

M346, VM mit Apache auf Cloud.

Thema:

Cloud, EC2-Service Lift and shift

Lernziele

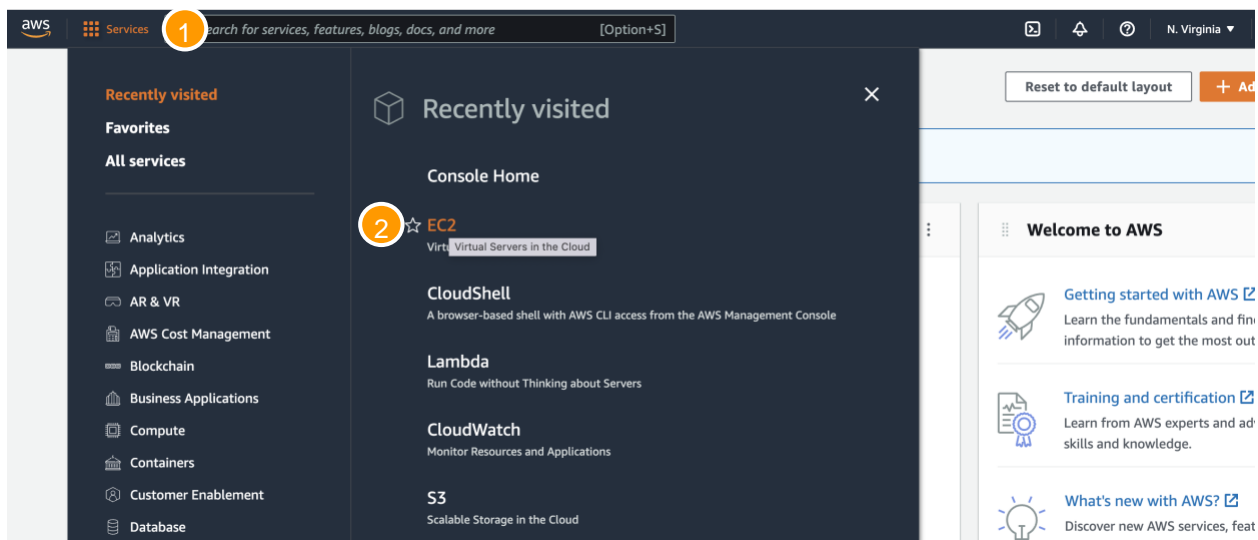
- Sie lernen das AWS-Cloud Learning Lab kennen
- Sie erstellen eine VM mit einem Apache-Webserver der Cloud
- Sie richten die Firewall so ein, dass ein Zugriff auf den Webserver von Aussen möglich ist
- Sie transferieren eine einfache Website auf den erstellten Webserver

Sozialform

Einzelarbeit oder Arbeit im Zweierteam

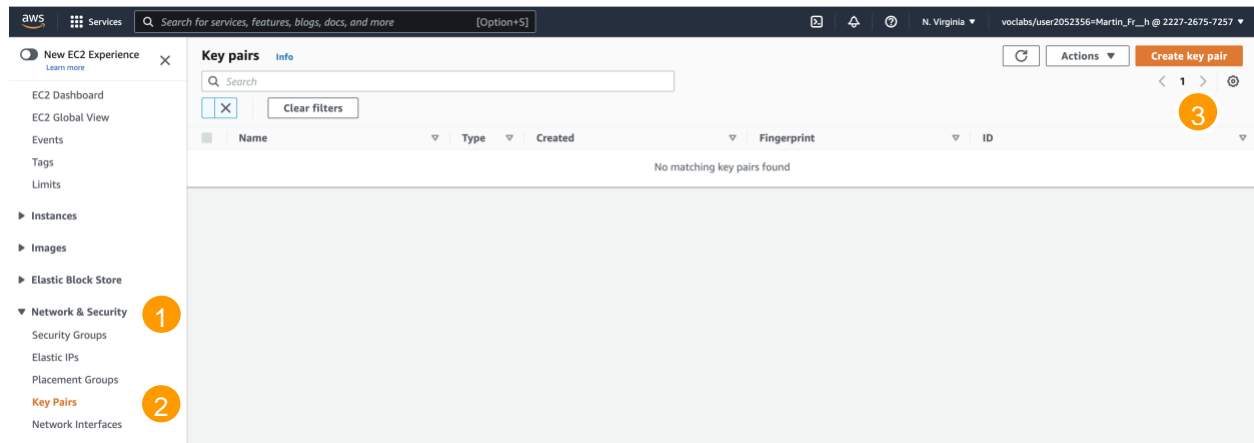
Zugriff auf EC2 Dashboard von AWS

AWS-Dashboard öffnen

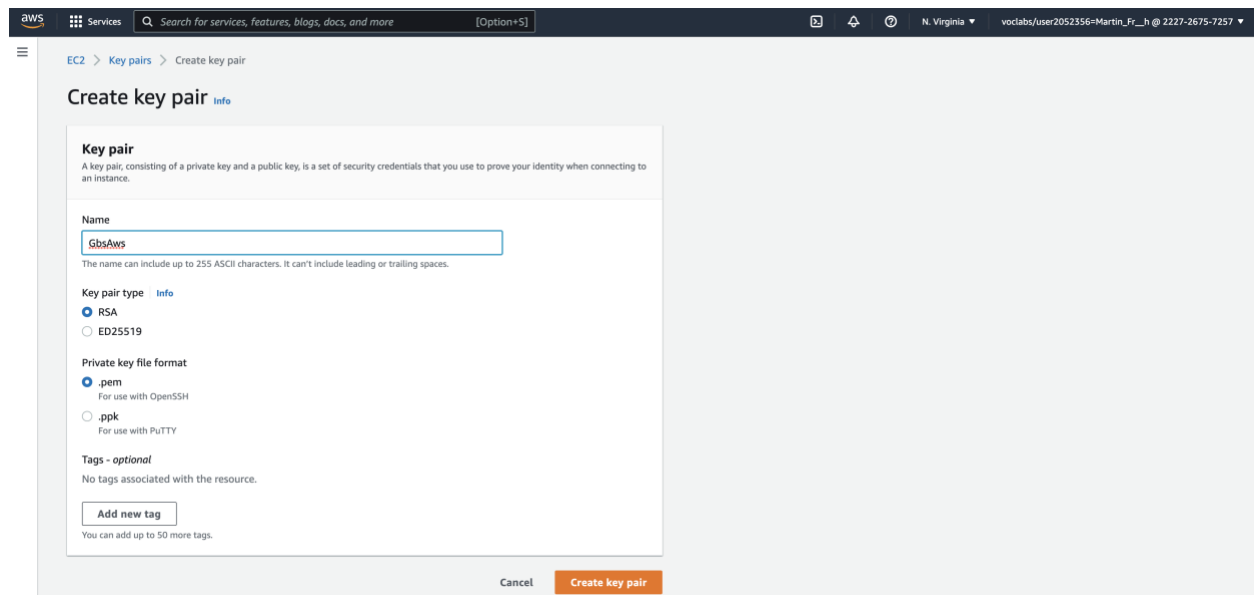


Services (1) -> EC2 (2)

1) SSH Keypair erstellen



Network & Security (1) -> Key Pairs (2) -> Create Key Pair (3)



Name: GbsAws\$

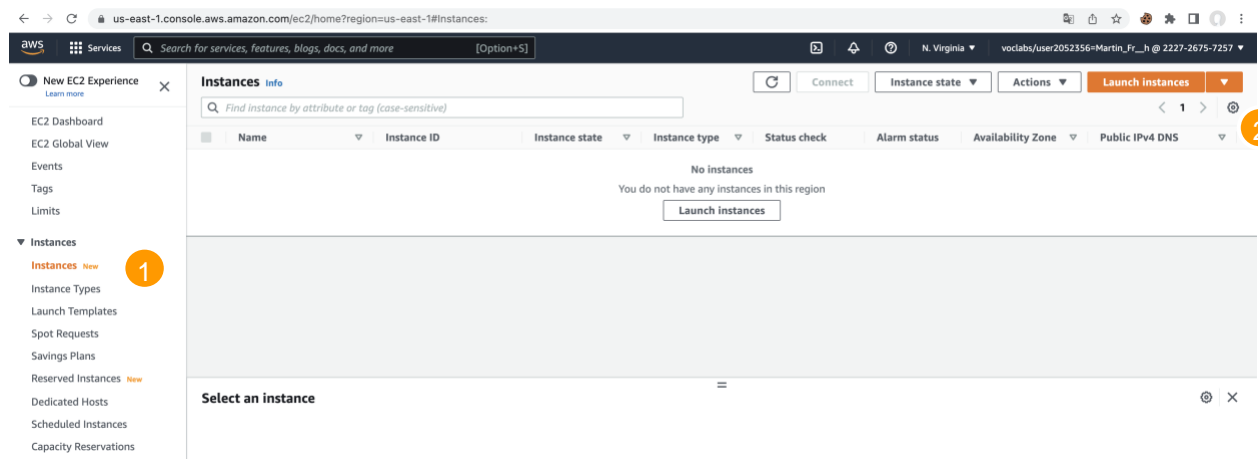
Private key file format: .pem

-> 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)

2) Ubuntu 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.

Search:

Recents | **Quick Start**

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type
ami-052ef3d9dad4825 (64-bit (x86)) / ami-070650c005c4203 (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 Free tier eligible [Compare instance types](#)

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

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

GbsAws [Create new key pair](#)

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

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.

3) 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\\.ssh\GbsAws.pem ubuntu@<Public IPv4>
```

4) Apache installieren

Über ssh-Verbindung, folgende Befehle ausführen:

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

5) Firewall konfigurieren

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

The screenshot shows the AWS Management Console interface for an EC2 instance named 'MyWebServer'. The instance is in a 'Running' state. The 'Security' tab is selected, showing the 'IAM Role' as 'sg-03b17c468f344aac6 (launch-wizard-1)'. The 'Security groups' section shows the same group. The 'Owner ID' is '222726757257'. The 'Launch time' is 'Tue Sep 13 2022 21:17:31 GMT+0200 (Mitteleuropäische Sommerzeit)'.

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

The screenshot shows the AWS Management Console interface for a security group named 'sg-03b17c468f344aac6 - launch-wizard-1'. The 'Inbound rules' tab is selected, showing a single rule for SSH access on port 22. The rule is named 'sgr-06de70965cb9a5b...' and is of type 'SSH' with protocol 'TCP' and port range '22'. The source is '0.0.0.0/0'.

Actions (1) -> Edit inbound rules

aws Services Search for services, features, blogs, docs, and more [Option+S] N. Virginia voclabs/user2052356=Martin_Fr_h @ 2227-2675-7257

EC2 > Security Groups > sg-03b17c468f344aac6 - launch-wizard-1 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	
sg-06de70965cb9a5be3	SSH	TCP	22	Custom		Delete
<input type="text" value="0.0.0.0/0"/>						

Add rule **1**

Cancel Preview changes **Save rules**

Add rule (1)

aws Services Search for services, features, blogs, docs, and more [Option+S] N. Virginia voclabs/user2052356=Martin_Fr_h @ 2227-2675-7257

EC2 > Security Groups > sg-03b17c468f344aac6 - launch-wizard-1 > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type <small>Info</small>	Protocol <small>Info</small>	Port range <small>Info</small>	Source <small>Info</small>	Description - optional <small>Info</small>	
sg-06de70965cb9a5be3	SSH	TCP	22	Custom		Delete
<input type="text" value="0.0.0.0/0"/>						
-	HTTP	TCP	80	Anywhere...		Delete
<input type="text" value="0.0.0.0/0"/>						

Add rule

Cancel Preview changes **Save rules**

Type: HTTP
Port range 80
CIDR blocks 0.0.0.0/0

-> Save rules

6) Apache Webserver testen

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

<Public IPv4>:80



7) Index html ändern

Index.html – Datei erstellen

```
<html>
  <head>
    <title>Meine Testseite</title>
  </head>
  <body>
    <p>Hallo GBS</p>
  </body>
</html>
```

`scp -i c:\users\Ajnur-ksb\.ssh\GbsAws.pem C:\Users\Ajnur-ksb\Downloads\index.html ubuntu@54.91.59.93:/var/www/html`

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
```

[hier Pfad eingeben](#)

Test über einen beliebigen Browser

[<Public IPv4>:80](#)



[Schlüssel andere Berechtigung \(M346\):](#)

1. Rechte Maustaste auf den KEY
2. Eigenschaften
3. Sicherheit
3. Erweitert klicken
4. Vererbung Deaktivieren
5. Das 1. Anklicken
6. Übernehmen
7. Ok
8. Zurück zu den Eigenschaften
9. Erweitert
10. ALLE ENTFERNEN AUS DEIN USER

[Ordner hochladen - Permission denied \(bzw. Berechtigung auf Webserver ändern\)](#)

root wird auf ubuntu gemacht

1. `ubuntu@ip-172-31-35-19:~$ ls -l /var/www`
2. `ubuntu@ip-172-31-35-19:~$ sudo chown -R ubuntu /var/www`
3. `ubuntu@ip-172-31-35-19:~$ ls -l /var/www`

[ALLE ORDNER + EINZELN FILE HOCHLADEN](#)

`scp -r -i c:\users\Ajnur-ksb\.ssh\GbsAws.pem "C:\Software_VMs\M346_test\myWebsiteCode\index.html" ubuntu@34.229.101.235:/var/www/html`