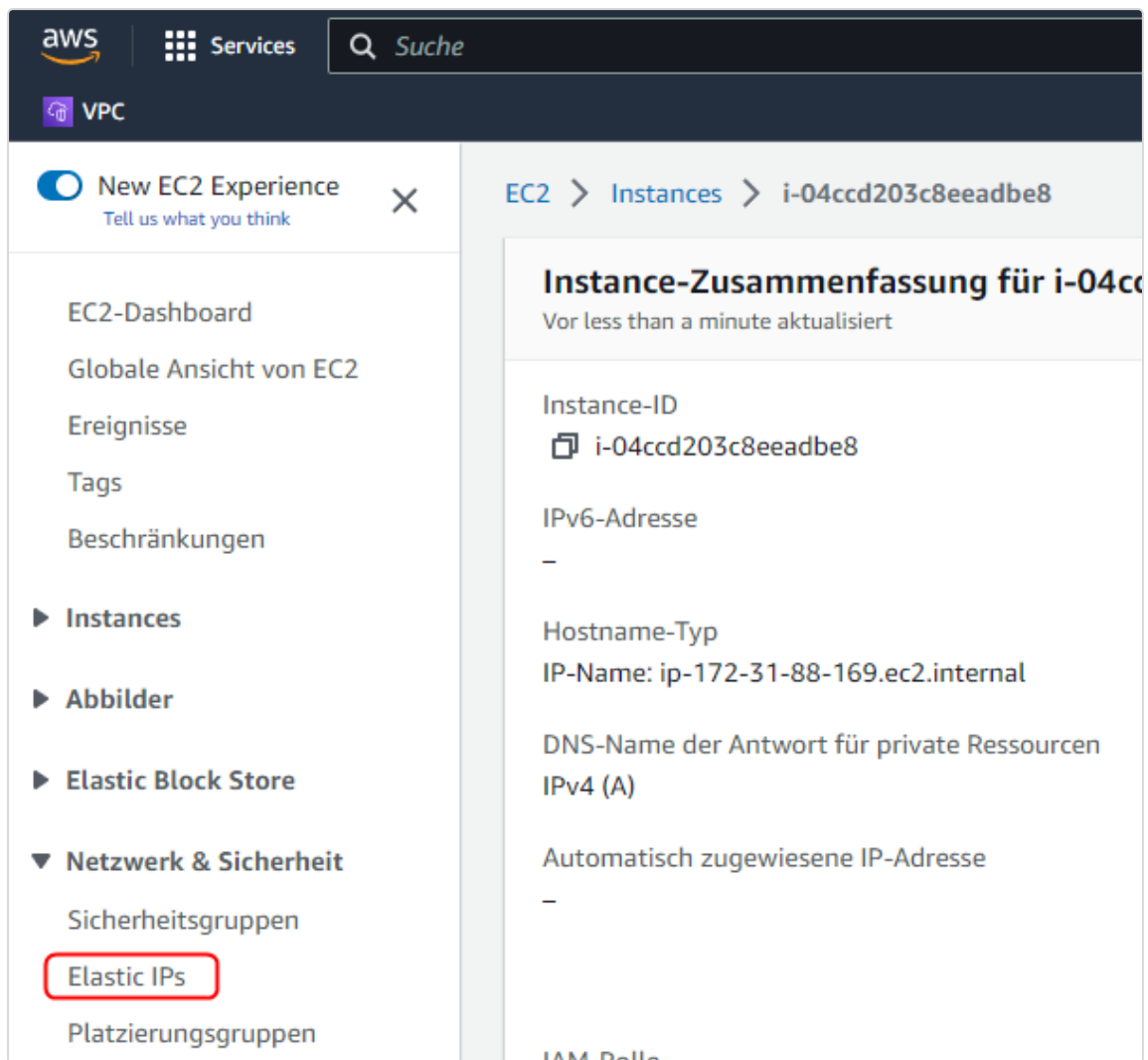
[Sicherheitsgruppenregeln vergleichen](#)

8. Weisen Sie der EC2-Instanz eine statische IP-Adresse zu.

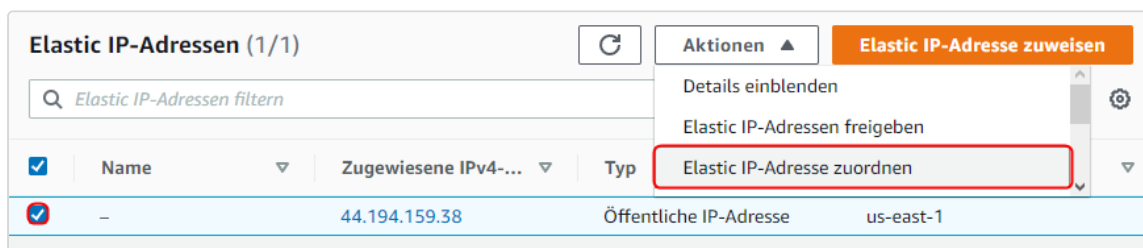
Statische IP-Adresse zuweisen

Standardmässig erhält eine VM keine statische IP-Adresse in AWS. Bei jedem Neustart einer Instanz wird dynamisch eine neue IP-Adresse zugewiesen. Dies ist bei einem Server ungünstig, da dieser immer unter der selben IP-Adresse erreichbar sein sollte. Statische IP-Adressen bei AWS sind eine kostenpflichtige Dienstleistung. Aus diesem Grund müssen Sie nun zu erst eine statische IP-Adresse erstellen und diese dann der erstellten VM zuweisen.

1. Navigieren Sie im Menü zum Punkt **Elastic IPs** in der Gruppe **Netzwerk & Sicherheit**



2. Klicken Sie auf den orangenen Button **Elastic IP-Adresse zuweisen**.
3. Die bereits gesetzten Einstellungen können Sie so belassen. Bestätigen Sie nun mit dem Button **Zuweisen**.
4. Selektieren Sie die neu erstellte IP-Adresse und wählen Sie unter **Aktionen** die Option **Elastic IP-Adresse zuordnen**:



5. Wählen Sie nun unter Instance die zuvor erstellte VM aus:

Elastic IP-Adresse: 44.194.159.38

Ressourcentyp
Wählen Sie die Art der Ressource aus, der die Elastic IP-Adresse zugeordnet werden soll.

☒ Instance
☐ Netzwerkschnittstelle

 Wenn Sie eine Elastic IP-Adresse einer Instance zuordnen, die bereits einer anderen Elastic IP-Adresse zugeordnet ist, wird die Zuordnung für die zuvor zugeordnete Elastic IP-Adresse aufgehoben. Sie bleibt Ihrem Konto jedoch weiterhin zugewiesen. [Weitere Informationen](#)

Instance

i-04ccd203c8eeadbe8 (DNS-SERVER) - running



Private IP-Adresse
Die private IP-Adresse, der die Elastic IP-Adresse zugeordnet werden soll.

Neuzuordnung
Geben Sie an, ob die Elastic IP-Adresse einer neuen Ressource zugeordnet werden kann, wenn sie bereits einer anderen Ressource zugeordnet ist.

☐ Neuzuordnung dieser elastischen IP-Adresse zulassen

6. Bestätigen Sie die Aktion mit dem Button **Zuordnen**.

7. Wechseln Sie zurück zur Instanz. Nun sollte die öffentliche IP-Adresse zugeordnet sein:

Instance-Zusammenfassung für i-04ccd203c8eeadbe8 (DNS-SERVER) Info	
Vor less than a minute aktualisiert	
Instance-ID  i-04ccd203c8eeadbe8 (DNS-SERVER)	Öffentliche IPv4-Adresse  44.194.159.38 offene Adresse
IPv6-Adresse -	Instance-Status  Läuft

Verbindung mit einem SSH-Client

Es ist am bequemsten per SSH auf einem Server zu arbeiten. Dazu haben Sie ein lokales Terminal auf Ihrem Gerät, welches eine SSH-Verbindung zum Server aufbaut.

Das kryptographische Netzwerkprotokoll Secure Shell (SSH) ermöglicht es, Netzwerkdienste über unsichere Netzwerke sicher zu betreiben. Mit SSH kann man eine lokale Kommandozeile auf einen entfernten

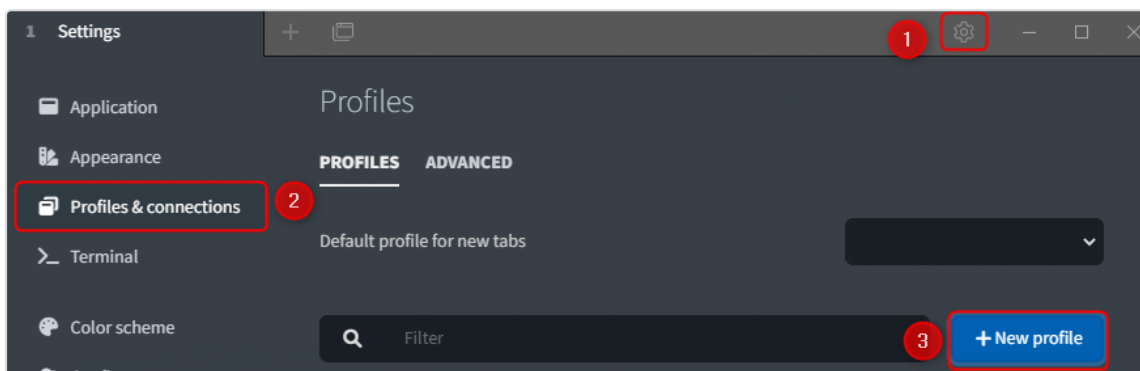
Rechner setzen, auf welchem dann die Ausgaben der entfernten Konsole angezeigt und lokale Tastatureingaben an den entfernten Rechner gesendet werden. Dadurch kann man z. B. einen Server, der in einem entfernten Rechenzentrum steht, fernwarten. Mit der neueren Protokollversion SSH-2 sind weitere Funktionen wie die Datenübertragung per SFTP verfügbar.

Sie dürfen natürlich jedes Terminal verwenden. Diese Anleitung zeigt die Konfiguration anhand vom Tabby Terminal. Es ist aber auch möglich die Verbindung mit Putty oder einem

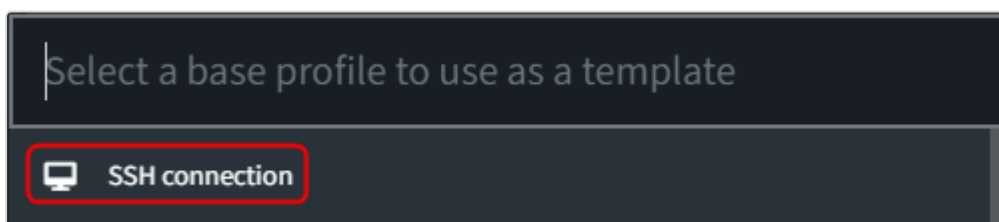
1. Laden Sie die Software Tabby Terminal von folgender Seite herunter und installieren Sie diese: <https://tabby.sh>

Laden Sie die Version **tabby-1.0.187-setup-x64.exe** herunter.

2. Starten Sie die Software und öffnen Sie die Einstellungen. Navigieren Sie dort zu **Profiles & connections** und fügen Sie ein neues Profil hinzu:



3. Sie müssen nun ein Basis-Profil als Vorlage auswählen. Nehmen Sie hier **SSH connection**:



4. Nun tragen Sie **ihre öffentliche IP-Adresse** (44.194.159.38 ist nur ein Beispiel) sowie den Port 22 ein. Als Benutzername setzen Sie **ec2-user**. Als Authentifizierungs-Methode Wählen Sie **Key**. Nun können Sie über den Button **Add a private key** den Gruppenschlüssel hinzufügen.

SSH DNS-Server

Name

SSH DNS-Server

Group

Ungrouped

Icon

fas fa-desktop 

Color

#000000

Disable dynamic tab title ☐

Connection name will be used instead

GENERAL PORTS ADVANCED CIPHERS LOGIN SCRIPTS

Host

44.194.159.38

Port

22

Username

ec2-user

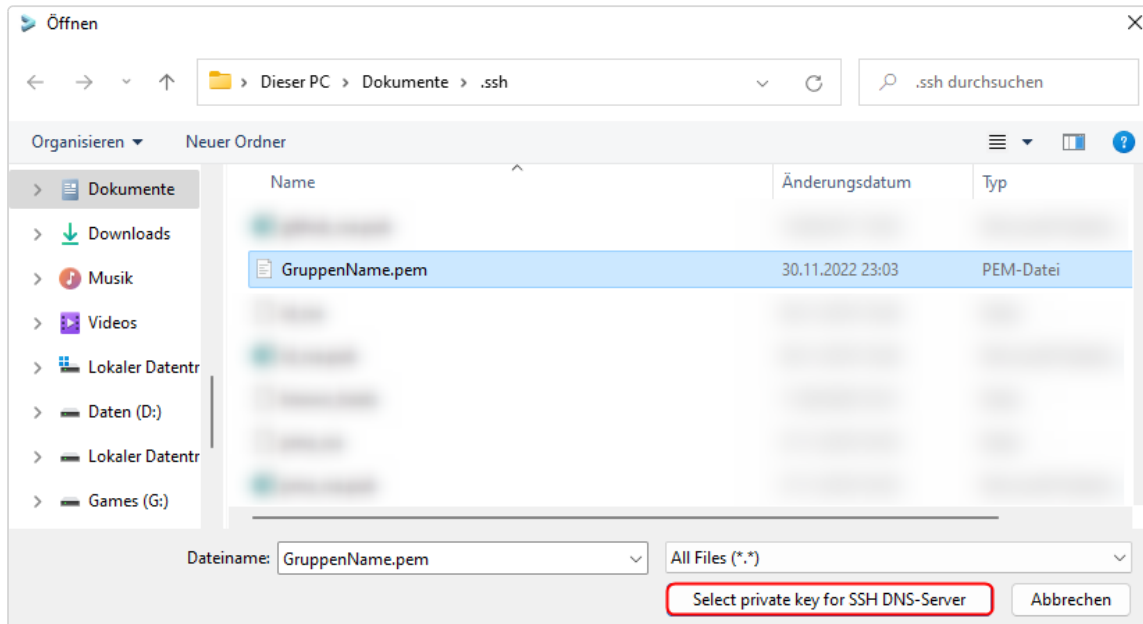
Authentication method

 Auto  Password  **Key**  Agent  Interactive

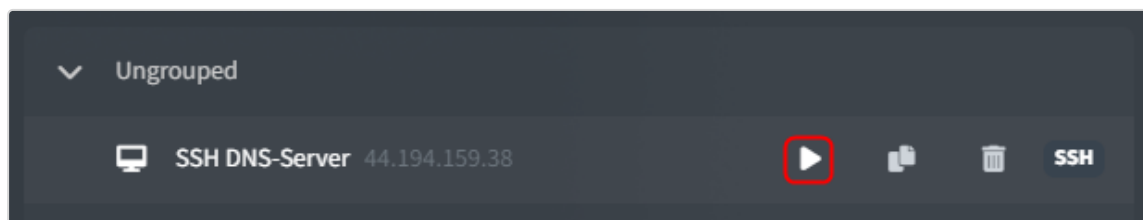
Private keys

 Add a private key

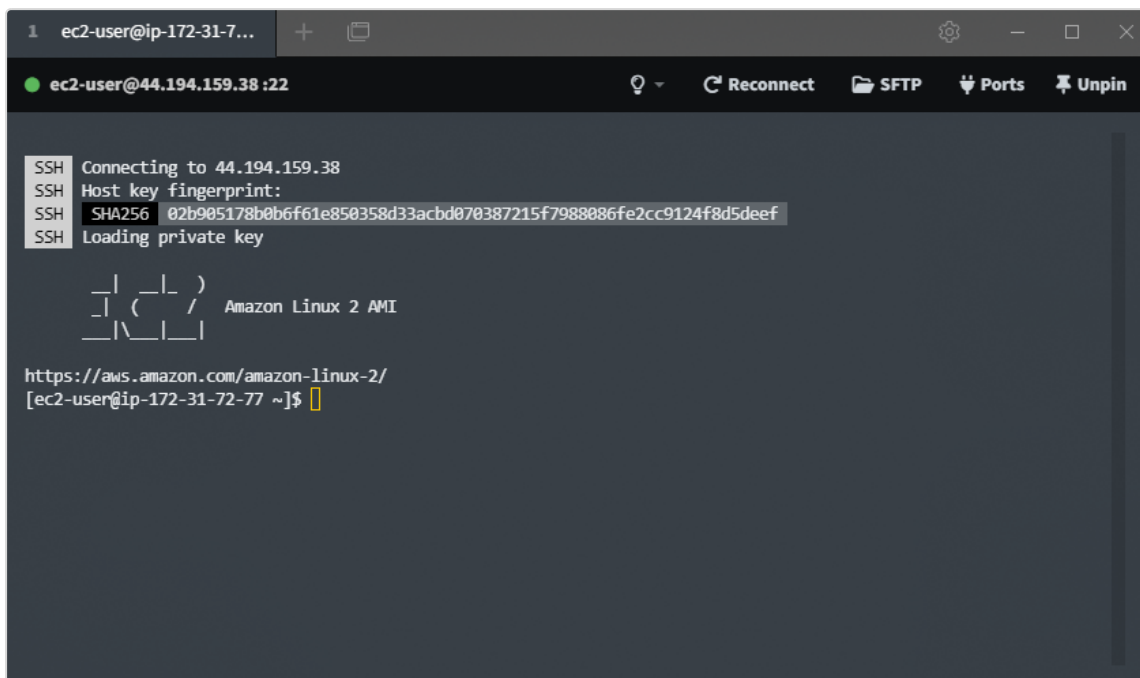
5. Wählen Sie hier den Gruppenschlüssel, welchen Sie vom Gruppenleiter erhalten haben sollten:



6. Speichern Sie das Profil und starten Sie anschliessend die Verbindung:



7. Möglicherweise müssen Sie nun den Host-Fingerprint bestätigen. Speichern Sie den Fingerprint und fahren sie fort.
8. Die Verbindung sollte nun möglich sein und Sie sollten den Willkommens-Bildschirm sehen:



```
1 ec2-user@ip-172-31-7... + [ ]
ec2-user@44.194.159.38 :22 [ ? ] Reconnect [ SFTP ] [ Ports ] [ Unpin ]

SSH Connecting to 44.194.159.38
SSH Host key fingerprint:
SSH SHA256 02b905178b0b6f61e850358d33acbd070387215f7988086fe2cc9124f8d5deef
SSH Loading private key

  _ | _ | _ )
  _ | ( _ /  Amazon Linux 2 AMI
  _ | \ | _ |

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-72-77 ~]$
```

DNS Server (Bind) installieren

1. Verbinden Sie sich per SSH von Ihrem lokalen Terminal auf den Server.
2. Wechseln Sie direkt in den Administrator-Modus mit **sudo su**
3. Installieren Sie nun über die Paketverwaltung **yum** die Software **bind**:

```
yum install bind
```

Yum wird Ihnen dann eine Auflistung der zu installierenden bind-Version inkl. aller Abhängigkeiten anzeigen. Bestätigen Sie die Installation indem Sie **y** eintippen.

```
Install 1 Package (+8 Dependent packages)
Total download size: 4.2 M
Installed size: 11 M
Is this ok [y/d/N]: y
```

Sie können nachvollziehen, wie **yum** nun die Software bind installiert.

4. Verifizieren Sie nun, dass **bind** installiert ist. Mit dem Befehl **yum list installed** können Sie eine Liste aller installierte Softwarepakete einsehen:

```
yum list installed
```

Sie sehen nun eine Liste mit allen installierten Softwarepaketen

```
# yum list installed
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Installed Packages
GeoIP.x86_64                                1.5.0-11.amzn2.0.2      installed
PyYAML.x86_64                              3.10-11.amzn2.0.2      installed
acl.x86_64                                 2.2.51-14.amzn2        installed
acpid.x86_64                               2.0.19-9.amzn2.0.1     installed
amazon-linux-extras.noarch                 2.0.1-1.amzn2          installed
amazon-linux-extras-yum-plugin.noarch      2.0.1-1.amzn2          installed
amazon-ssm-agent.x86_64                    3.1.1732.0-1.amzn2     installed
[...]
```

Wie Sie sicherlich bemerkt haben, ist die Liste sehr lange. Aus diesem Grund werden Sie nun den Output mit dem Befehl **grep** nach **bind** filtern. Hierzu fügen Sie hinter dem bereits bestehenden Befehl einen weiteren Befehl an, mit dem Zeichen **|** übergeben Sie die Ausgabe aus dem vorhergehenden Befehl an den nachfolgenden.

```
yum list installed | grep bind
```

Sie erhalten nun eine List, welche nach dem Stichwort **bind** gefiltert ist.

```
# yum list installed | grep bind
bind.x86_64                                32:9.11.4-26.P2.amzn2.5.2 @amzn2-core
bind-export-libs.x86_64                    32:9.11.4-26.P2.amzn2.5.2 installed
bind-libs.x86_64                           32:9.11.4-26.P2.amzn2.5.2 installed
bind-libs-lite.x86_64                      32:9.11.4-26.P2.amzn2.5.2 installed
bind-license.noarch                        32:9.11.4-26.P2.amzn2.5.2 installed
bind-utils.x86_64                          32:9.11.4-26.P2.amzn2.5.2 installed
rpcbind.x86_64                             0.2.0-44.amzn2         installed
```

Nun ist die Liste etwas übersichtlicher.

Nun ist die Software bind installiert. Im nächsten Kapitel werden Sie den Dienst starten und die Konfiguration genauer unter die Lupe nehmen.

Verwendete Befehle

yum: Mit der Paketverwaltung yum können Sie ganz einfach Software auf Ihrem RHEL-Basierten Linux installieren (rhel, centos, Amazon linux, fedora). Yum organisiert die Software in sogenannten Repositories. Dies sind Verzeichnisse, in denen bekannte Software zur Verfügung gestellt wird. In den Standard-Repositories sind die am meisten verwendeten Softwarepakete vorhanden. Weiter können aber zusätzliche Software-Repositories eingebunden werden, damit auch eine spezielle Software installiert werden kann. Im Rahmen dieses Moduls ist dies aber nicht nötig.

yum stellt eine Reihe von Befehlen zur Verfügung, um Software auf dem Server zu verwalten:

- `yum list <package>` Liste der installierten und verfügbaren Paketen <package>
- `yum list all` Liste aller installierten und verfügbaren Pakete
- `yum list available <package>` Liste aller verfügbaren und installierbaren Pakete
- `yum list updates <package>` Liste aller verfügbaren Pakete <package>, die aktueller als die installierten sind
- `yum list installed <package>` Liste aller installierten Pakete <package>
- `yum info <package>` Kurzbeschreibung zu installierten und verfügbaren Paketen <package>
- `yum search <zeichenkette>` Paketnamen und Beschreibungen durchsuchen nach <zeichenkette>
- `yum install <package>` Installiere die aktuellste Version der Pakete <package> (inkl. der abhängigen!)
- `yum check-update` gibt es aktuellere Pakete in den Repos?
- `yum update` aktualisiere alle z.Z. installierten Pakete
- `yum update <package>` aktualisiere die Pakete <package> (inkl. der abhängigen!)
- `yum erase <package>` deinstalliere Pakete <package> (inkl. aller abhängigen Pakete!)
- `yum remove <package>` deinstalliere Pakete <package> (inkl. aller abhängigen Pakete!)

In anderen Linux-Distributionen kommen andere Paketverwaltungen zum Einsatz. Debian derivative (debian, ubuntu, kali linux) haben mit **apt-get** ein sehr ähnliches Tool zur Verfügung.

grep: Der Befehl grep ist ein Linux-Befehl, der dazu verwendet wird, um Zeichenfolgen in Textdateien zu suchen. Es durchsucht Dateien nach bestimmten Zeichenketten, die angegeben wurden, und gibt alle

Zeilen zurück, in denen es die angegebene Zeichenfolge gefunden hat. Es kann auch dazu verwendet werden, um einzelne Dateien oder mehrere Dateien nach den angegebenen Zeichenketten zu durchsuchen.

pipe: Dies ist ein Begriff, der sich aus dem englischen Wort "Pipeline" ableitet, was übersetzt so viel wie "Rohrleitung" bedeutet. Unter Linux bildet eine Pipe einen Datenstrom zwischen zwei Prozessen, die nicht immer miteinander verbunden sind. Dies bedeutet, dass das Ergebnis (Ausgabe) eines Programms als Eingabe für ein anderes Programm genutzt werden kann. Dadurch können größere Aufgaben in kleinere Teilaufgaben aufgeteilt werden, um eine bessere Übersicht zu erhalten.

Revision #14

Created 17 October 2022 16:26:58 by Admin

Updated 15 December 2022 12:26:14 by Admin