

Cloud EC2-Service Lift and shift

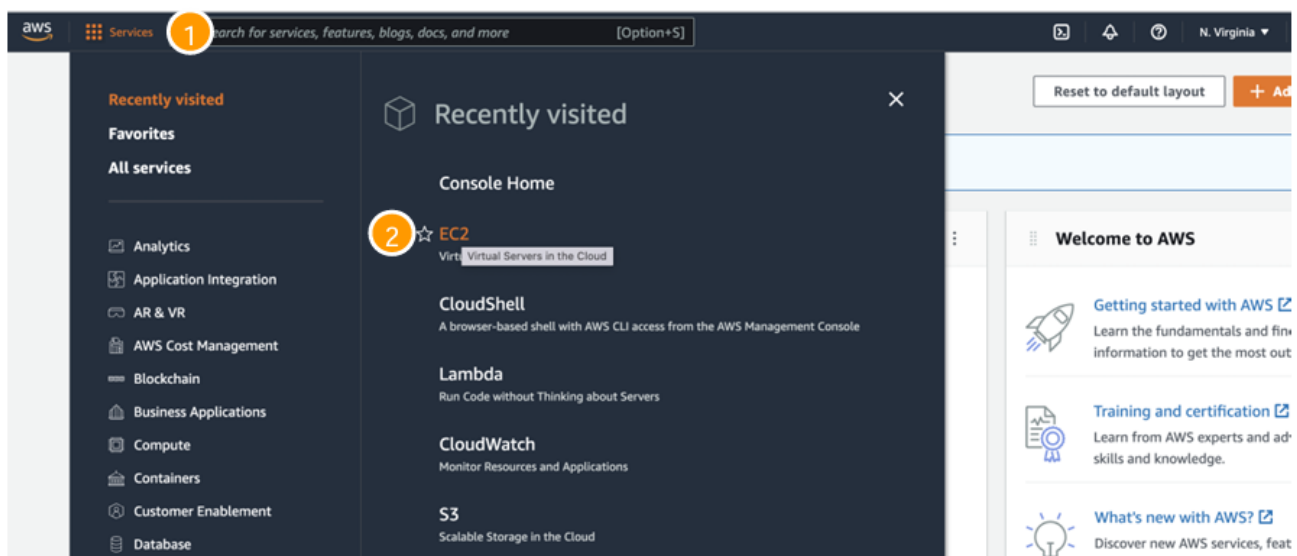
Zugriff auf EC2 Dashboard von AWS

öffnen

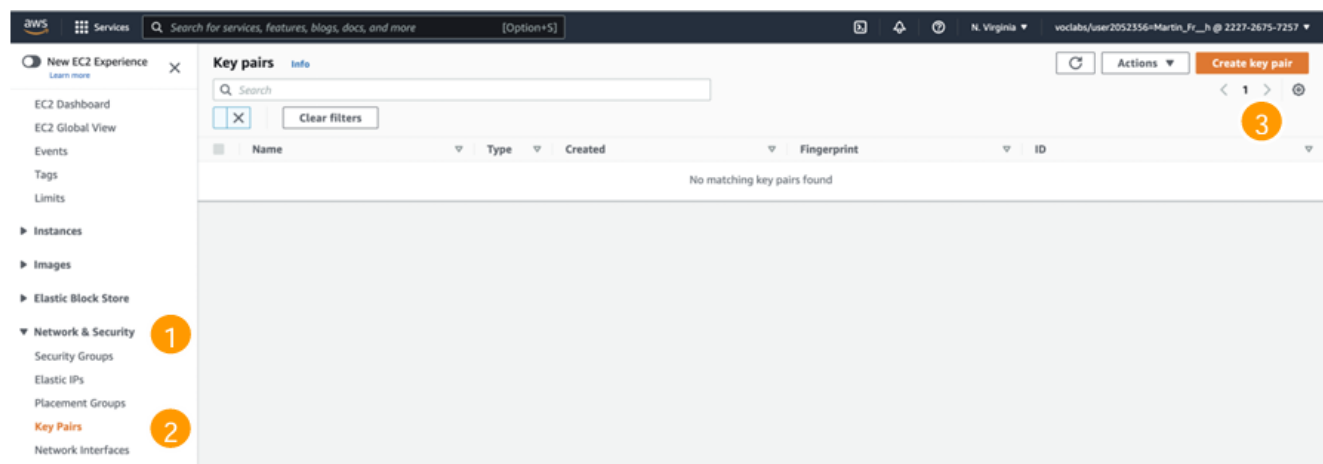
[https://awsacademy.instructure.com/courses/68933?](https://awsacademy.instructure.com/courses/68933?invitation=awAvJEA6z8OXXZAr22JG7SCqo9AlCWjYO9kfVv)

[invitation=awAvJEA6z8OXXZAr22JG7SCqo9AlCWjYO9kfVv](#)

und dann



SSH Keypair erstellen



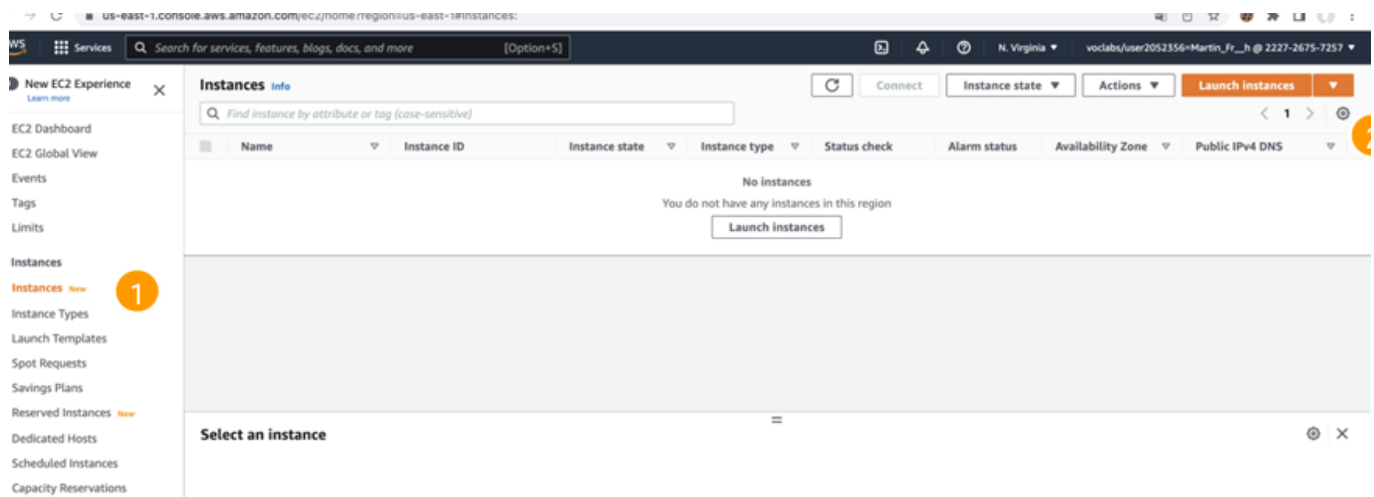
The screenshot shows the 'Create key pair' page in the AWS Management Console. The breadcrumb navigation is 'EC2 > Key pairs > Create key pair'. The page title is 'Create key pair' with an 'Info' link. Below the title is a 'Key pair' section with a description: 'A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.' The form includes a 'Name' field with the value 'GbsAws', a 'Key pair type' section with 'RSA' selected, and a 'Private key file format' section with '.pem' selected. There is also a 'Tags - optional' section with an 'Add new tag' button. At the bottom right are 'Cancel' and 'Create key pair' buttons.

Name GbsAws\$

Private key file format: .pem -> Mit Button "Create key pair" abschliessen

Schlüssel wird erstellt und automatisch heruntergeladen. -> Private Key auf dem lokalen Rechner sichern (z.B. c:\users<user>.ssh)

Ubunte VM erstellen



instances (1) -> Launch instances (2)

Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags [Info](#)

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Recents

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

S

>

Q

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-052efd3df9dad4825 (64-bit (x86)) / ami-070650c005cce4203 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible ▼

Name: myWebServer

Application and OS Images: Ubuntu

▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

Free tier eligible ▼

[Compare instance types](#)

Auswahl von t2.micro (Free tier)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

[Create new key pair](#)

Key pair -> GbsAws (Key pair wurde im 1. Schritt erstellt)

3 / 8

▼ Network settings Info Edit

Network Info
vpc-02706859a1813c3d6

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ Allow SSH traffic from
Helps you connect to your instance
Anywhere
0.0.0.0/0

☐ Allow HTTPs traffic from the internet
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

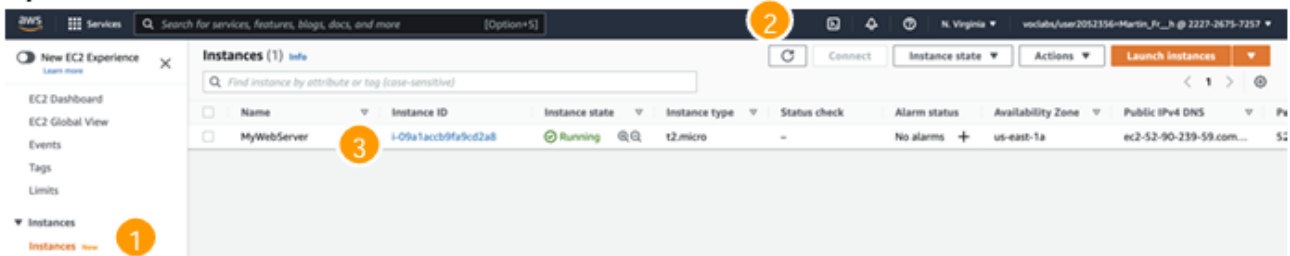
“Create Security group” wählen

“Allow SSH traffic from” aktivieren und “Anywhere 0.0.0.0/0” auswählen

Cancel Launch instance

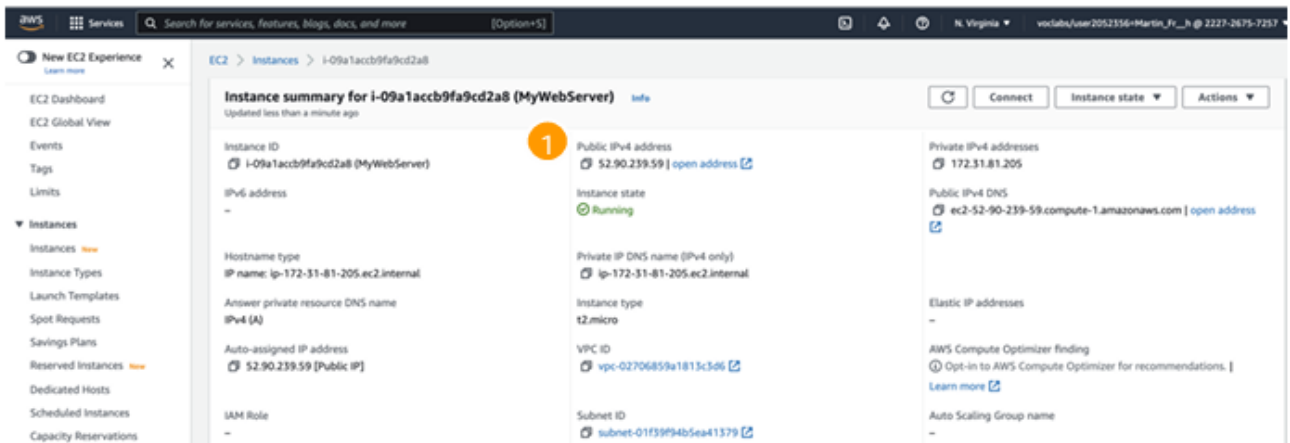
Instanz mit Launch instance erstellen.

VM testen



Instances (1) -> Refresh* (2) -> MyWebServer (3)

* Es dauert manchmal einige Sekunden, bis die VM bereit ist und in der Liste angezeigt wird.



Public IPv4 address (1) kopieren

Auf Lokalem PC ssh-Verbindung prüfen

```
ssh -i c:\users\<user>\.ssh\GbsAws.pem ubuntu@<Public IPv4>
```

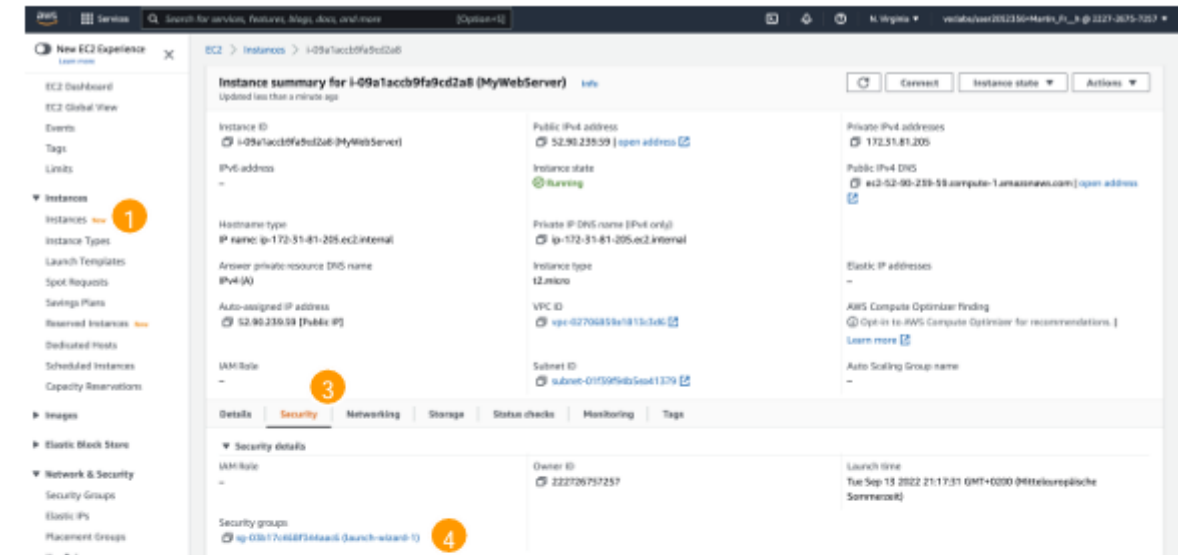
Apach Verbindung erstellen

Über ssh-Verbindung folgende Befehle ausführen

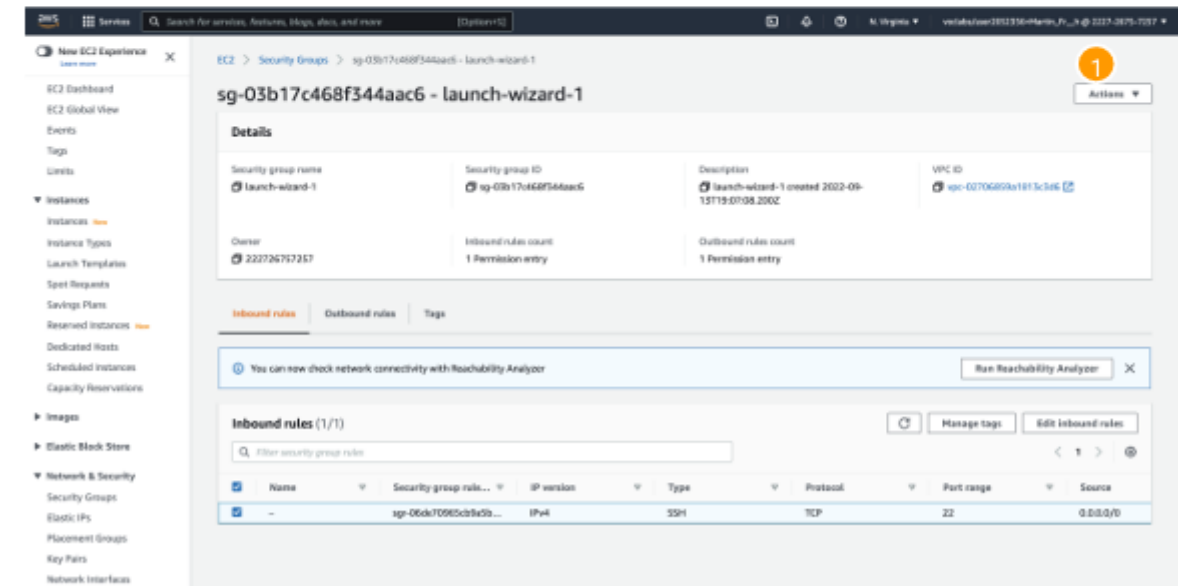
```
sudo apt update
sudo apt install apache2
sudo chmod 777 /var/www/html/index.html
```

Firewall konfigurieren

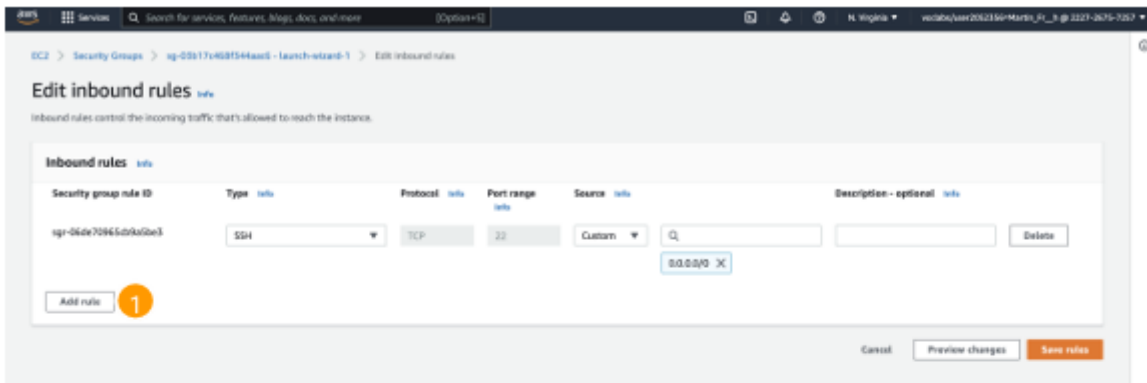
Damit von Aussen auf den Webserver zugegriffen werden kann, muss eine Firewall-Regel für Inbouded HTTP konfiguriert werden:



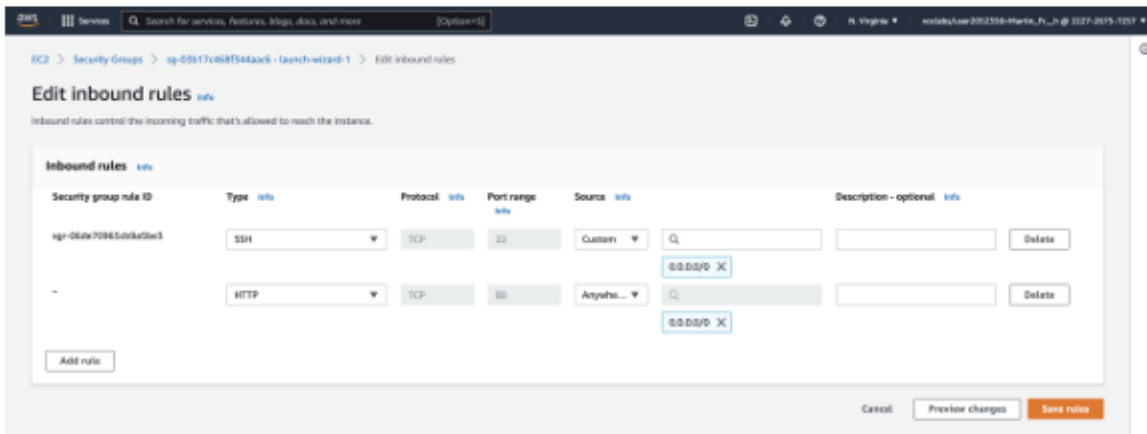
Instances (1) -> MyWebServer -> Security (3) -> <verknüpfte Security group> (4)



Actions (1) -> Edit inbound rules



Add rule (1)



Type: HTTP
Port range 80
CIDR blocks 0.0.0.0/0

-> Save rules

Apache Webserver testen

Test über einen beliebigen Browser (8-ung: kein HTTPS)

<Public IPv4>:80



Index.html Datei erstellen

Erstellte lokale index.html – Datei mit Datei auf dem Apache-Server ersetzen:

```
scp -i c:\users\<user>\.ssh\GbsAws.pem index.html ubuntu@<Public  
IPv4>:/var/www/html
```

Test über einen Belibigen Browser

:80