

Initiatie AWS Cloud

Inleiding	2
Initiatie in AWS Cloud	3
a. Een SSH-keypair maken in de Cloud Shell	3
b. De keys gebruiken in Powershell op je laptop	7
c. De keys in de AWS-omgeving brengen	8
d. Een nieuw Virtual Private Cloud aanmaken	14
e. Cloud Instances in dit nieuwe subnet van een publiek IP voorzien en publieke DNS naam	31
f. Cloud Instances in dit nieuwe subnet (eigenlijk VPC) voorzien van een publieke DNS naam	33
g. Een Ubuntu 22.04 -Compute-instance aanmaken	36
h. Cloud instance een vast Publiek IP adres geven	43
i. Over SSH verbinden met de server	48
j. Waarom werkt de SSH out-of-the-box?	53
k. Hoe komt de instance aan een Private IP-adres?	58
l. Uitzetten van de systembell in de Ubuntu instance	59
m. De webserver installeren	60
n. De webserver lokaal testen	62
o. De webserver vanop de laptop testen en Firewall aanpassen	64
p. De Webserver een Publieke DNS-naam geven	71
q. HTTPS met Let's Encrypt en publieke DNS	77
Eindpresentatie	87

Inleiding

Deze taak wordt gemaakt per student. Iedere student heeft dus zijn eigen Cloud en Cloud-instance.

De opdracht wordt volledig uitgewerkt op het AWS-platform.

We beginnen met het begin, namelijk een initiatie in AWS Cloud Infrastructure.

Je zal alles zelf moeten uitvoeren om jouw cloud-infrastructuur op te zetten.

In een eindpresentatie (zie achteraan dit document) toon je aan dat je alles hebt gemaakt en dat je de verschillende onderdelen hebt begrepen.

Initiatie in AWS Cloud

a. Een SSH-keypair maken in de Cloud Shell

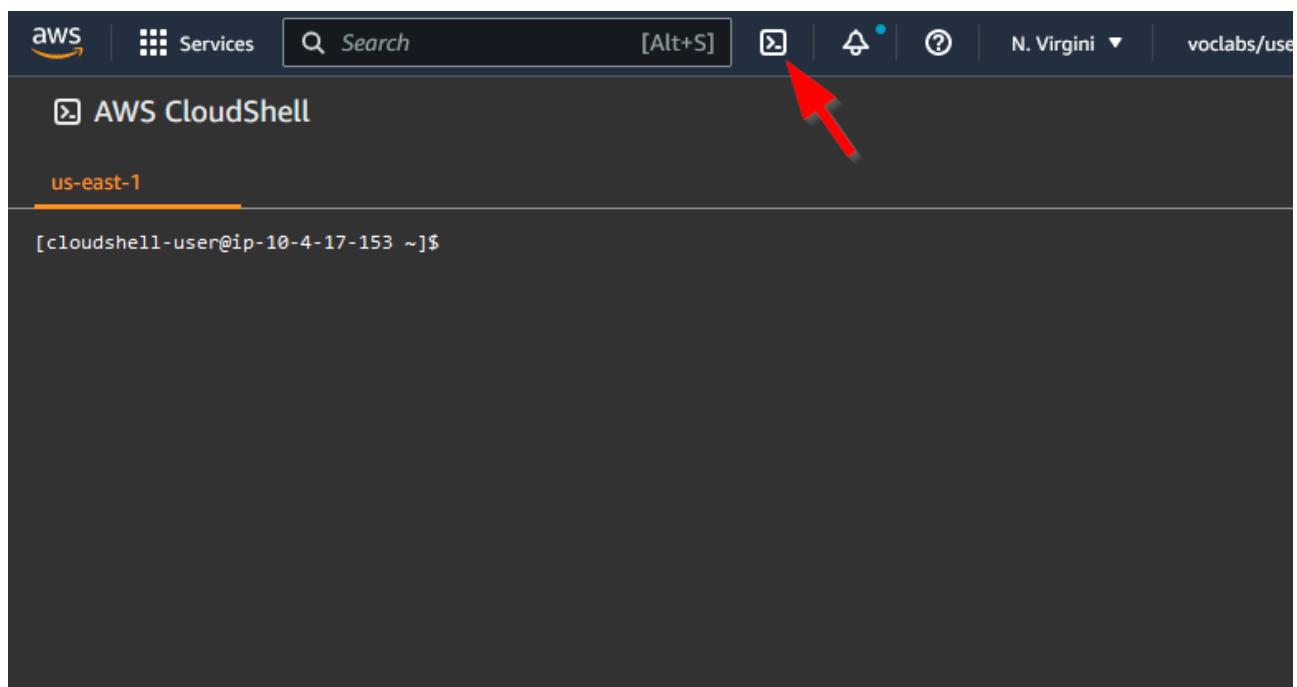
Als we straks een Webserver-instance (lees server) hebben aangemaakt, dienen we steeds in te loggen over ssh met een keypair. We kunnen tijdens creatie van een instance een ssh-key laten aanmaken en deze downloaden. Maar indien we bijvoorbeeld reeds een SSH key hebben die we willen hergebruiken met de AWS-servers, dan moet dit ook kunnen. Om deze handeling te leren, maken we eerst een SSH-keypair aan en brengen deze dan in onze AWS-omgeving. Vanaf dan kunnen we dit keypair telkens koppelen aan iedere nieuwe cloud-instance die we aanmaken.

We gaan dus eerst een keypair aanmaken en deze dan gebruiken voor alle servers die we in de toekomst gaan maken. We gaan dit doen in de AWS Cloud shell. Dit heeft twee voordelen.

Ten eerste bestaat het commando ssh-keygen omdat dit een Linux omgeving is.

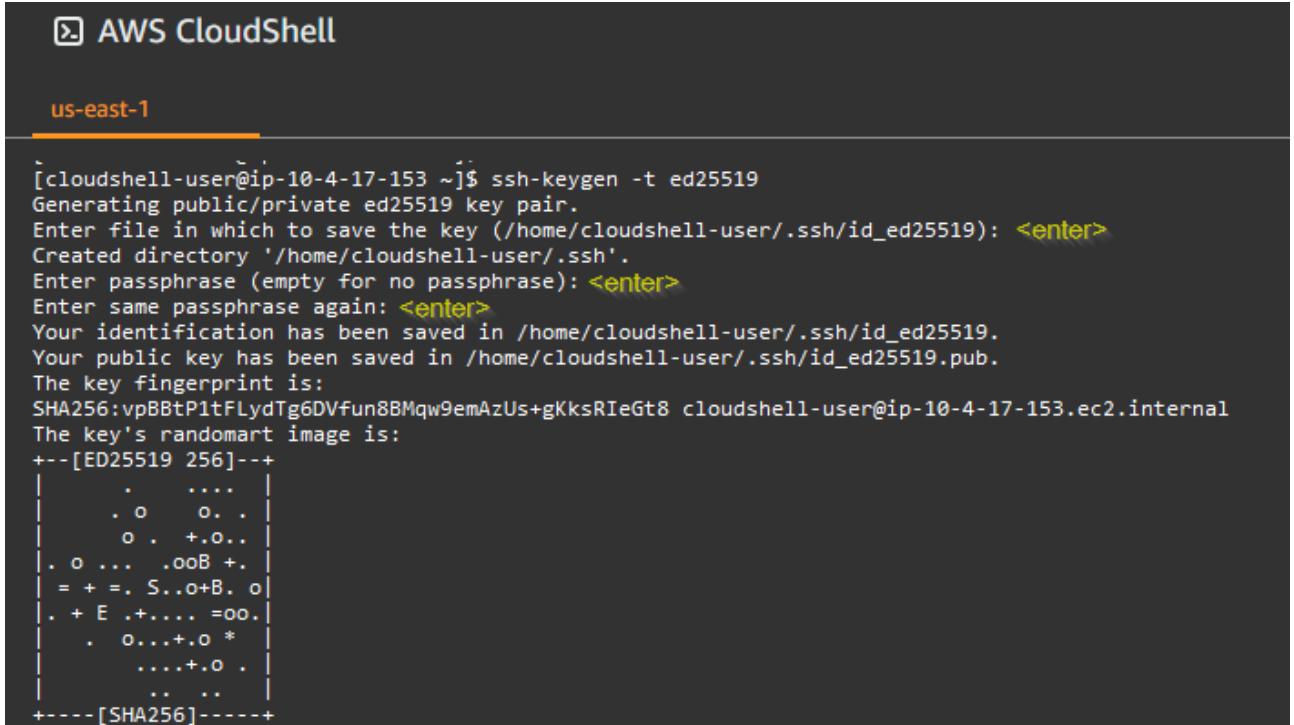
Ten tweede wordt de key in onze Cloud shell aangemaakt en daar dan ook bewaard in de toekomst. We downloaden deze key naar onze laptop, maar dan hebben we ook nog altijd een backup van deze keys in de cloud (bvb. voor als de harde schijf van onze laptop zou crashen)

Open de Cloud Shell



De Cloud Shell is een afgeslankte VM in de cloud, waar je je eigen shell hebt om een aantal zaken te doen met je Cloud-resources.

Maak een ECDSA-keypair aan

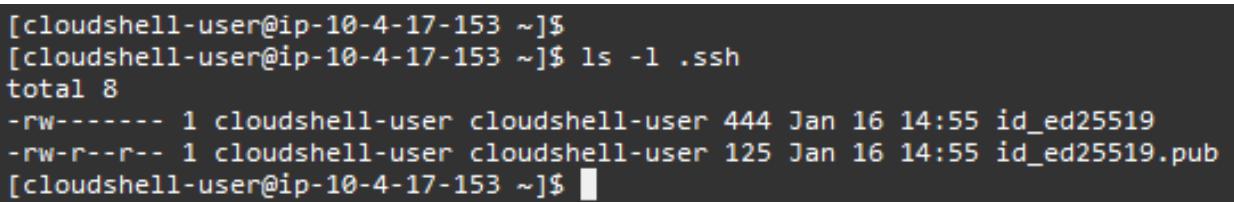


The screenshot shows the AWS CloudShell interface with the region set to 'us-east-1'. A terminal window is open, displaying the command `ssh-keygen -t ed25519` being run. The output shows the generation of a key pair, including prompts for saving the key and entering a passphrase. It also displays the public key fingerprint and the SHA256 hash of the private key.

```
[cloudshell-user@ip-10-4-17-153 ~]$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/cloudshell-user/.ssh/id_ed25519): <enter>
Created directory '/home/cloudshell-user/.ssh'.
Enter passphrase (empty for no passphrase): <enter>
Enter same passphrase again: <enter>
Your identification has been saved in /home/cloudshell-user/.ssh/id_ed25519.
Your public key has been saved in /home/cloudshell-user/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:vpBBtP1tFLydTg6DVfun8BMqw9emAzUs+gKksRIeGt8  cloudshell-user@ip-10-4-17-153.ec2.internal
The key's randomart image is:
++-[ED25519 256]++
|   ...
|   . o   o.. .
|   o . +.o..
| . o ... .ooB +.
| = + =. S..o+B. o
| . + E .+.... =oo.
|   . o...+.o *
|   ....+.o .
|   ...
+---[SHA256]---
```

Er is een private en een public key aangemaakt in de directory .ssh

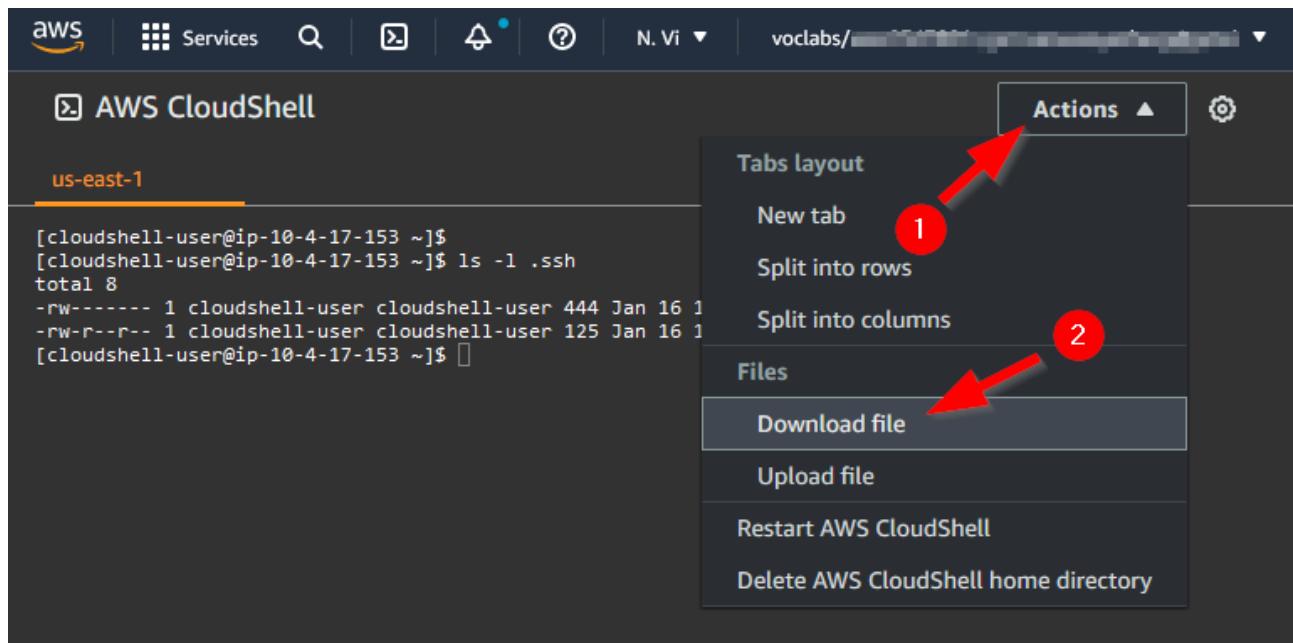
Let ook op de rechten van de keys.



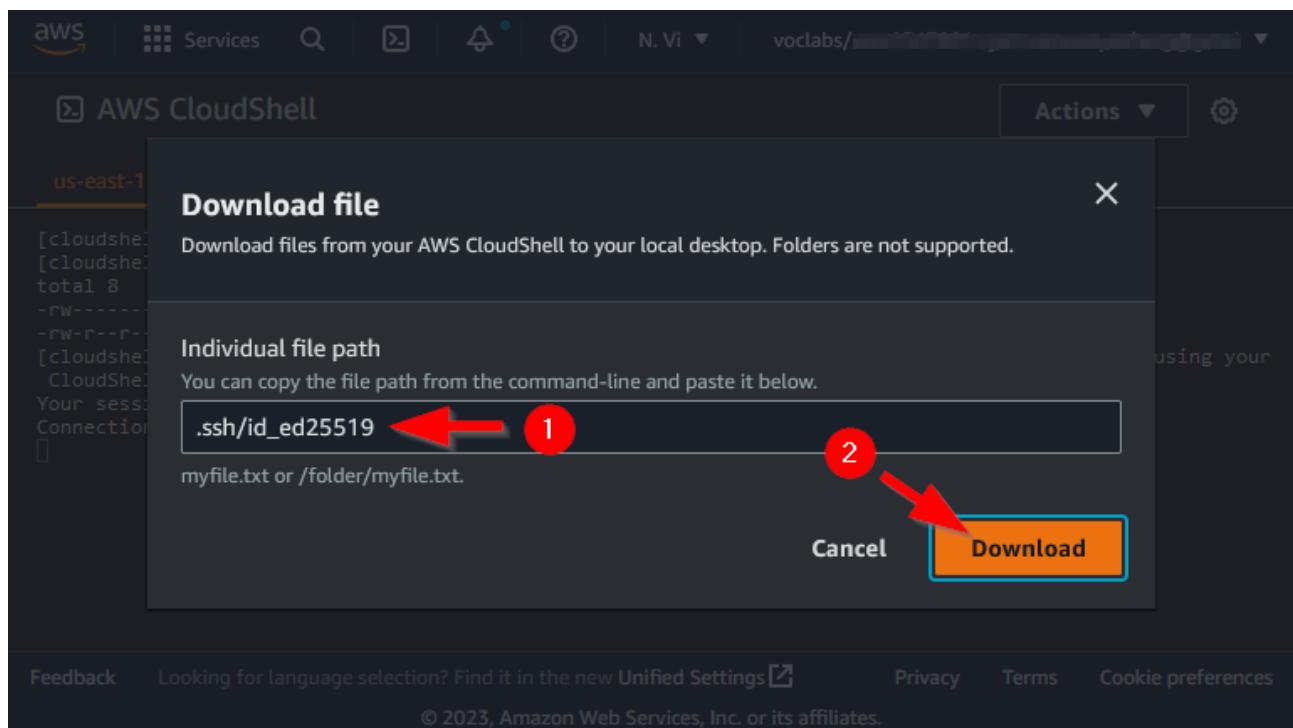
The screenshot shows the AWS CloudShell interface with the command `ls -l .ssh` being run. The output lists two files: `id_ed25519` (private key) and `id_ed25519.pub` (public key). The private key has permissions `rw-----` and the public key has permissions `rwxr--r--`.

```
[cloudshell-user@ip-10-4-17-153 ~]$
[cloudshell-user@ip-10-4-17-153 ~]$ ls -l .ssh
total 8
-rw----- 1 cloudshell-user cloudshell-user 444 Jan 16 14:55 id_ed25519
-rw-r--r-- 1 cloudshell-user cloudshell-user 125 Jan 16 14:55 id_ed25519.pub
[cloudshell-user@ip-10-4-17-153 ~]$ █
```

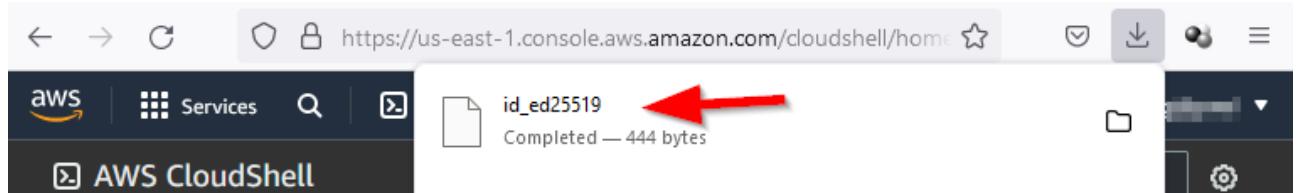
Deze keys zijn dus de enige sleutel die je hebt om in de instance binnen te geraken. Super belangrijk om deze te backen op jouw laptop dus. Dit kunnen we doen door de SSH-keys uit de Cloud Shell te downloaden. We kunnen geen (ssh) connectie maken naar de Cloud Shell, dus moeten we dit doen via de GUI-interface.



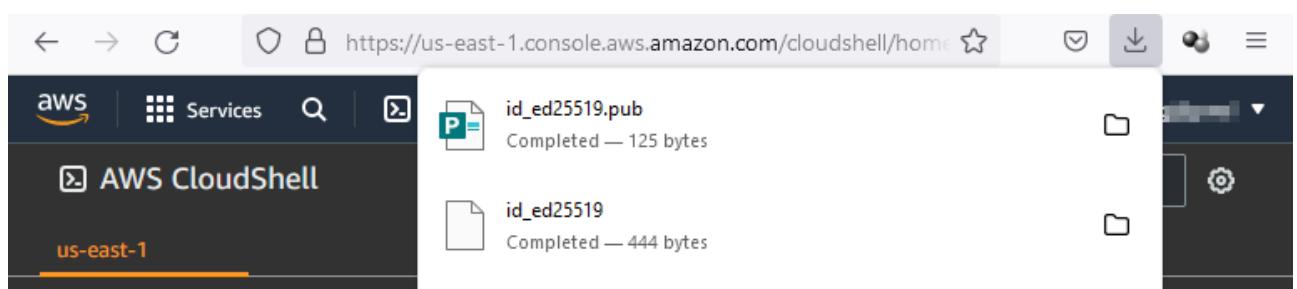
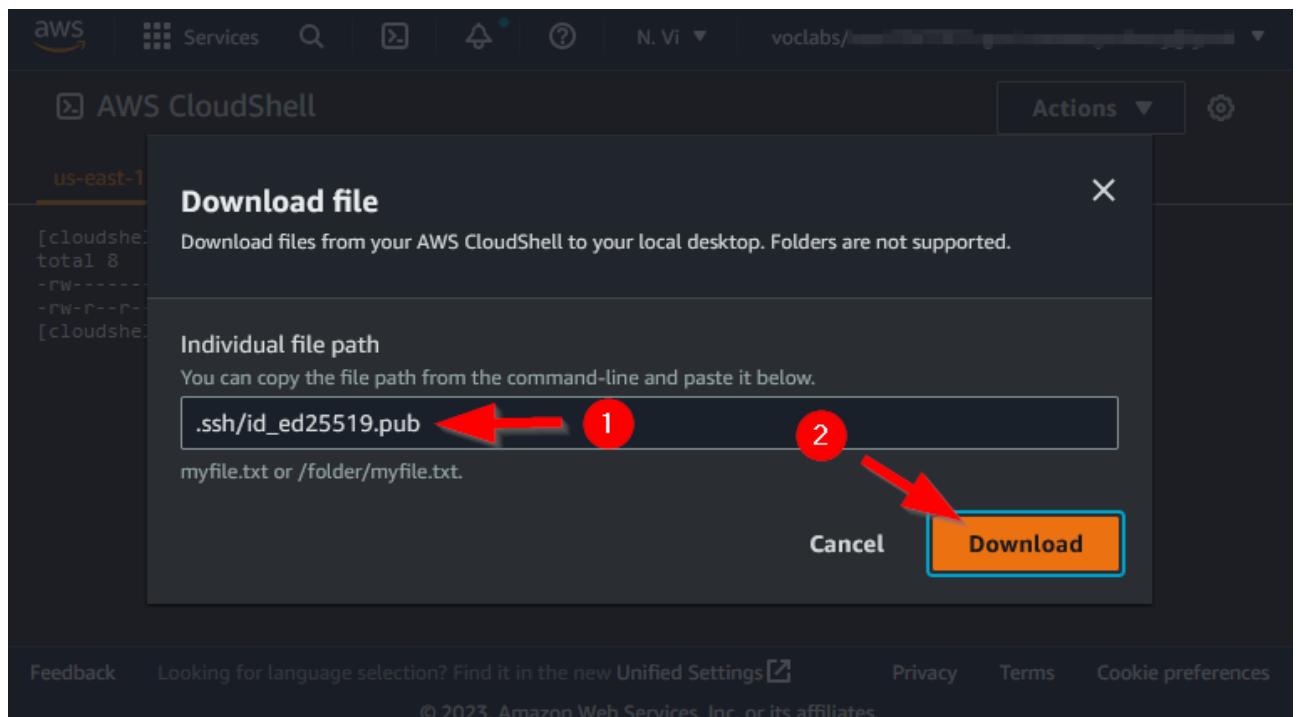
Download eerst de private key



De key wordt gedownload naar je laptop

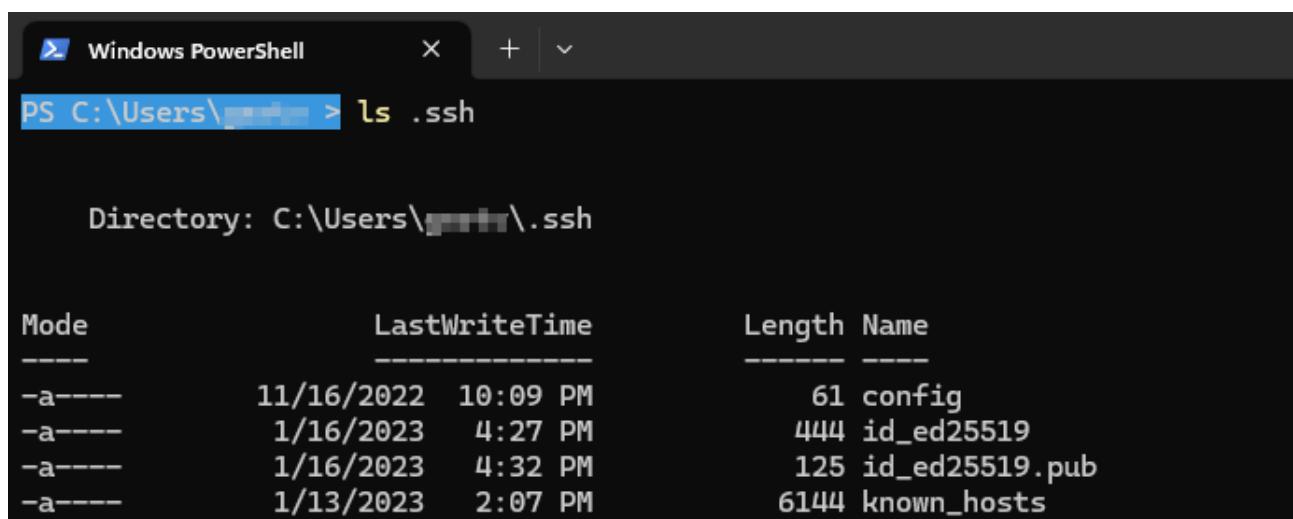


Download vervolgens ook de public key



b. De keys gebruiken in Powershell op je laptop

Indien je in de toekomst een ssh connectie wilt maken vanuit Powershell of de Windows Terminal, dan kan je de keys die je zonet hebt gedownload kopiëren naar een .ssh folder op je laptop.



```
Windows PowerShell
PS C:\Users\[REDACTED] > ls .ssh

Directory: C:\Users\[REDACTED]\.ssh

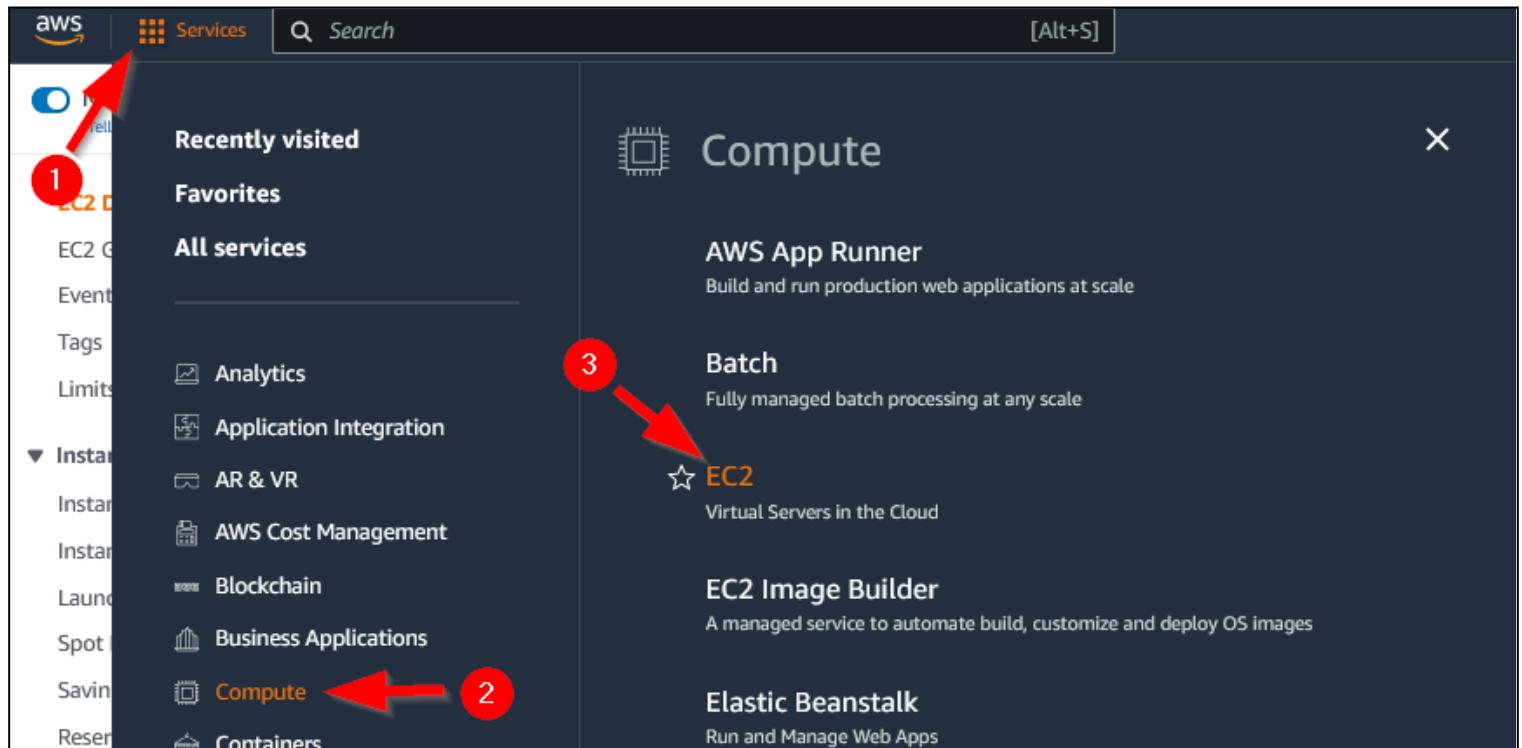
Mode                LastWriteTime     Length Name
----                -----          ---- 
-a---       11/16/2022 10:09 PM        61 config
-a---       1/16/2023  4:27 PM       444 id_ed25519
-a---       1/16/2023  4:32 PM      125 id_ed25519.pub
-a---       1/13/2023  2:07 PM     6144 known_hosts
```

Je kan dan later een ssh connectie starten naar je Cloud-Instance via Powershell of de Windows Terminal.

c. De keys in de AWS-omgeving brengen

We dienen deze keys nu in onze AWS-omgeving te brengen, zodanig dat deze gekoppeld kunnen worden aan nieuwe Cloud-instances om er zo via SSH mee te kunnen connecteren.

Klik op het hamburgermenu en selecteer *Compute* en vervolgens *EC2*



Klik- in het linkermenu op *Key Pairs*. Klik vervolgens op *Actions* en dan op *Import key pair*

The screenshot shows the AWS Cloud Services console with the 'Instances' service selected in the sidebar. In the main content area, the 'Key pairs' section is displayed, showing one entry: 'vokey' (rsa, 2023/01/12 16:07 GM). A red arrow labeled '1' points to the 'Key Pairs' link in the sidebar. A red arrow labeled '2' points to the 'Actions' button in the top right corner of the table header. A red arrow labeled '3' points to the 'Import key pair' option in the dropdown menu that appears when the 'Actions' button is clicked.

Name	Type	Created
vokey	rsa	2023/01/12 16:07 GM

Geef het keypair een fatsoenlijke naam en klik op *Browse*

EC2 > Key pairs > Import key pair

Import key pair

Import settings

Name ←

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair file ←

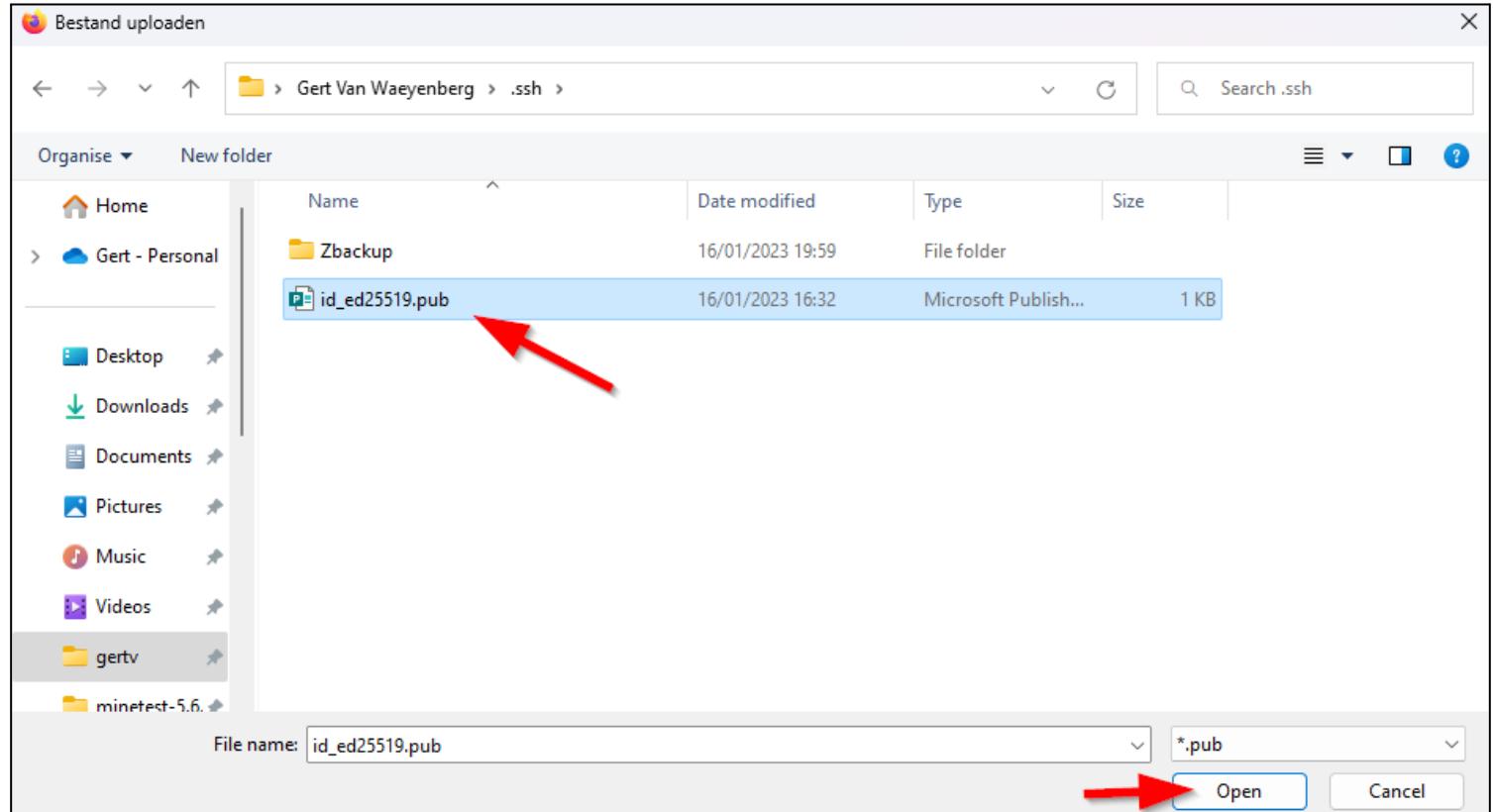
Choose Browse and navigate to your public key. You may change the name of your key. Alternatively, paste the contents of your public key into the **Public key contents** text box.

Tags - *optional*

No tags associated with the resource.

You can add up to 50 more tags.

Selecteer de public key en klik op *Open*



Klik op *Import keypair*

Import key pair

Import settings

Name

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair file

Choose Browse and navigate to your public key. You may change the name of your key. Alternatively, paste the contents of your public key into the Public key contents text box.

id_ed25519.pub

0.125kb

ssh-ed25519

```
AAAAC3NzaC1lZDI1NTE5AAAIK8x0n46iAxb15qLHMS7M+Iugb8MFKeVQ38fKI4dcqs
w cloudshell-user@ip-10-4-17-153.ec2.internal
```

Tags - optional

No tags associated with the resource.

You can add up to 50 more tags.

Cancel

Import key pair

De key is geïmporteerd

✓ Successfully imported key pair

Key pairs (2) [Info](#)



[Actions ▾](#)

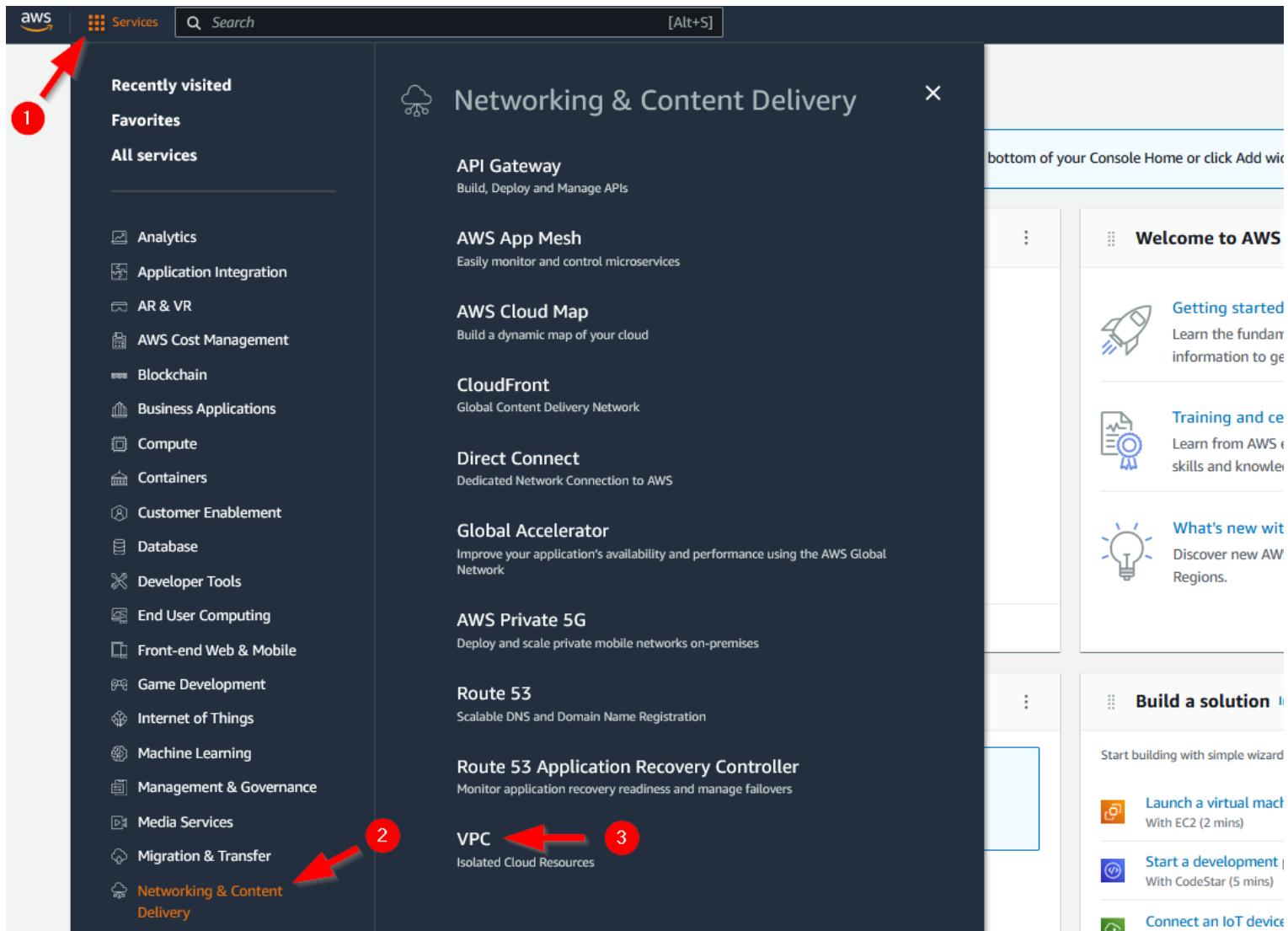
[Search](#)

<input type="checkbox"/>	Name	Type	Created	<input type="checkbox"/>	Fingerprint
<input type="checkbox"/>	vockey	rsa	2023/01/12 16:07 GMT+1		99:ba:f1:b4:71:0b:
<input type="checkbox"/>	gert-keys	ed25519	2023/01/18 18:05 GMT+1		vpBBtP1tFLydTg6

d. Een nieuw Virtual Private Cloud aanmaken

By default is er reeds een Virtual Private Cloud (VPC) voorhanden. Tijdens het aanmaken van een Cloud-instance kan er dan gebruik gemaakt worden van deze default VPC. Maar het is altijd fijner om te weten hoe alles werkt en daarom maken we er liever zelf eentje op voorhand.

Dit doe je door op het Hamburger-menu te klikken en te kiezen voor "Networking & Content Delivery" en vervolgens "VPC".



We gaan in **5 stappen** te werk gaan:

- VPC aanmaken met een bepaald intern netwerk (cidr block)
- Een subnet aanmaken in onze VPC
- Internet Gateway aanmaken en koppelen aan de VPC
- Default Route via Internet Gateway toevoegen aan default route tabel van VPC
- Default route tabel van VPC koppelen aan subnet

Stap 1: VPC aanmaken met een bepaald intern netwerk (cidr block)

Klik op Create VPC

We maken een VPC netwerk aan met een ip-block van 10.0.0.0/24

Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

Name tag - optional
Creates a tag with a key of 'Name' and a value that you specify.
gert-vpc

IPv4 CIDR block Info
 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

IPv4 CIDR
10.0.0.0/24

IPv6 CIDR block Info
 No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block IPv6 CIDR owned by me

Tenancy Info
Default ▾

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	Remove
<input type="text"/> Name	<input type="text"/> gert-vpc	<input type="button"/> Remove

De VPC is aangemaakt.

Klik op "Your VPCs"

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with various options like Subnets, Route tables, Internet gateways, etc. Under 'Virtual private cloud', 'Your VPCs' is selected. The main area shows a success message: 'You successfully created vpc-045958566c3c024c0 / gert-vpc'. Below this, the 'Details' tab is active, showing information for the VPC 'vpc-045958566c3c024c0 / gert-vpc'. The VPC ID is 'vpc-045958566c3c024c0', State is 'Available', and the IPv4 CIDR is '10.0.0.0/24'. The 'CIDRs' tab is also visible. At the bottom, there's a table for CIDRs with one entry: 'IPv4' with CIDR '10.0.0.0/24' and status 'Associated'.

In dit overzicht zie je de nieuwe en default VPC.

Klik de nieuwe VPC om opnieuw de configuratie te bekijken.

The screenshot shows the 'Your VPCs' list page. It displays two VPC entries: 'gert-vpc' (VPC ID: 'vpc-045958566c3c024c0') and another entry with a long, partially obscured VPC ID. Both VPCs are listed as 'Available'. A red arrow points to the VPC ID column for the first entry ('gert-vpc').

Stap 2: Een subnet aanmaken in onze VPC

We kunnen ons netwerk (10.0.0.0/24) in ons VPC subnetten. We subnetten het naar 8 netwerken van 32 IPs.

We maken voorlopig enkel het eerste subnet aan.

Selecteer in het linkerdeelvenster *Subnets* en klik op *Create subnet*

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with 'Virtual private cloud' expanded, showing 'Your VPCs' and 'Subnets' (which is highlighted with a red arrow and circled with '1'). At the top right, there's a large table titled 'Subnets (6)'. In the top right corner of this table, there's a red arrow pointing to a blue 'Create subnet' button. Another red arrow with '2' inside a circle points to the same button.

Name	Subnet ID	State	VPC	IPv4 CIDR
-	subnet-0b88a156a4b7c0543	Available	vpc-0a730d44f188f6ac7	172.31.0.0/20
-	subnet-08418f617a90aff8a	Available	vpc-0a730d44f188f6ac7	172.31.16.0/20
-	subnet-08c23229589814585	Available	vpc-0a730d44f188f6ac7	172.31.64.0/20
-	subnet-0c77f2840e2c631dc	Available	vpc-0a730d44f188f6ac7	172.31.48.0/20
-	subnet-0197e72cd638eeeca6	Available	vpc-0a730d44f188f6ac7	172.31.80.0/20
-	subnet-0f7c4bc238d056ad2	Available	vpc-0a730d44f188f6ac7	172.31.32.0/20

Vul de gegevens in en klik op *Create subnet*. We plaatsen dit subnet in Availability Zone *us-east-1a*.

Screenshot of the AWS VPC Create Subnet wizard.

VPC

VPC ID
Create subnets in this VPC.
vpc-045958566c3c024c0 (gert-vpc) 

Associated VPC CIDRs

IPv4 CIDRs
10.0.0.0/24

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
gert-subnet1 

The name can be up to 256 characters long.

Availability Zone 
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1a 

IPv4 CIDR block 
Q 10.0.0.0/27 

Tags - optional

Key	Value - optional	Remove
Q Name	Q gert-subnet1	X Remove

Add new tag 

You can add 49 more tags.

Remove 

Add new subnet 

Create subnet 

Het subnet is aangemaakt.

The screenshot shows the AWS Subnets list page. At the top, a green banner displays the message: "You have successfully created 1 subnet: subnet-0889e393110f14c20". Below the banner, the title "Subnets (1) Info" is followed by a search bar labeled "Filter subnets" and a button "Clear filters". On the right side of the header are buttons for "Actions" and "Create subnet". The main content area contains a table with one row of data. The columns are: Name, Subnet ID, State, VPC, IPv4 CIDR, and IPv6 CIDR. The single row shows: "gert-subnet1", "subnet-0889e393110f14c20", "Available", "vpc-045958566c3c024c0 | ger...", "10.0.0.0/27", and "-".

	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input type="checkbox"/>	gert-subnet1	subnet-0889e393110f14c20	Available	vpc-045958566c3c024c0 ger...	10.0.0.0/27	-

Stap 3: Internet gateway aanmaken en koppelen aan VPC

Nu maken we een gateway naar het Internet toe. Klik op *Create Internet gateway* om een nieuwe aan te maken.

VPC dashboard X
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways ①

Internet gateways (1/1) Info

Name	Internet gateway ID	State	VPC ID
-	igw-0d3de573db8e28f9d	Attached	vpc-0a730d44f188f6ac7

Create internet gateway ②

Geef de internet gateway een *Name tag* en klik op *Create Internet gateway*.

VPC > Internet gateways > Create internet gateway

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

igw-Gert ①

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
Name	igw-Gert

Add new tag ②

You can add 49 more tags.

Cancel Create internet gateway

De Internet gateway is aangemaakt.

The following internet gateway was created: igw-0a5dbdfadf9118f33 - igw-Gert. You can now attach to a VPC to enable the VPC to communicate with the internet.

Attach to a VPC X

VPC > Internet gateways > igw-0a5dbdfadf9118f33

igw-0a5dbdfadf9118f33 / igw-Gert

Actions ▾

Details Info

Internet gateway ID igw-0a5dbdfadf9118f33	State Detached	VPC ID -	Owner 986210483412
--	-------------------	-------------	-----------------------

Tags

Manage tags

Search tags

Key Value

Name	igw-Gert
------	----------

We dienen nu de nieuwe gateway te koppelen aan de nieuwe VPC.

VPC > Internet gateways > igw-0a5dbdfadf9118f33

igw-0a5dbdfadf9118f33 / igw-Gert

Actions ▾

1

2

- 1 Attach to VPC
- 2 Detach from VPC
- Manage tags
- Delete

Details Info

Internet gateway ID igw-0a5dbdfadf9118f33	State Detached	VPC ID -	Owner 986210483412
--	-------------------	-------------	-----------------------

Tags

Manage tags

Search tags

Key Value

Name	igw-Gert
------	----------

Klik in het zoekvak en je ziet de VPC. Selecteer de VPC.

VPC > Internet gateways > Attach to VPC (igw-0a5dbdfadf9118f33)

Attach to VPC (igw-0a5dbdfadf9118f33) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

 1
 2

▶ AWS Command Line Interface command

Cancel

Attach internet gateway

Klik nu op *Attach internet gateway*

VPC > Internet gateways > Attach to VPC (igw-0a5dbdfadf9118f33)

Attach to VPC (igw-0a5dbdfadf9118f33) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

 1

▶ AWS Command Line Interface command

Cancel

Attach internet gateway

We zien nu dat de status veranderd is naar *Attached* en erachter staat de *VPC ID*

The screenshot shows the AWS CloudFormation console with a success message at the top: "Internet gateway igw-0a5dbdfadf9118f33 successfully attached to vpc-045958566c3c024c0". Below this, the navigation path is "VPC > Internet gateways > igw-0a5dbdfadf9118f33". The main title is "igw-0a5dbdfadf9118f33 / igw-Gert". On the right, there is an "Actions" dropdown menu. The "Details" tab is selected, showing the following information:

Internet gateway ID igw-0a5dbdfadf9118f33	State Attached	VPC ID vpc-045958566c3c024c0 gert-vpc	Owner 986210483412
--	-------------------	--	-----------------------

Below the details, the "Tags" section is shown, featuring a search bar and a "Manage tags" button. A single tag is listed:

Key	Value
Name	igw-Gert

Stap 4: Default Route via Internet Gateway toevoegen aan default route tabel van VPC

Ga opnieuw naar het overzicht van de VPCs.

Klik de nieuwe VPC om opnieuw de configuratie te bekijken

Your VPCs (1/2) Info						
		Name		VPC ID	State	
				IPv4 CIDR	IPv6 CIDR	DHCP opt
<input checked="" type="checkbox"/>	gert-vpc	vpc-045958566c3c024c0	Available	10.0.0.0/24	-	dopt-04ec
<input type="checkbox"/>	-	vpc-0a730d44f188ff6ac7	Available	172.31.0.0/16	-	dopt-04ec

We passen nu de route-tabel aan van de VPC zodat we de Default gateway kunnen specifiëren.

Klik op het ID van de *Main route table* om de configuratie te zien van de route table die gebruikt wordt door de nieuwe VPC

VPC > Your VPCs > vpc-045958566c3c024c0 / gert-vpc			
Details Info			
VPC ID <input type="checkbox"/> vpc-045958566c3c024c0	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-04ede6ef7b0c28970	Main route table rtb-000f67c4c39fa3105	Main network ACL acl-076917e721c743b6d
Default VPC No	IPv4 CIDR 10.0.0.0/24	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID <input type="checkbox"/> 986210483412	
CIDRs Flow logs Tags			
CIDRs Info			
Address type	▲ CIDR	Network Border Group	Pool
IPv4	10.0.0.0/24	-	-
			Associated

Klik nogmaals op het *Route table ID* om de configuratie te zien

Route tables (1/1) Info							Actions
<input type="text"/> Filter route tables							
<input checked="" type="checkbox"/>	Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC	
<input checked="" type="checkbox"/>	-	rtb-000f67c4c39fa3105	-	-	Yes	vpc-045958566c3c024c0 gert-vpc	

Klik op *Edit routes*. We zien dat het lokale netwerk (10.0.0.0/24) wijst naar het *target local*. Klik op *Edit routes* om de configuratie aan te passen.

VPC > Route tables > rtb-000f67c4c39fa3105								Actions															
rtb-000f67c4c39fa3105																							
<p>ⓘ You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer X</p>																							
<p>Details Info</p>																							
<table><tr><td>Route table ID <input type="text"/> rtb-000f67c4c39fa3105</td><td>Main <input checked="" type="checkbox"/> Yes</td><td>Explicit subnet associations -</td><td>Edge associations -</td></tr><tr><td>VPC <input type="text"/> vpc-045958566c3c024c0 gert-vpc</td><td>Owner ID <input type="text"/> 986210483412</td><td></td><td></td></tr></table>									Route table ID <input type="text"/> rtb-000f67c4c39fa3105	Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations -	Edge associations -	VPC <input type="text"/> vpc-045958566c3c024c0 gert-vpc	Owner ID <input type="text"/> 986210483412									
Route table ID <input type="text"/> rtb-000f67c4c39fa3105	Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations -	Edge associations -																				
VPC <input type="text"/> vpc-045958566c3c024c0 gert-vpc	Owner ID <input type="text"/> 986210483412																						
<p>Routes Subnet associations Edge associations Route propagation Tags</p>																							
<p>Routes (1) Edit routes</p>																							
<table><tr><th colspan="2">Filter routes</th><th>Both</th><th>< 1 ></th><th>⚙️</th></tr><tr><th>Destination</th><th>Target</th><th>Status</th><th>Propagated</th><th></th></tr><tr><td>10.0.0.0/24</td><td>local</td><td> ⓘ Active</td><td>No</td><td></td></tr></table>									Filter routes		Both	< 1 >	⚙️	Destination	Target	Status	Propagated		10.0.0.0/24	local	 ⓘ Active	No	
Filter routes		Both	< 1 >	⚙️																			
Destination	Target	Status	Propagated																				
10.0.0.0/24	local	 ⓘ Active	No																				

Klik op *Add route* om een route toe te voegen.

VPC > Route tables > rtb-000f67c4c39fa3105 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/24	<input type="text"/> local X	 ⓘ Active	No

[Add route](#) Cancel Preview Save changes

Kies voor de route 0.0.0.0/0 (=default route) de target *Internet Gateway*

VPC > Route tables > rtb-000f67c4c39fa3105 > Edit routes

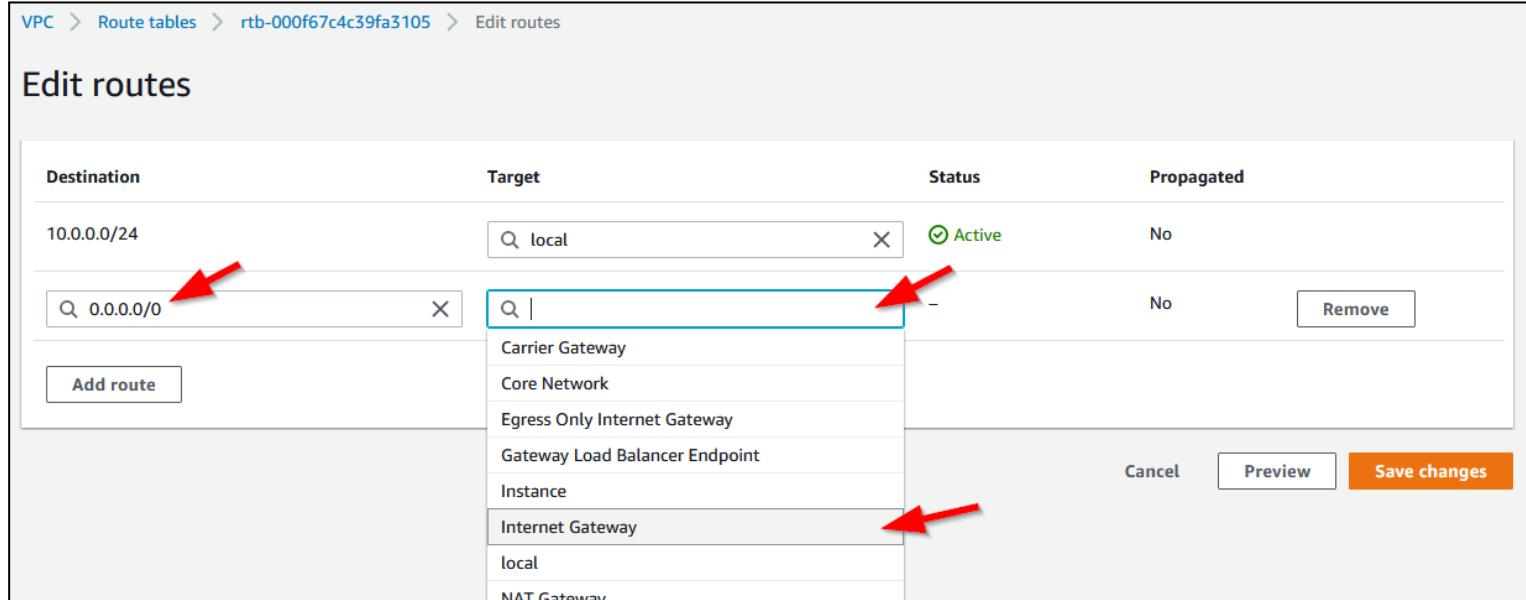
Edit routes

Destination	Target	Status	Propagated
10.0.0.0/24	local	Active	No
Q 0.0.0.0/0	Q	-	No

Add route

Carrier Gateway
Core Network
Egress Only Internet Gateway
Gateway Load Balancer Endpoint
Instance
Internet Gateway
local
NAT Gateway

Cancel Preview Save changes



Selecteer vervolgens de Internet GateWay die wordt weergegeven. Dit is de gateway die we daarnet hebben aangemaakt en gekoppeld aan onze VPC

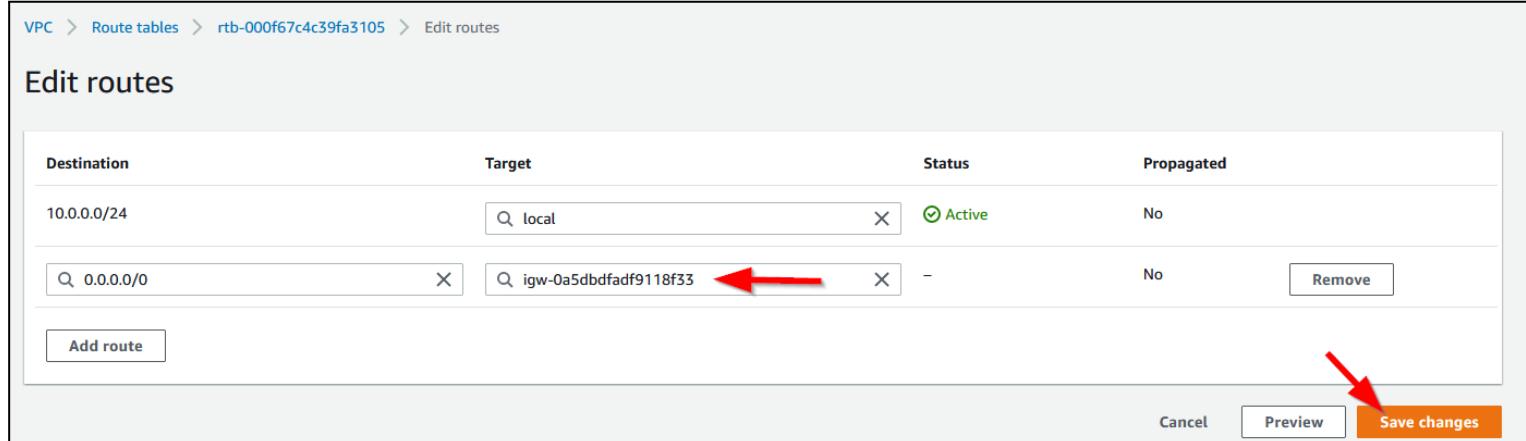
VPC > Route tables > rtb-000f67c4c39fa3105 > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/24	local	Active	No
Q 0.0.0.0/0	Q igw-0a5dbdfadf9118f33	-	No

Add route

Cancel Preview Save changes



We zien nu dat de Default Route is toegevoegd en Active is. Indien we nu een Cloud Instance een IP-adres geven van dit VPC netwerk (10.0.0.0/24) dan kan deze ook naar het Internet.

The screenshot shows the AWS VPC Route Tables page. At the top, a green header bar indicates "Updated routes for rtb-000f67c4c39fa3105 successfully". Below this, the breadcrumb navigation shows "VPC > Route tables > rtb-000f67c4c39fa3105". The main title is "rtb-000f67c4c39fa3105". On the right, there is an "Actions" dropdown menu. A message box at the top says "You can now check network connectivity with Reachability Analyzer" with buttons for "Run Reachability Analyzer" and "X".

Details Info

Route table ID rtb-000f67c4c39fa3105	Main Yes	Explicit subnet associations -	Edge associations -
VPC vpc-045958566c3c024c0 gert-vpc	Owner ID 986210483412		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0	igw-0a5dbdfadf9118f33	Active	No
10.0.0.0/24	local	Active	No

Buttons: Edit routes < 1 > Filter routes

Stap 5: Default route tabel van VPC koppelen aan subnet

Ga opnieuw naar het overzicht van de VPCs.

Klik de nieuwe VPC om opnieuw de configuratie te bekijken

Your VPCs (1/2) Info						
	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP opt
<input checked="" type="checkbox"/>	gert-vpc	vpc-045958566c3c024c0	Available	10.0.0.0/24	-	dopt-04ed
<input type="checkbox"/>	-	vpc-0a730d44f188f6ac7	Available	172.31.0.0/16	-	dopt-04ed

We passen nu de route-tabel aan van de VPC zodat we deze kunnen koppelen aan ons nieuw subnet.

Klik op het ID van de *Main route table* om de configuratie te zien van de route table die gebruikt wordt door de nieuwe VPC

vpc-045958566c3c024c0 / gert-vpc			
Details Info		CIDRs Info	
VPC ID	State	CIDR	Address type
vpc-045958566c3c024c0	Available	10.0.0.0/24	IPv4
Tenancy	DHCP option set	Route 53 Resolver DNS Firewall rule groups	IPv6
Default	dopt-04ede6ef7b0c28970	Failed to load rule groups	IPv6 CIDR (Network border group)
Default VPC	IPv4 CIDR	Main route table	-
No	10.0.0.0/24	rtb-000f67c4c39fa3105	-
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	IPv6 pool	Owner ID
Disabled	Failed to load rule groups	-	986210483412
CIDRs Info		Tags	
Address type	CIDR	Network Border Group	Pool
IPv4	10.0.0.0/24	-	-
			Associated

Klik op het tabblad *Subnet association* en vervolgens op *Edit subnet associations*

The screenshot shows the AWS Route Tables page. A red arrow labeled '1' points to the 'Subnet associations' tab, which is highlighted in orange. Another red arrow labeled '2' points to the 'Edit subnet associations' button in the top right corner of the main content area.

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Ow...
-	rtb-000f67c4c39fa3105	-	-	Yes	vpc-045958566c3c024c0 ger...	98621...

rtb-000f67c4c39fa3105

Details Routes **Subnet associations** Edge associations Route propagation Tags

Explicit subnet associations (0)

No subnet associations
You do not have any subnet associations.

Vink het subnet aan en klik op *Save Associations*

The screenshot shows the 'Edit subnet associations' dialog. A red arrow labeled '1' points to the checkbox next to 'gert-subnet1' in the 'Available subnets' list. Another red arrow labeled '2' points to the 'Save associations' button in the bottom right corner.

VPC > Route tables > rtb-000f67c4c39fa3105 > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/1)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/> gert-subnet1	subnet-0889e393110f14c20	10.0.0.0/27	-	Main (rtb-000f67c4c39fa3105)

Selected subnets

subnet-0889e393110f14c20 / gert-subnet1 X

Cancel **Save associations**

De koppeling is gelukt

✓ You have successfully updated subnet associations for rtb-000f67c4c39fa3105.

Route tables (1/1) Info

Actions Create route table

Filter route tables

Route table ID: rtb-000f67c4c39fa3105 Clear filters

<input checked="" type="checkbox"/>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Ow...
<input checked="" type="checkbox"/>	-	rtb-000f67c4c39fa3105	subnet-0889e393110f1...	-	Yes	vpc-045958566c3c024c0 ger...	98621...

rtb-000f67c4c39fa3105

Details | Routes | **Subnet associations** | Edge associations | Route propagation | Tags

Explicit subnet associations (1)

Edit subnet associations

Find subnet association

Subnet ID	IPv4 CIDR
subnet-0889e393110f14c20 / gert-subnet1	10.0.0.0/27

e. Cloud Instances in dit nieuwe subnet van een publiek IP voorzien en publieke DNS naam

We hebben een Default Route toegevoegd in onze VPC en gekoppeld aan ons subnet, maar nu moeten Cloud Instances die een IP krijgen in dit subnet ook een bijkomend Publiek IP adres krijgen, zodanig dat pakketjes ook het Internet op kunnen.

We kunnen dit doen door middel van een *NAT Gateway* of door de optie in een subnet genaamd *Enable auto-assign public IPv4 address* (*hetwelk automatisch een Public IP toekent aan een Cloud Instance*)

Maar een *NAT Gateway* is zeer kostelijk bij AWS dus kiezen we voor de tweede optie.

Selecteer in het linkermenu *Subnets* en vink het nieuwe subnet aan. Klik vervolgens op *Actions* en dan op *Edit subnet settings*

The screenshot shows the AWS VPC dashboard with the 'Subnets' section selected. A red arrow labeled '1' points to the 'Subnets' link in the left sidebar. Another red arrow labeled '2' points to the checkbox next to the subnet 'gert-subnet1' in the list. On the right, a context menu is open over the selected subnet, with a red arrow labeled '3' pointing to the 'Actions' button. A red circle labeled '4' highlights the 'Edit subnet settings' option in the menu, which is also highlighted with a blue border. The table lists seven subnets, each with a checkbox, name, subnet ID, state, VPC, and CIDR range.

Name	Subnet ID	State	VPC	CIDR Range
-	subnet-08418f617a90aff8a	Available	vpc-0a730d44f188f6ac7	172.31.16.0/20
-	subnet-0b88a156a4b7c0543	Available	vpc-0a730d44f188f6ac7	172.31.0.0/20
-	subnet-08c23229589814585	Available	vpc-0a730d44f188f6ac7	172.31.64.0/20
-	subnet-0c77f2840e2c631dc	Available	vpc-0a730d44f188f6ac7	172.31.48.0/20
-	subnet-0197e72cd638eeeca6	Available	vpc-0a730d44f188f6ac7	172.31.80.0/20
-	subnet-0f7c4bc238d056ad2	Available	vpc-0a730d44f188f6ac7	172.31.32.0/20
<input checked="" type="checkbox"/> gert-subnet1	subnet-0889e393110f14c20	Available	vpc-045958566c3c024c0 ger...	10.0.0.0/27

Vink *Enable auto-assign public IPv4 address* aan en klik op *Save*

VPC > Subnets > subnet-0889e393110f14c20 > Edit subnet settings

Edit subnet settings Info

Subnet

Subnet ID	Name
<input type="checkbox"/> subnet-0889e393110f14c20	<input type="checkbox"/> gert-subnet1

Auto-assign IP settings Info
Enable the auto-assign IP settings to automatically request a public IPv4 or IPv6 address for a new network interface in this subnet.

Enable auto-assign public IPv4 address Info 

Enable auto-assign customer-owned IPv4 address Info
Option disabled because no customer owned pools found.

Resource-based name (RBN) settings Info
Specify the hostname type for EC2 instances in this subnet and optional RBN DNS query settings.

Enable resource name DNS A record on launch Info

Enable resource name DNS AAAA record on launch Info

Hostname type Info

Resource name
 IP name

DNS64 settings
Enable DNS64 to allow IPv6-only services in Amazon VPC to communicate with IPv4-only services and networks.

Enable DNS64 Info 

Cancel **Save** 

Het subnet is aangepast.

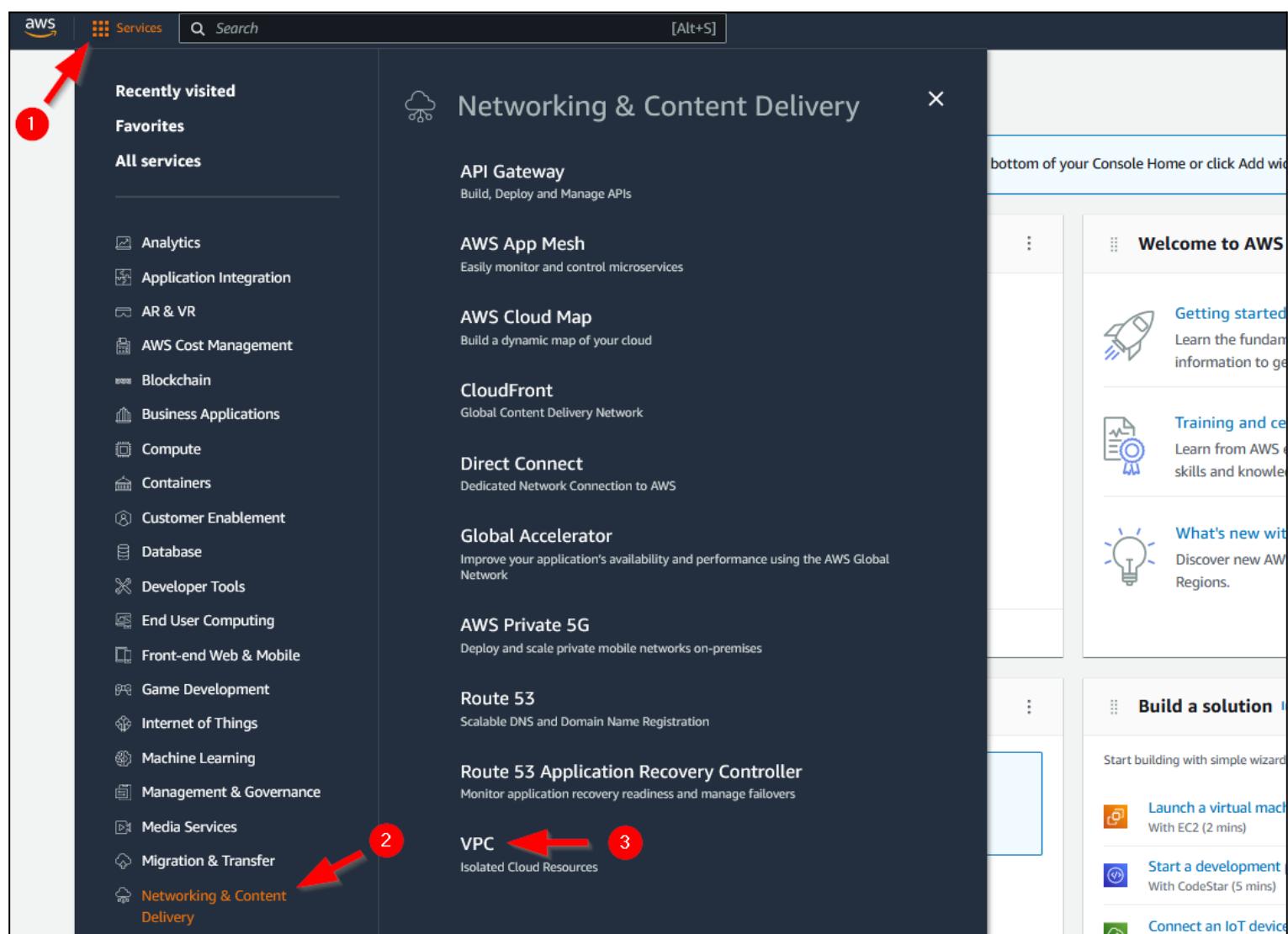
f. Cloud Instances in dit nieuwe subnet (eigenlijk VPC) voorzien van een publieke DNS naam

De Instances die in een subnet zitten van onze VPC krijgen nu een publiek IP adres, maar het zou fijn zijn als we ook via een DNS naam naar deze Instances zouden kunnen gaan.

We kunnen er voor zorgen dat AWS zelf een DNS naam maakt die gekoppeld is met het IP adres (dat hij ook zelf aanmaakt) dat de Instance krijgt telkens dat deze opnieuw opstart.

Hiervoor editeren we onze VPC.

Dit doe je door op het Hamburger-menu te klikken en te kiezen voor "Networking & Content Delivery" en vervolgens "VPC".



Klik in het linkermenu op *Your VPCs*. Vink jouw VPC aan. Klik op *Actions* en vervolgens op *Edit VPC settings*

The screenshot shows the AWS VPC service interface. In the left sidebar, under 'Virtual private cloud', the 'Your VPCs' link is highlighted with a red arrow and labeled '1'. The main table lists two VPCs: 'gert-vpc' (selected, indicated by a checked checkbox) and another entry. A red circle labeled '2' is on the checkbox for 'gert-vpc'. At the top right, there's a 'Actions' button with a dropdown menu. A red arrow labeled '3' points to the 'Actions' button, and a red circle labeled '4' highlights the 'Edit VPC settings' option in the dropdown.

Name	VPC ID	State	IPv4 CIDR
<input checked="" type="checkbox"/> gert-vpc	vpc-045958566c3c024c0	Available	10.0.0.0/24
	vpc-0a730d44f188f6ac7	Available	172.31.0.0/1

Vink *Enable DNS hostnames* aan en klik op Save

VPC > Your VPCs > vpc-045958566c3c024c0 > Edit VPC settings

Edit VPC settings Info

Introducing the new edit VPC settings experience
We've added a new option to make it easier to edit VPC settings. You can now manage all VPC settings in one place. [Tell us what you think.](#)

VPC details

VPC ID	Name
<input type="checkbox"/> vpc-045958566c3c024c0	<input type="checkbox"/> gert-vpc

DHCP settings

DHCP option set Info

DNS settings

Enable DNS resolution Info

Enable DNS hostnames Info

1

Network Address Usage metrics settings

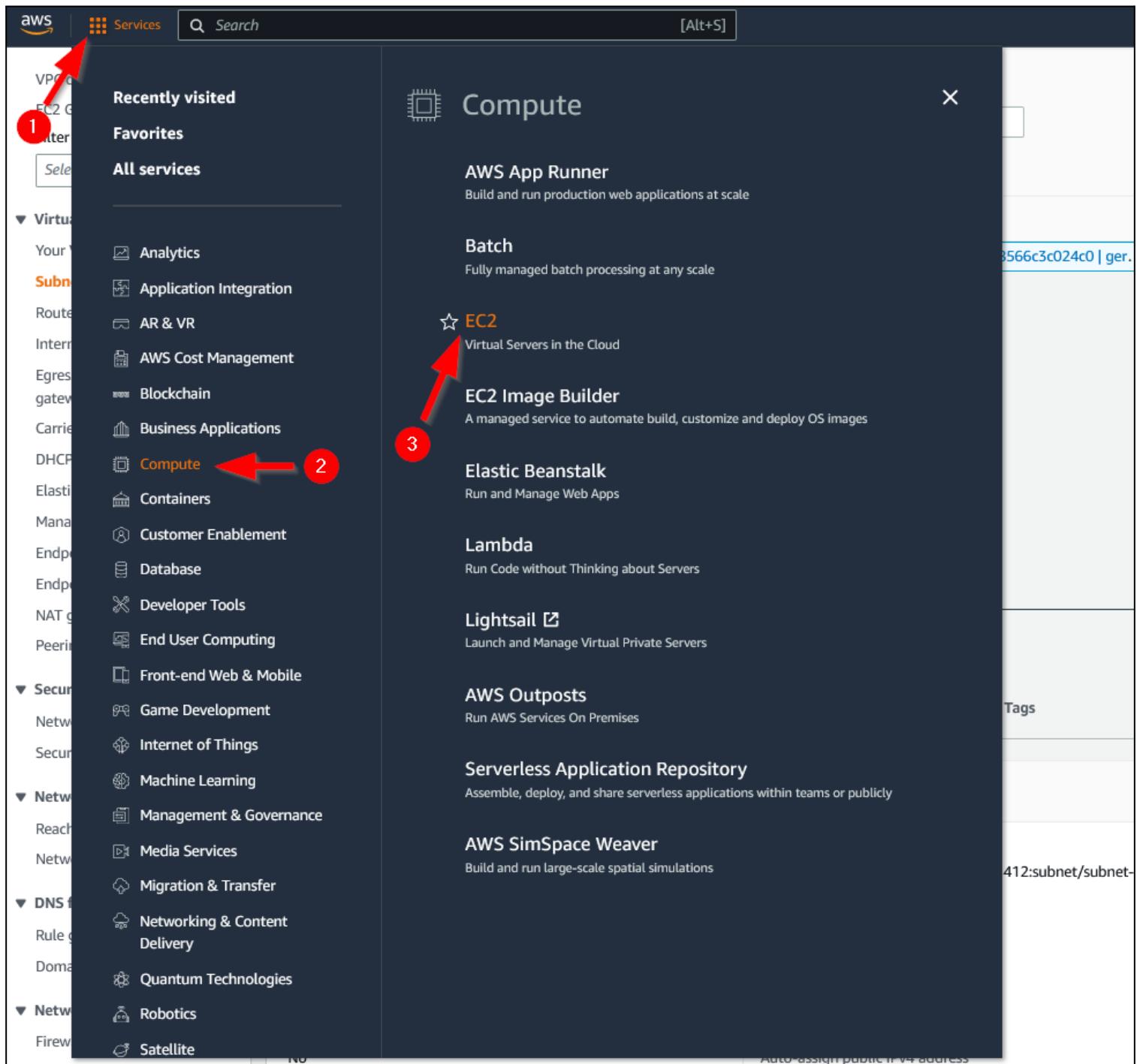
Enable Network Address Usage metrics Info

2

g. Een Ubuntu 22.04 -Compute-instance aanmaken

We maken een Ubuntu 22.04 Server -Cloud Instance aan. Deze gaan we dan gebruiken als webserver.

Klik op het Hamburger-menu en kies voor "Compute" en vervolgens "EC2".



Klik op "Launch Instance"

The screenshot shows the AWS EC2 Dashboard. On the left, there's a sidebar with various navigation links like EC2 Dashboard, Instances, Images, and Elastic Block Store. The main area has a section titled 'Resources' with a summary of current resources. Below that is a callout box with a tip about launching Microsoft SQL Server Always On availability groups. The central part of the dashboard features a 'Launch instance' section with a large orange 'Launch instance' button, which is highlighted with a red arrow pointing to it. To the right of this section is a 'Service health' panel showing the status of the service.

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Dedicated Hosts	0	Elastic IPs	0
Instances	0	Key pairs	2	Load balancers	0
Placement groups	0	Security groups	3	Snapshots	0
Volumes	0				

Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▾ **Migrate a server** ↗

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

C AWS Health Dashboard ↗

Region
US East (N. Virginia)

Status
This service is operating normally

Geef als naam <vn>-webserver en selecteer Ubuntu

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 gert-webserver 1 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 our full catalog including 1000s of application and OS images

Quick Start

Ubuntu 2 Ubuntu

Amazon Linux aws

macOS Mac

Windows Microsoft

Red Hat Red Hat

>

🔍 **Browse more AMIs**
Including AMIs from AWS, Marketplace and the Community

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type Free tier eligible

ami-06878d265978313ca (64-bit (x86)) / ami-0ffe6a92e2553e8a8 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

Description
Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2022-12-06

Architecture 64-bit (x86) **AMI ID** ami-06878d265978313ca Verified provider

Selecteer als Instance type *t2.nano*

Selecteer het keypair dat je zelf hebt aangemaakt en geupload naar het AWS-platform

Klik op *Edit*

The screenshot shows the AWS Instance Configuration page with three steps highlighted:

- Step 1:** A red arrow points to the "Instance type" dropdown menu, which is set to "t2.nano". A red circle with the number "1" is positioned above the dropdown.
- Step 2:** A red arrow points to the "Key pair name - required" input field, which contains "gert-keys". A red circle with the number "2" is positioned above the input field.
- Step 3:** A red arrow points to the "Edit" button located next to the "Network settings" section. A red circle with the number "3" is positioned above the "Edit" button.

Instance type [Info](#)

Instance type
t2.nano

Family: t2 1 vCPU 0.5 GiB Memory

On-Demand Linux pricing: 0.0058 USD per Hour

On-Demand Windows pricing: 0.0081 USD per Hour

[Compare instance types](#)

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*

gert-keys

[Create new key pair](#)

Network settings [Info](#)

Network [Info](#)
vpc-0a730d44f188f6ac7

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

Auto-assign public IP [Info](#)
Enable

[Edit](#)

Zorg dat de Instance gekoppeld is aan jouw VPC en jouw Subnet

Zorg er voor dat de Instance automatisch een Public IP adres krijgt

Maak een nieuwe *Security group* aan met een fatsoenlijke naam en beschrijving

Zorg er voor dat via deze Security group *SSH* wordt toegelaten van *eender waar*

Klik op *Launch Instance* om de server aan te maken en te starten

The screenshot shows the 'Network settings' section of the AWS Launch Instance wizard. It includes fields for selecting a VPC (vpc-045958566c3c024c0), Subnet (gert-subnet1), enabling Auto-assign public IP, creating a new security group (gert-webserver-sg), and defining an inbound rule for port 22 (TCP) from anywhere. To the right, the 'Summary' section shows one instance being launched with the Canonical AMI (Ubuntu 22.04 LTS). A callout box provides information about the Free tier. Step 7 is highlighted with a red arrow pointing to the 'Launch instance' button.

Network settings

- VPC - required Info vpc-045958566c3c024c0 (gert-vpc)
10.0.0.0/24
- Subnet Info subnet-0889e393110f14c20
VPC: vpc-045958566c3c024c0 Owner: 986210483412 Availability Zone: us-east-1a IP addresses available: 27 CIDR: 10.0.0.0/27
- Create new subnet

Auto-assign public IP Info Enable
2

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
3

Security group name - required gert-webserver-sg
4

Description - required Info Gert Webserver Security Group created 2023-01-18T17:44:18.162Z
5

Inbound security groups rules

Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type Info	Protocol Info	Port range Info
ssh	TCP	22
Source type Info	Source Info	Description - optional Info
Anywhere	Add CIDR, prefix list or security 0.0.0.0/0	e.g. SSH for admin desktop

Remove

Summary

- Number of instances Info 1
- Software Image (AMI) Canonical, Ubuntu, 22.04 LTS, ...read more ami-06878d265978313ca
- Virtual server type (instance type) t2.nano
- Firewall (security group) New security group
- Storage (volumes) 1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance
7

De Instance is succesvol aangemaakt.

Klik op *View all instances*

EC2 > Instances > Launch an instance

 Success
Successfully initiated launch of instance ([i-089d3f6d1c68e13db](#))

▶ Launch log

Next Steps

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
[Create billing alerts](#)

Connect to your instance
Once your instance is running, log into it from your local computer.
[Connect to instance](#) 
[Learn more](#) 

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
[Connect an RDS database](#) 
[Create a new RDS database](#) 
[Learn more](#) 

 [View all instances](#) 

De Webserver-instance is *Running*

We zien ook een Public IP adres en DNS-naam. Via dit IP-adres en/of DNS-naam kunnen we bvb connectie maken over SSH

Instances (1) Info					
<input type="text"/> Find instance by attribute or tag (case-sensitive)					
<input type="checkbox"/>	Name	Instance ID	Instance state	Insta...	Status check
<input type="checkbox"/>	gert-webserver	i-013209f1d8f529fe9	Running	t2.nano	2/2 checks pa



<input type="checkbox"/>	Connect	Instance state	Actions	Launch instances	▼
<input type="checkbox"/>	Alarm... No ... +	Availability us-east-1a	Public IPv4 DNS ec2-3-235-28-0.compute-1.amazonaws.com	Public IPv4 ... 3.235.28.0	▼



h. Cloud instance een vast Publiek IP adres geven

Van zodra je de Cloud-instance wordt gestopt en opnieuw herstart krijgt deze telkens een ander IP adres.

The diagram illustrates the process of assigning a static public IP address to a Cloud instance. It consists of four panels arranged in a 2x2 grid, connected by a downward arrow indicating the sequence of events:

- Top Left Panel:** Shows the AWS CloudWatch Logs interface with three log entries:
 - Successfully started i-013209f1d8f529fe9
 - Successfully stopped i-013209f1d8f529fe9
 - Successfully rebooted i-013209f1d8f529fe9
- Top Right Panel:** Shows the AWS CloudWatch Metrics interface for the instance i-013209f1d8f529fe9. The Public IPv4 DNS metric shows the value `ec2-3-235-28-0.compute-1.amazonaws.com`, and the Public IPv4 Address metric shows the value `3.235.28.0`.
- Bottom Left Panel:** Shows the AWS CloudWatch Logs interface again, identical to the top-left panel, displaying the same log entries.
- Bottom Right Panel:** Shows the AWS CloudWatch Metrics interface for the same instance. The Public IPv4 DNS metric now shows the value `ec2-44-203-247-73.compute-1.amazonaws.com`, and the Public IPv4 Address metric shows the value `44.203.247.73`.

Om dit op te lossen moeten we een Elastic IP aanmaken en koppelen aan deze Instance.

Klik in het linkermenu op *Elastic IPs* en vervolgens op *Allocate Elastic IP address*

The screenshot shows the AWS EC2 console interface. On the left, there is a navigation menu with the following items:

- New EC2 Experience (with a 'Tell us what you think' link)
- EC2 Dashboard
- EC2 Global View
- Events
- Tags
- Limits
- Instances** (expanded): Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations
- Images** (expanded): AMIs, AMI Catalog
- Elastic Block Store** (expanded): Volumes, Snapshots, Lifecycle Manager
- Network & Security** (expanded): Security Groups, **Elastic IPs** (highlighted with a red arrow and circled with a red number 1)

The main content area is titled "Elastic IP addresses". It features a search bar labeled "Filter Elastic IP addresses" and a table header with columns: Name, Allocated IPv4 add..., Type, and Allocation ID. At the top right of the table, there is a "Actions" dropdown and a prominent orange button labeled "Allocate Elastic IP address". A red arrow points from the number 2 to this orange button.

We maken een nieuw Elastic IP aan door op *Allocate* te klikken

The screenshot shows the 'Allocate Elastic IP address' configuration page. At the top, the breadcrumb navigation shows 'EC2 > Elastic IP addresses > Allocate Elastic IP address'. The main section is titled 'Elastic IP address settings' with a 'Network Border Group' dropdown set to 'us-east-1'. Below this, under 'Public IPv4 address pool', the 'Amazon's pool of IPv4 addresses' option is selected. There are three other options listed: 'Public IPv4 address that you bring to your AWS account' (disabled), and 'Customer owned pool of IPv4 addresses' (disabled). A 'Create accelerator' button is available. In the 'Tags - optional' section, it says 'No tags associated with the resource.' and has an 'Add new tag' button. A note states 'You can add up to 50 more tag'. At the bottom right, there are 'Cancel' and 'Allocate' buttons, with a red arrow pointing to the 'Allocate' button.

Selecteer, indien nodig, het Elastic IP address en klik op Actions en vervolgens op *Associate Elastic IP address*

Elastic IP addresses (1/1)

Filter Elastic IP addresses

Public IPv4 address: 3.231.186.123

Clear filters

Allocated IPv4 add... Type

Name - 3.231.186.123 Public IP eipalloc-0d5e0712d7dd54d51

Actions ▾ Allocate Elastic IP address

View details

Release Elastic IP addresses

Associate Elastic IP address

Disassociate Elastic IP address

Revert

Selecteer de *Instance* waar dit Elastic IP adres aan gekoppeld moet worden en klik op *Associate*

EC2 > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (3.231.186.123)

Elastic IP address: 3.231.186.123

Resource type
Choose the type of resource with which to associate the Elastic IP address.

Instance 1

Network interface

⚠️ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Instance 2

Choose an instance 3

i-013209f1d8f529fe9 (gert-webserver) - running

The private IP address with which to associate the Elastic IP address.

Choose a private IP address

Reassociation
Specify whether the Elastic IP address can be reassigned with a different resource if it is already associated with a resource.

Allow this Elastic IP address to be reassigned

4

Cancel Associate

Het Elastic IP adres is succesvol gekoppeld aan onze Webserver-instance

Elastic IP address associated successfully.
Elastic IP address 3.231.186.123 has been associated with instance i-013209f1d8f5.

Elastic IP addresses (1/1)

Filter Elastic IP addresses

Public IPv4 address: 3.231.186.123 X Clear filters

Name	Allocated IPv4 add...	Type
-	3.231.186.123	Public IP

Associated instance ID: i-013209f1d8f529fe9
Private IP address: 10.0.0.6

We zien dat dit gelukt is als we opnieuw naar de Instance gaan kijken. Wanneer we nu de instance gaan stoppen en nadien opnieuw starten, dan zal het IP adres en bijhorende DNS naam hetzelfde blijven.

Klik in het linkermenu op Instances en vervolgens op *Refresh*. We zien nu dat het Elastic IP adres en bijhorende DNS-naam in gekoppeld zijn

New EC2 Experience Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instances (1) Info

Find instance by attribut

Name: gert-webserver

Health check: 2 checks passed

Alarm... No ... +

Instance state Actions Launch instances

Public IPv4 DNS: ec2-3-231-186-123.compute-1.amazonaws.com

Public IP address: 3.231.186.123

i. Over SSH verbinden met de server

SSH vanuit Powershell

Om op de Webserver te werken gaan we best een SSH sessie starten vanop onze laptop. Om de gegevens hiervoor op te vragen doen we het volgende.

Klik *Instances*. Selecteer vervolgens de Webserver-instance en klik op *Connect*

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'Instances' section, there is a red arrow pointing to the 'Instances' link with a red circle labeled '1'. In the main content area, a red arrow points to the 'gert-webserver' instance row with a red circle labeled '2'. A third red arrow points to the 'Connect' button at the top right of the table with a red circle labeled '3'.

AWS stelt een SSH-commando voor met een bepaalde key, maar let op, onze key op de laptop noemt anders

The screenshot shows the 'Connect to instance' dialog for the instance 'i-013209f1d8f529fe9'. At the top, there are four tabs: 'EC2 Instance Connect', 'Session Manager', 'SSH client' (which is selected and highlighted with a red circle labeled '1'), and 'EC2 serial console'. Below the tabs, the 'Instance ID' is listed as 'i-013209f1d8f529fe9 (gert-webserver)'. A numbered list provides instructions for connecting via SSH:

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is `gert-keys.pem`.
3. Run this command, if necessary, to ensure your key is not publicly viewable.
 `chmod 400 gert-keys.pem`
4. Connect to your instance using its Public DNS:
 `ec2-3-231-186-123.compute-1.amazonaws.com`

An 'Example' section shows the command to run:
`ssh -i "gert-keys.pem" ubuntu@ec2-3-231-186-123.compute-1.amazonaws.com`

In a note box, it says: **Note:** In most cases, the guessed user name is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

At the bottom right, there is a red circle labeled '3' with a red arrow pointing to the 'Cancel' button.

We starten een Powershell of Windows Terminal en plakken het commando, maar passen de naam van onze key aan.

```
PS C:\Users\gerty\.ssh > ssh -i "id_ed25519" ubuntu@ec2-3-231-186-123.compute-1.amazonaws.com
The authenticity of host 'ec2-3-231-186-123.compute-1.amazonaws.com (3.231.186.123)' can't be established.
ED25519 key fingerprint is SHA256:FwAxbdwQob/qlXnt8Rn0P210ddfjfDM6SXAmKMLwfE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-231-186-123.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1026-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Wed Jan 18 21:14:56 UTC 2023

System load: 0.0078125      Processes:          98
Usage of /:   25.3% of 7.57GB  Users logged in:     0
Memory usage: 43%           IPv4 address for eth0: 10.0.0.6
Swap usage:   0%

46 updates can be applied immediately.
25 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Wed Jan 18 18:07:19 2023 from 18.206.107.29
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-0-6:~$ |
```

Of we laten de -i optie volledig weg, want de key heeft de default naam en zal dan ook gewoon gevonden worden.

```
PS C:\Users\gerty\.ssh > ssh ubuntu@ec2-3-231-186-123.compute-1.amazonaws.com
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1026-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Wed Jan 18 21:40:16 UTC 2023

System load: 0.0      Processes:          99
Usage of /:   25.3% of 7.57GB  Users logged in:     1
Memory usage: 44%       IPv4 address for eth0: 10.0.0.6
Swap usage:   0%

46 updates can be applied immediately.
25 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Wed Jan 18 21:27:49 2023 from 34.239.172.14
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-0-6:~$ |
```

SSH vanuit de AWS webinterface

Een andere optie is om even een connectie te maken via een Web-interface

The screenshot shows the 'Connect to instance' page for an EC2 instance. A red arrow labeled '1' points to the 'EC2 Instance Connect' tab. Another red arrow labeled '2' points to the 'Connect' button at the bottom right.

EC2 > Instances > i-013209f1d8f529fe9 > Connect to instance

Connect to instance Info 1

Connect to your instance i-013209f1d8f529fe9 (gert-webserver) using any of these options

EC2 Instance Connect 2 Session Manager SSH client EC2 serial console

Instance ID

Public IP address

User name Enter the user name defined in the AMI used to launch the instance. If you didn't define a custom user name, use the default user name, ubuntu.

Note: In most cases, the default user name, ubuntu, is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI user name.

Cancel Connect

The screenshot shows a terminal window titled "AWS CloudShell" with a dark theme. At the top, there's a navigation bar with the AWS logo, a "Services" button, a search bar containing "Search", and several icons for "Alt+S", "X", a bell, and a question mark.

```
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1026-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 System information as of Wed Jan 18 21:25:24 UTC 2023

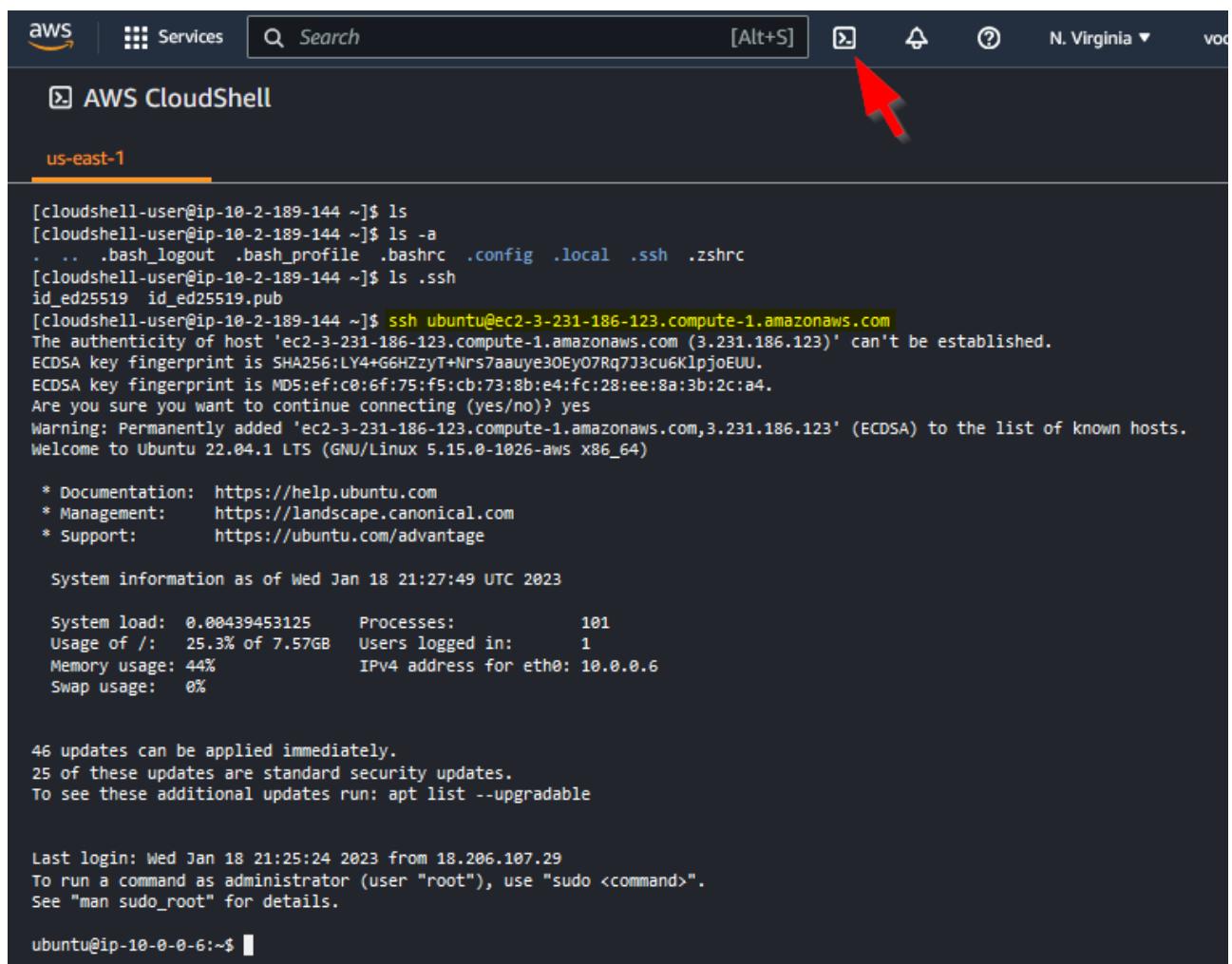
 System load: 0.080078125      Processes: 98
 Usage of /: 25.3% of 7.57GB   Users logged in: 1
 Memory usage: 44%           IPv4 address for eth0: 10.0.0.6
 Swap usage: 0%

46 updates can be applied immediately.
25 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Wed Jan 18 21:14:57 2023 from 84.195.122.178
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-0-6:~$
```

SSH vanuit de AWS CloudShell



```
[cloudshell-user@ip-10-2-189-144 ~]$ ls
[cloudshell-user@ip-10-2-189-144 ~]$ ls -a
. .. .bash_logout .bash_profile .bashrc .config .local .ssh .zshrc
[cloudshell-user@ip-10-2-189-144 ~]$ ls .ssh
id_ed25519 id_ed25519.pub
[cloudshell-user@ip-10-2-189-144 ~]$ ssh ubuntu@ec2-3-231-186-123.compute-1.amazonaws.com
The authenticity of host 'ec2-3-231-186-123.compute-1.amazonaws.com (3.231.186.123)' can't be established.
ECDSA key fingerprint is SHA256:LY4+G6HZzyT+Nrs7aauye30Ey07Rq7J3cu6KlpjoEUU.
ECDSA key fingerprint is MD5:ef:c0:6f:75:f5:cb:73:8b:e4:fc:28:ee:8a:3b:2c:a4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-3-231-186-123.compute-1.amazonaws.com,3.231.186.123' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1026-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Jan 18 21:27:49 UTC 2023

System load:  0.00439453125   Processes:           101
Usage of /:   25.3% of 7.57GB  Users logged in:     1
Memory usage: 44%              IPv4 address for eth0: 10.0.0.6
Swap usage:   0%

46 updates can be applied immediately.
25 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Wed Jan 18 21:25:24 2023 from 18.206.107.29
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-10-0-0-6:~$
```

j. Waarom werkt de SSH out-of-the-box?

Het is wel eens leuk om na te gaan waarom onze SSH connectie naar de Webserver juist kan/mag. Dan komen de instellingen die we tot nu toe gedaan hebben samen tot een werkend geheel.

SSH is geïnstalleerd in de Instance

```
ubuntu@ip-10-0-0-6:~$ apt list --installed | grep ssh
WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

libssh-4/jammy,now 0.9.6-2build1 amd64 [installed,automatic]
openssh-client/jammy,now 1:8.9p1-3 amd64 [installed,upgradable to: 1:8.9p1-3ubuntu0.1]
openssh-server/jammy,now 1:8.9p1-3 amd64 [installed,upgradable to: 1:8.9p1-3ubuntu0.1]
openssh-sftp-server/jammy,now 1:8.9p1-3 amd64 [installed,upgradable to: 1:8.9p1-3ubuntu0.1]
ssh-import-id/jammy,now 5.11-0ubuntu1 all [installed]
```

De SSH-service draait

```
ubuntu@ip-10-0-0-6:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Drop-In: /usr/lib/systemd/system/ssh.service.d
            └─ec2-instance-connect.conf
    Active: active (running) since Wed 2023-01-18 19:56:34 UTC; 1h 48min ago
      Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 630 (sshd)
     Tasks: 1 (limit: 539)
    Memory: 18.0M
```

Er wordt op de juiste poort geluisterd

```
ubuntu@ip-10-0-0-6:~$ ss -lt
State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
LISTEN      0           4096       127.0.0.53%lo:domain      0.0.0.0:*
LISTEN      0           128        0.0.0.0:ssh              0.0.0.0:*
LISTEN      0           128        [::]:ssh                [::]:*
ubuntu@ip-10-0-0-6:~$ ss -ltn
State      Recv-Q      Send-Q      Local Address:Port          Peer Address:Port
LISTEN      0           4096       127.0.0.53%lo:53          0.0.0.0:*
LISTEN      0           128        0.0.0.0:22              0.0.0.0:*
LISTEN      0           128        [::]:22                [::]:*
```

De Uncomplicated Firewall draait niet

```
ubuntu@ip-10-0-0-6:~$ sudo ufw status  
Status: inactive
```

De Uncomplicated Firewall is een gemakkelijke en overzichtelijke firewall voor eindgebruikers. Omdat deze uitgeschakeld is, is er misschien een veel ingewikkeldere firewall aanwezig, namelijk iptables.

De IPTables-Firewall heeft geen aparte regels, maar wel de Policy ACCEPT voor binnenkomend, uitgaand en doorgaand verkeer. Dus alle verkeer, en dus ook het inkomend SSH verkeer, is toegelaten.

```
ubuntu@ip-10-0-0-6:~$ sudo iptables -L  
Chain INPUT (policy ACCEPT)  
target     prot opt source          destination  
  
Chain FORWARD (policy ACCEPT)  
target     prot opt source          destination  
  
Chain OUTPUT (policy ACCEPT)  
target     prot opt source          destination
```

We hebben de Webserver instance ook voorzien van een Publiek IP-adres en DNS-naam

Instances (1) Info		Instance state	Actions	Launch instances	▼
<input type="checkbox"/>	Find instance by attrib				◀ 1 ▶ ⚙️
<input type="checkbox"/>	Name	Public IPv4 DNS		ec2-3-231-186-123.compute-1.amazonaws.com	3.231.186.123

Er zijn ook Route tabellen voor de Instance

Route tables (1/1) [Info](#)

Filter route tables

Route table ID: rtb-000f67c4c39fa3105 X Clear filters

<input checked="" type="checkbox"/>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input checked="" type="checkbox"/>	-	rtb-000f67c4c39fa3105	subnet-0889e393110f1...	-	Yes	vpc-04595856

rtb-000f67c4c39fa3105

Details [Routes](#) Subnet associations Edge associations Route propagation Tags

Routes (2)

Filter routes Both

Destination	Target	Status
0.0.0.0/0	igw-0a5dbdfad9118f33	<input checked="" type="checkbox"/> Active
10.0.0.0/24	local	<input checked="" type="checkbox"/> Active

We hebben ook een SSH-key geïmporteerd in de AWS-omgeving en gekoppeld aan de Webserver-instance

Successfully imported key pair

Key pairs (2) [Info](#)

C Actions ▾

Search

<input type="checkbox"/>	Name	Type	Created	Fingerprint
<input type="checkbox"/>	vockey	rsa	2023/01/12 16:07 GMT+1	99:ba:f1:b4:71:0b:
<input type="checkbox"/>	gert-keys	ed25519	2023/01/18 18:05 GMT+1	vpBBtP1tFLydTq6

Instances (1/1) Info						
<input type="text"/> Find instance by attribute or tag (case-sensitive)						
	Name	Instance ID	Instance state	Insta...	Status check	Alarm...
<input checked="" type="checkbox"/>	gert-webserver	i-013209f1d8f529fe9	Running	t2.nano	2/2 checks passed	No ... + us-east-

Instance: i-013209f1d8f529fe9 (gert-webserver)						
▼ Instance details Info						
Platform		AMI ID				
<input type="checkbox"/> Ubuntu (Inferred)		<input type="checkbox"/> ami-06878d265978313ca				
Platform details		AMI name				
<input type="checkbox"/> Linux/UNIX		<input type="checkbox"/> ubuntu/images/hvm-ssd/ubuntu-jammy-22.04-amd64-server-20221206				
Stop protection		Launch time				
Disabled		<input type="checkbox"/> Wed Jan 18 2023 20:56:05 GMT+0100 (Central European Standard Time) (about 2 hours)				
Instance auto-recovery		Lifecycle				
Default		normal				
AMI Launch index		Key pair name				
0		<input type="checkbox"/> gert-keys				
Credit specification		Kernel ID				

En we hebben op AWS niveau ook Firewall regels staan in een Security Group

VPC > Security Groups > sg-072b5f533482ea51b - gert-webserver-sg

sg-072b5f533482ea51b - gert-webserver-sg

Actions ▾

Details			
Security group name gert-webserver-sg	Security group ID sg-072b5f533482ea51b	Description Gert Webserver Security Group created 2023-01-18T17:44:18.162Z	VPC ID vpc-045958566c3c024c0
Owner 986210483412	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer [Run Reachability Analyzer](#) X

Inbound rules (1/1)

<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Source
<input checked="" type="checkbox"/>	-	sgr-043db8fc99518fd70	IPv4	SSH	TCP	22	0.0.0.0/0

k. Hoe komt de instance aan een Private IP-adres?

De instance zit in een subnet dat we hebben aangemaakt (10.0.0.0/27) en een DHCP-server geeft dan automatisch IP-adressen uit in dit subnet. Behalve de IPs (10.0.0.0/27=network address, 10.0.0.255=broadcast address, 10.0.0.1=Default Gateway en 10.0.0.2=DNS)

```
ubuntu@ip-10-0-0-6:~$ networkctl status
●
    State: routable
  Online state: online
      Address: 10.0.0.6 on eth0
                  fe80::43:34ff:fea:8f9b on eth0
    Gateway: 10.0.0.1 on eth0
      DNS: 10.0.0.2
Search Domains: ec2.internal
```

De instance krijgt een IP-adres (hier 10.0.0.6) van een DHCP-server.

In onderstaande afbeelding zien we eerst het MAC-adres en het IP-adres van onze Netwerkkaart (eth0). Eronder zien we de instellingen staan in netplan, die aangeven dat DHCP gebruikt wordt voor IPv4. En in de algemene logfile zien we dat er een aanvraag is gedaan naar een DHCP-server en dat uiteindelijk het IP-adres en Default Gateway zijn aangenomen door de Client.

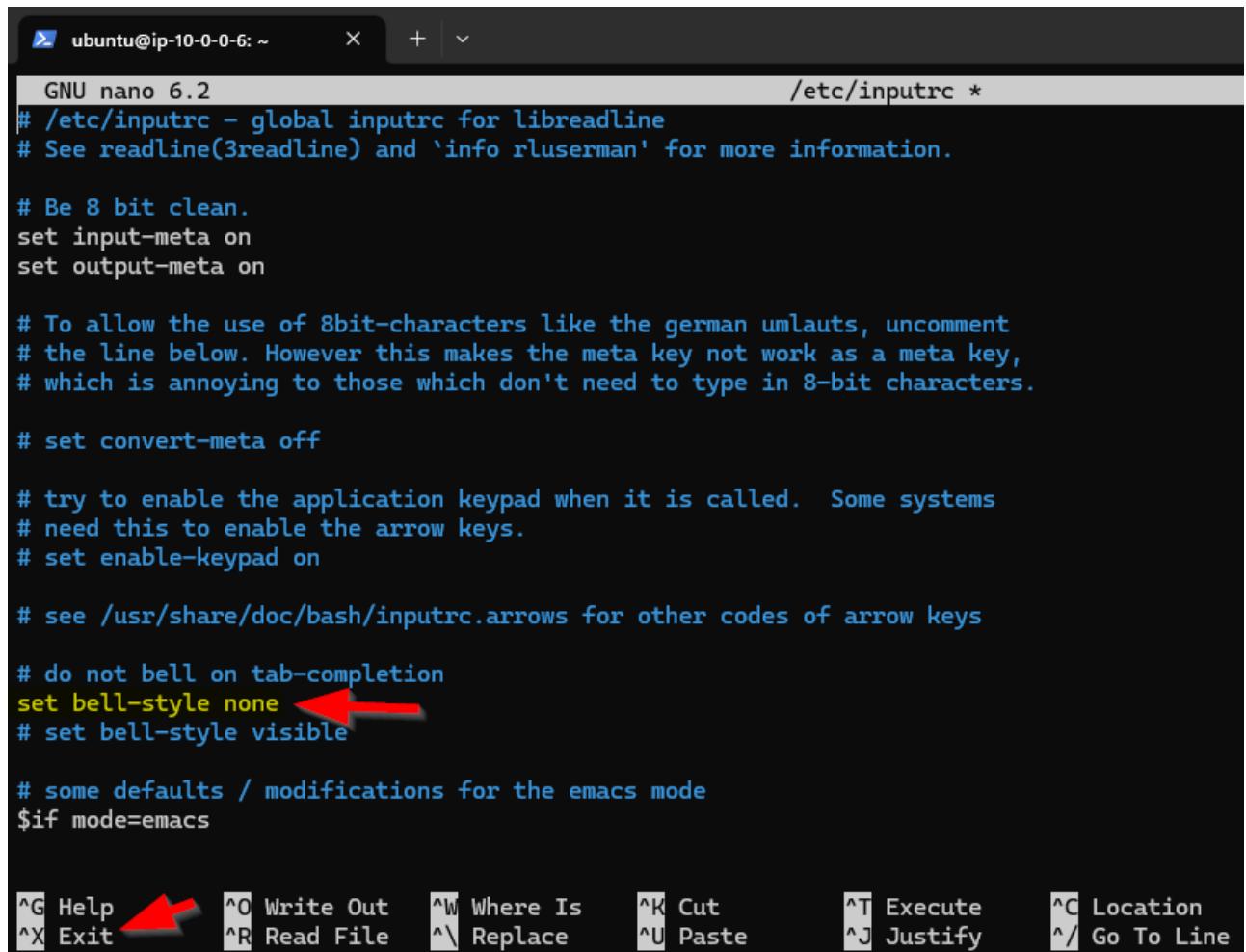
```
ubuntu@ip-10-0-0-6:~$ ip address show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:43:34:ca:8f:9b brd ff:ff:ff:ff:ff:ff
        inet 10.0.0.6/27 metric 100 brd 10.0.0.31 scope global dynamic eth0
            valid_lft 2499sec preferred_lft 2499sec
        inet6 fe80::43:34ff:fea:8f9b/64 scope link
            valid_lft forever preferred_lft forever
ubuntu@ip-10-0-0-6:~$
ubuntu@ip-10-0-0-6:~$ cat /etc/netplan/50-cloud-init.yaml
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    eth0:
      dhcp4: true
      dhcp6: false
      match:
        macaddress: 02:43:34:ca:8f:9b
      set-name: eth0
  version: 2
ubuntu@ip-10-0-0-6:~$ grep -i dhcp /var/log/syslog | head
Jan 18 17:52:41 ip-10-0-0-6 dhclient[364]: Internet Systems Consortium DHCP Client 4.4.1
Jan 18 17:52:41 ip-10-0-0-6 dhclient[364]: For info, please visit https://www.isc.org/software/dhcp
Jan 18 17:52:41 ip-10-0-0-6 dhclient[364]: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 60
Jan 18 17:52:41 ip-10-0-0-6 dhclient[364]: DHCPOFFER of 10.0.0.6 from 10.0.0.1
Jan 18 17:52:41 ip-10-0-0-6 dhclient[364]: DHCPREQUEST for 10.0.0.6 on eth0 to 255.255.255.255 port 67
Jan 18 17:52:41 ip-10-0-0-6 dhclient[364]: DHCPACK of 10.0.0.6 from 10.0.0.1 (xid=0x89d3306e)
Jan 18 17:52:41 ip-10-0-0-6 systemd-networkd[399]: eth0: DHCPv4 address 10.0.0.6/27 via 10.0.0.1
Jan 18 17:52:41 ip-10-0-0-6 kernel: [    7.933054] audit: type=1400 audit(1674064352.780:5): apparmor="/profile_load" profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-client.action" pid=328
Jan 18 17:52:41 ip-10-0-0-6 kernel: [    7.934972] audit: type=1400 audit(1674064352.784:6): apparmor="/profile_load" profile="unconfined" name="/usr/lib/NetworkManager/nm-dhcp-helper" pid=328 comm="a
Jan 18 18:37:01 ip-10-0-0-6 dhclient[369]: Internet Systems Consortium DHCP Client 4.4.1
ubuntu@ip-10-0-0-6:~$ |
```

I. Uitzetten van de systembell in de Ubuntu instance

Indien je het vrij vervelend vindt om steeds de systembell te horen bij een tab-completion, dan kan je deze uitzetten:

- via de file /etc/inputrc
- OF
- via het verwijderen van de pcspkr -kernelmodule

sudo nano /etc/inputrc



```
ubuntu@ip-10-0-0-6: ~          +  -  /etc/inputrc *
GNU nano 6.2
# /etc/inputrc - global inputrc for libreadline
# See readline(3readline) and 'info rluserman' for more information.

# Be 8 bit clean.
set input-meta on
set output-meta on

# To allow the use of 8bit-characters like the german umlauts, uncomment
# the line below. However this makes the meta key not work as a meta key,
# which is annoying to those which don't need to type in 8-bit characters.

# set convert-meta off

# try to enable the application keypad when it is called. Some systems
# need this to enable the arrow keys.
# set enable-keypad on

# see /usr/share/doc/bash/inputrc.arrows for other codes of arrow keys

# do not bell on tab-completion
set bell-style none
# set bell-style visible

# some defaults / modifications for the emacs mode
$if mode=emacs

^G Help      ^O Write Out   ^W Where Is    ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File   ^\ Replace     ^U Paste      ^J Justify    ^/ Go To Line
```

Haal de regel "set bell-style none" uit commentaar door het hekje vooraan weg te halen.

De ssh-sessie verlaten en opnieuw aanmelden over ssh om het resultaat te bekomen.

Als dat niet werkt, dan kan je het proberen met het verwijderen van de pc-speaker-kernelmodule (als deze geïmplementeerd is) met

sudo rmmod pcspkr

m. De webserver installeren

We installeren de nginx-webserver

`sudo apt update`

- dit zorgt er voor dat de computer de laatste versies van alle pakketten kent

```
ubuntu@ip-10-0-0-6:~$ sudo apt -y update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [99.8 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [831 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [183 kB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [12.1 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [566 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [87.1 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [556 B]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [786 kB]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [136 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [14.6 kB]
Get:13 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 2940 kB in 1s (3471 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
49 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

`sudo apt -y upgrade`

- update alle pakketten naar hun laatste versie

```
ubuntu@ip-10-0-0-6:~$ sudo apt -y upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
#
# News about significant security updates, features and services will
# appear here to raise awareness and perhaps tease /r/Linux ;)
# Use 'pro config set apt_news=false' to hide this and future APT news.
#
The following NEW packages will be installed:
  linux-aws-headers-5.15.0-1028 linux-headers-5.15.0-1028-aws linux-image-5.15.0-1028-aws
  linux-modules-5.15.0-1028-aws
The following packages have been kept back:
  grub-common grub-pc grub-pc-bin grub2-common python-apt-common python3-apt update-notifier-common
The following packages will be upgraded:
  apport curl git git-man initramfs-tools initramfs-tools-bin initramfs-tools-core libcurl3-gnutls libcurl4 libksba8
  libpython3.10 libpython3.10-minimal libpython3.10-stdlib libsasl2-2 libsasl2-modules libsasl2-modules-db linux-aws
  linux-headers-aws linux-image-aws open-vm-tools openssh-client openssh-server openssh-sftp-server python3-apport
  python3-distupgrade python3-problem-report python3-software-properties python3-tz python3-update-manager python3.10
  python3.10-minimal software-properties-common sudo tmux tzdata ubuntu-release-upgrader-core update-manager-core vim
  vim-common vim-runtime vim-tiny xxd
42 upgraded, 4 newly installed, 0 to remove and 7 not upgraded.
21 standard LTS security updates
Need to get 3223 kB/75.2 MB of archives.
After this operation, 230 MB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:8.9p1-3ubuntu0
...
Restarting services...
  systemctl restart packagekit.service
Service restarts being deferred:
  systemctl restart networkd-dispatcher.service
  systemctl restart unattended-upgrades.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-10-0-0-6:~$
```

Herstart de Webserver-Instance met sudo reboot

```
ubuntu@ip-10-0-0-6:~$ sudo reboot
ubuntu@ip-10-0-0-6:~$ Connection to ec2-3-231-186-123.compute-1.amazonaws.com closed by remote host.
Connection to ec2-3-231-186-123.compute-1.amazonaws.com closed.
```

```
sudo apt -y install nginx
```

- installeert de nginx-webserver

```
ubuntu@ip-10-0-0-6:~$ sudo apt -y install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  fontconfig-config fonts-dejavu-core libdeflate0 libfontconfig1 libgd3 libjbig0 libjpeg-turbo8 libjpeg8
  libnginx-mod-http-geoip2 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail
  libnginx-mod-stream libnginx-mod-stream-geoip2 libtiff5 libwebp7 libxpm4 nginx-common nginx-core
Suggested packages:
  libgd-tools fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
  fontconfig-config fonts-dejavu-core libdeflate0 libfontconfig1 libgd3 libjbig0 libjpeg-turbo8 libjpeg8
  libnginx-mod-http-geoip2 libnginx-mod-http-image-filter libnginx-mod-http-xslt-filter libnginx-mod-mail
  libnginx-mod-stream libnginx-mod-stream-geoip2 libtiff5 libwebp7 libxpm4 nginx nginx-common nginx-core
0 upgraded, 20 newly installed, 0 to remove and 7 not upgraded.
Need to get 2689 kB of archives.
After this operation, 8335 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 fonts-dejavu-core all 2.37-2build1 [1041 kB]
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 fontconfig-config all 2.13.1-4.2ubuntu5 [29.1 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 libdeflate0 amd64 1.10-2 [70.9 kB]
Get:4 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 libfontconfig1 amd64 2.13.1-4.2ubuntu5 [131 kB]
Preparing to unpack .../19-nginx_1.18.0-6ubuntu14.3_amd64.deb ...
Unpacking nginx (1.18.0-6ubuntu14.3) ...
Setting up libxpm4:amd64 (1:3.5.12-1ubuntu0.22.04.1) ...
Setting up libdeflate0:amd64 (1.10-2) ...
Setting up nginx-common (1.18.0-6ubuntu14.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /lib/systemd/system/nginx.service.
Setting up libjbig0:amd64 (2.1-3.1ubuntu0.22.04.1)
```

Met dezelfde procedure als bij SSH (zie hierboven) controleer je of

- nginx draait
- er wordt geluisterd op de juiste poort

```
ubuntu@ip-10-0-0-6:~$ systemctl status --no-pager nginx
● nginx.service - A high performance web server and a reverse proxy server
  Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2023-01-19 08:05:17 UTC; 6min ago
    Docs: man:nginx(8)
 Process: 454 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited, pid=454)
 Process: 520 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, pid=520)
 Main PID: 539 (nginx)
   Tasks: 2 (limit: 539)
     Memory: 9.0M
        CPU: 32ms
      CGroup: /system.slice/nginx.service
          ├─539 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on; pid=539"
          └─545 "nginx: worker process" "pid=545"

Jan 19 08:05:17 ip-10-0-0-6 systemd[1]: Starting A high performance web server and a rever
Jan 19 08:05:17 ip-10-0-0-6 systemd[1]: Started A high performance web server and a revers
```

```
ubuntu@ip-10-0-0-6:~$ ss -ltn
State      Recv-Q      Send-Q      Local Address:Port      Peer Address:Port
LISTEN      0           511           0.0.0.0:80           0.0.0.0:*
LISTEN      0           4096          127.0.0.53:53          0.0.0.0:*
LISTEN      0           128            0.0.0.0:22           0.0.0.0:*
LISTEN      0           511            [::]:80             [::]:*
LISTEN      0           128            [::]:22             [::]:*
```

n. De webserver lokaal testen

We testen lokaal of de webserver werkt. Omdat we op een Linux Server zitten en geen GUI hebben, moeten we dit dus doen met een Text-based-browser

- installeer lynx

```
ubuntu@ip-10-0-0-6:~$ sudo apt install -y lynx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  lynx
0 upgraded, 1 newly installed, 0 to remove and 7 not upgraded.
Need to get 719 kB of archives.
After this operation, 2029 kB of additional disk space will be used.
Get:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 lynx amd64 2.9.0dev.10-1 [719 kB]
Fetched 719 kB in 0s (20.5 MB/s)
Selecting previously unselected package lynx.
(Reading database ... 93068 files and directories currently installed.)
Preparing to unpack .../lynx_2.9.0dev.10-1_amd64.deb ...
Unpacking lynx (2.9.0dev.10-1) ...
Setting up lynx (2.9.0dev.10-1) ...
```

- en surf naar
 - 127.0.0.1

```
ubuntu@ip-10-0-0-6:~$ lynx 127.0.0.1
```

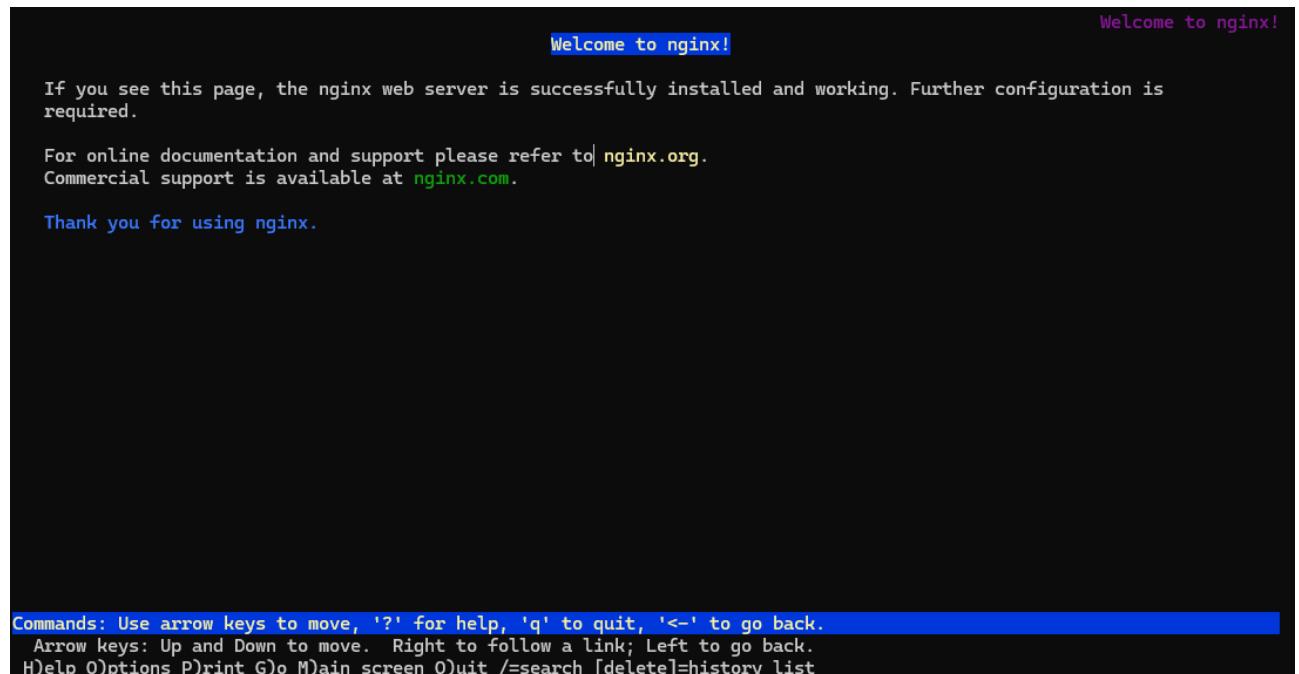
- localhost

```
ubuntu@ip-10-0-0-6:~$ lynx localhost
```

- het private IP-adres dat is toegekend aan de eth0-interface
 - op te vragen met "ip a"

```
ubuntu@ip-10-0-0-6:~$ ip a s eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
  link/ether 02:43:34:ca:8f:9b brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.6/27 metric 100 brd 10.0.0.31 scope global dynamic eth0
      valid_lft 2521sec preferred_lft 2521sec
    inet6 fe80::43:34ff:fea:8f9b/64 scope link
      valid_lft forever preferred_lft forever
ubuntu@ip-10-0-0-6:~$ lynx 10.0.0.6
```

Je zou op onderstaande pagina moeten uitkomen. De webbrowser verlaten doe je met Q



0. De webserver vanop de laptop testen en Firewall aanpassen

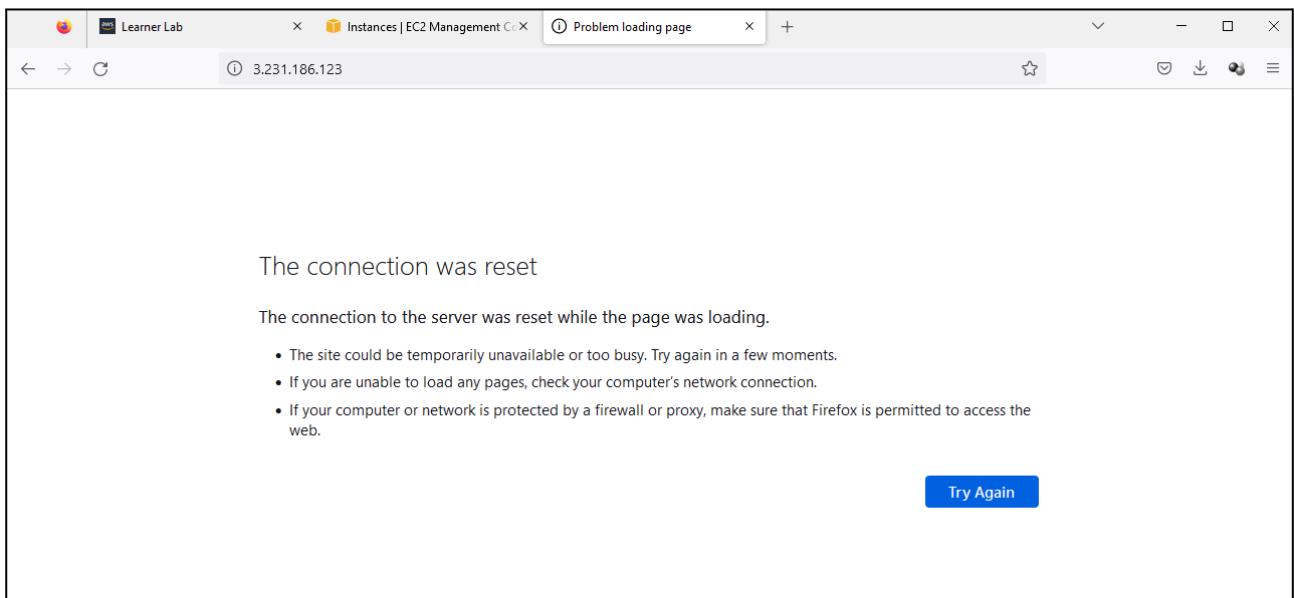
Surf vanop je laptop naar het publieke IP van de website over **http** (voor het testen van poort 80)

The screenshot shows the AWS Management Console with the EC2 service selected. The left sidebar lists various services under 'Instances', 'Images', and 'Elastic Block Store'. The main pane displays the 'Instances (1/1)' page for the 'gert-webserver' instance. A red arrow labeled '1' points to the 'Instances' link in the sidebar. Another red arrow labeled '2' points to the instance name 'gert-webserver' in the list. A red arrow labeled '3' points to the 'Networking' tab in the instance details. A red arrow labeled '4' points to the public IPv4 address '3.231.186.123'.

De website blijft een heel aantal minuten gewoon hangen bij het laden

The screenshot shows a Firefox browser window. The address bar contains the URL '3.231.186.123'. The main content area of the browser is completely blank, indicating that the website is not loading properly. The Firefox logo is visible at the top center of the browser window.

Na een hele tijd krijgen we *The connection was reset*.



Het blijkt dus nog niet te werken!

Omdat dit niet werkt zoeken we uit of er http-traffic aankomt op de Webserver

- sudo tcpdump -i eth0 port 80 (als eth0 de naam is van jouw NIC)
- We surfen nu vanaf de laptop naar het extern IP-adres van de Webserver (of refreshen)
- We kijken wat er toekomt en vertrekt van pakketjes op de Webserver

```
ubuntu@ip-10-0-0-6:~$ sudo tcpdump -i eth0 port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

We zien dat er geen enkel pakketje aankomt. Er komt dus geen externe trafiek binnen op de webserver. De trafiek wordt voordien al ergens weggefilterd.

Stop het sniffen met CTRL-C

```
ubuntu@ip-10-0-0-6:~$ sudo tcpdump -i eth0 port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C  CTRL+C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
ubuntu@ip-10-0-0-6:~$ |
```

PS: Het kan zijn dat je toch wat pakketjes ziet die komen van een APIPA adres (=169.254.0.0/16), maar niet van een extern IP

```
09:00:30.053437 IP ip-10-0-0-6.ec2.internal.49014 > 169.254.169.254.http: Flags [S], seq 620681579, win 62727, options [mss 8961,sackOK,TS val 458526329 ecr 0,nop,wscale 6], length 0
09:00:30.053797 IP 169.254.169.254.http > ip-10-0-0-6.ec2.internal.49014: Flags [S.], seq 3514497431, ack 620681580, win 62643, options [mss 8961,sackOK,TS val 1940859609 ecr 458526329,nop,wscale 7], length 0
09:00:30.053821 IP ip-10-0-0-6.ec2.internal.49014 > 169.254.169.254.http: Flags [.], ack 1, win 981, options [nop,nop,TS val 458526329 ecr 1940859609], length 0
09:00:30.053962 IP ip-10-0-0-6.ec2.internal.49014 > 169.254.169.254.http: Flags [P.], seq 1:2417, ack 1, win 981, options
```

Het surfen werkt niet omdat de trafiek wordt weggefilterd op AWS-niveau en meerbepaald via de Security Group. Dit moeten we dus oplossen.

Toevoegen van een nieuwe inbound rule in de Security Group die inkomende trafiek naar poort 80 toelaat.

Klik in het linkermenu op **Security Groups** en nadien op het ID van jouw Security Group

The screenshot shows the AWS Management Console interface. The left sidebar has a 'Network & Security' section with a 'Security Groups' link, which is highlighted with a red arrow and the number '1'. The main content area displays a table titled 'Security Groups (5)'. The table has columns for Name, Security group ID, Security group name, and VPC ID. One of the rows, for the security group 'sg-038d06718492a7108', is circled with a red circle and the number '2', indicating it is the target for modification. The table also includes a search bar at the top and various actions buttons.

	Name	Security group ID	Security group name	VPC ID
<input type="checkbox"/>	-	sg-079bab85fc36edee	launch-wizard-2	vpc-0a730d44f18
<input type="checkbox"/>	-	sg-072b5f533482ea51b	gert-webserver-sg	vpc-045958566c3
<input type="checkbox"/>	-	sg-038d06718492a7108	default	vpc-045958566c3
<input type="checkbox"/>	-	sg-097aed0bd086e01c0	launch-wizard-1	vpc-0a730d44f18
<input type="checkbox"/>	-	sg-0d80c53673cff7cf5	default	vpc-0a730d44f18

Klik op *Edit inbound rules*

EC2 > Security Groups > sg-072b5f533482ea51b - gert-webserver-sg

sg-072b5f533482ea51b - gert-webserver-sg

Actions ▾

Details

Security group name gert-webserver-sg	Security group ID sg-072b5f533482ea51b	Description Gert Webserver Security Group created 2023-01-18T17:44:18.162Z	VPC ID vpc-045958566c3c024c0
Owner 986210483412	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules Outbound rules Tags

(1) You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer X

Inbound rules (1/1)

C	Manage tags	Edit inbound rules				
<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range
<input checked="" type="checkbox"/>	-	sgr-043db8fc99518fd70	IPv4	SSH	TCP	22

Klik op *Add rule* en voeg een rule toe die inkomend HTTP verkeer toelaat over IPv4 van overal

EC2 > Security Groups > sg-072b5f533482ea51b - gert-webserver-sg > 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 Info	Protocol Info	Port range Info	Source Info	Description - optional Info
sgr-043db8fc99518fd70	SSH	TCP	22	Custom	0.0.0.0/0
-	HTTP	TCP	80	Anywhere-IPv4	0.0.0.0/0

Add rule

1. Click 'Add rule' (red arrow)

2. Select 'HTTP' from the Type dropdown (red arrow)

3. Select 'Anywhere-IPv4' from the Source dropdown (red arrow)

4. Click 'Save rules' (red arrow)

5. Click 'Save rules' (red arrow)

Het toevoegen is gelukt

ⓘ Inbound security group rules successfully modified on security group (sg-072b5f533482ea51b | gert-webserver-sg)

▶ Details

EC2 > Security Groups > sg-072b5f533482ea51b - gert-webserver-sg

sg-072b5f533482ea51b - gert-webserver-sg

Actions ▾

Details			
Security group name gert-webserver-sg	Security group ID sg-072b5f533482ea51b	Description Gert Webserver Security Group created 2023-01-18T17:44:18.162Z	VPC ID vpc-045958566c3c024c0
Owner 986210483412	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules Outbound rules Tags

ⓘ You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer X

Inbound rules (2)

	Name	Security group rule...	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-043db8fc99518fd70	IPv4	SSH	TCP	22
<input type="checkbox"/>	-	sgr-002a8e2ddae136e...	IPv4	HTTP	TCP	80

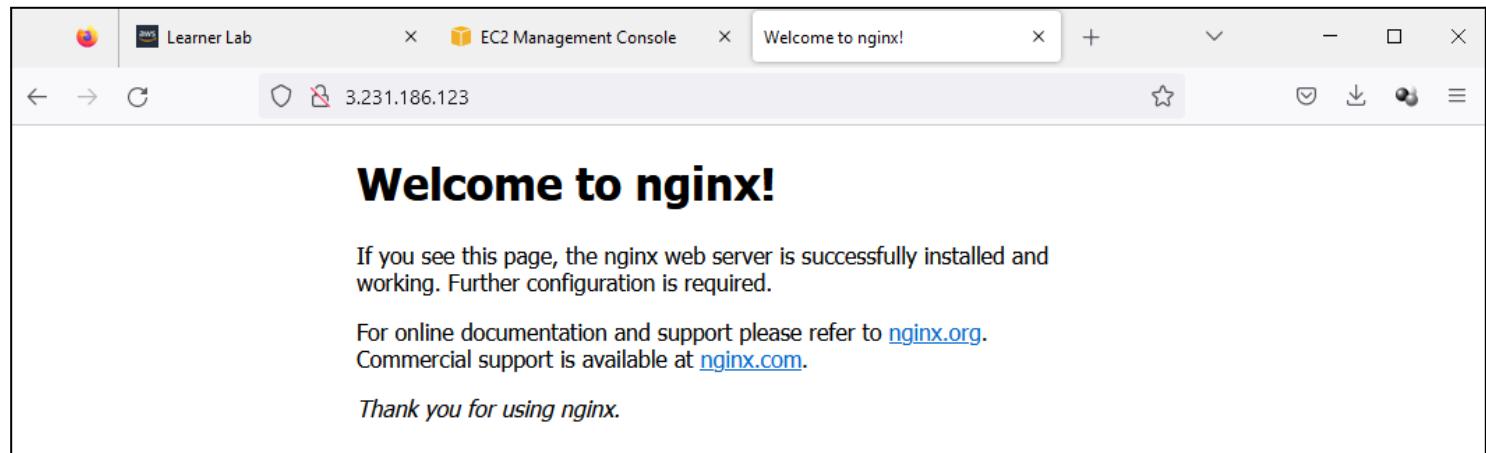
We gaan opnieuw testen of het surfen werkt

We beginnen eerst met sniffen...

- sudo tcpdump -i eth0 port 80 (als eth0 de naam is van jouw NIC)
- We surfen opnieuw vanaf de laptop naar het extern IP-adres van de Webserver via http (of Refresh)
- We kijken wat er toekomt en vertrekt van pakketjes

```
ubuntu@ip-10-0-0-6:~$ sudo tcpdump -i eth0 port 80
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
09:14:14.540820 IP 193.190.154.178.10407 > ip-10-0-0-6.ec2.internal.http: Flags [S], seq 2131210161, win 65535, options [mss 1460,nop,nop,sackOK,nop,wscale 3], length 0
09:14:14.540854 IP ip-10-0-0-6.ec2.internal.http > 193.190.154.178.10407: Flags [S.], seq 1466802162, ack 2131210162, win 62727, options [mss 8961,nop,nop,sackOK,nop,wscale 6], length 0
09:14:14.627494 IP 193.190.154.178.10407 > ip-10-0-0-6.ec2.internal.http: Flags [.], ack 1, win 65535, length 0
09:14:14.627494 IP 193.190.154.178.10407 > ip-10-0-0-6.ec2.internal.http: Flags [P.], seq 1:400, ack 1, win 32768, length 399: HTTP: GET / HTTP/1.1
09:14:14.627528 IP ip-10-0-0-6.ec2.internal.http > 193.190.154.178.10407: Flags [.], ack 400, win 974, length 0
09:14:14.627870 IP ip-10-0-0-6.ec2.internal.http > 193.190.154.178.10407: Flags [P.], seq 1:655, ack 400, win 974, length 654: HTTP: HTTP/1.1 200 OK
09:14:14.731801 IP 193.190.154.178.10407 > ip-10-0-0-6.ec2.internal.http: Flags [.], ack 655, win 32768, length 0
09:14:14.756313 IP 193.190.154.178.10407 > ip-10-0-0-6.ec2.internal.http: Flags [P.], seq 400:752, ack 655, win 32768, length 352: HTTP: GET /favicon.ico HTTP/1.1
09:14:14.756400 IP ip-10-0-0-6.ec2.internal.http > 193.190.154.178.10407: Flags [P.], seq 655:984, ack 752, win 969, length 329: HTTP: HTTP/1.1 404 Not Found
09:14:14.861890 IP 193.190.154.178.10407 > ip-10-0-0-6.ec2.internal.http: Flags [.], ack 984, win 32768, length 0
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
```

We zien dat er nu wel pakketjes aankomen van een extern adres en terug vertrekken naar dat extern adres.



De website werkt

p. De Webserver een Publieke DNS-naam geven

Voor een persoon is het natuurlijk leuker om te surfen naar een DNS-naam (www.pxl.be) dan naar een IP-adres (193.190.154.243).

We hebben gezien dat AWS zelf een heel lange DNS-naam maakt voor onze Webserver, maar we gaan er hier van uit dat we er geen hebben.

We gaan dus onze website van een DNS-naam moeten voorzien. Om dit gratis te kunnen bewerkstelligen gebruiken we de website:

<https://freedns.afraid.org/>

Surf naar de link en maak een account

The screenshot shows the homepage of Freedns.afraid.org. On the left, there's a sidebar with sections for 'For Members:' and 'For Everybody:'. The 'For Members:' section contains links like Main Menu, Domains, Subdomains, Web Forward, Dynamic DNS, IPv6 Reverse, Backup DNS, Preferences, Registry, and Logout. The 'For Everybody:' section contains links for Home, About Us, FAQ, News, DNS Stats, AUP/TOS, Contact, and Router Setup Guide. The main content area features a heading 'Free DNS Hosting, Dynamic DNS Hosting, Static DNS Hosting, subdomain and domain hosting.' Below this are two code snippets demonstrating dynamic updates via curl commands. Further down, there's a 'Common Uses:' section with a bulleted list of services offered, including Free DNS, Dynamic DNS, Static DNS, and Premium DNS. A 'Feature List:' section follows with another bulleted list of features. At the bottom right, there are two buttons: 'Sign up Free' and 'Premium Plans'. A red arrow points from the text above to the 'Sign up Free' button.

Sign Up!

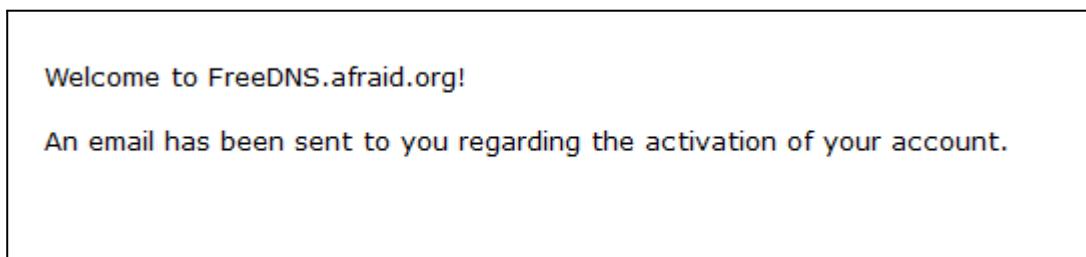
Membership Level	Starter
First Name	Gert
Last Name	Van Waeyenberg
UserID	HIDDEN
Password	*****
Password (confirm)	*****
E-Mail	gert.vanwaeyenberg@px

 [Different Image]

I agree to abide by the [Terms and Conditions](#)

Send activation email

De UserID is de loginnaam waarmee je in de toekomst wilt inloggen.



Er is een mail gestuurd naar het opgegeven email-adres.

Ga naar de mail en klik op de link.

Outlook interface showing an incoming email from FreeDNS.

Red arrows numbered 1, 2, and 3 point to specific elements:

- Arrow 1 points to the 'Ongewenste e-mail' (Spam) folder icon in the left sidebar.
- Arrow 2 points to the 'FreeDNS [freedns]: Welcome new member! A...' email preview in the inbox.
- Arrow 3 points to the activation URL in the email body.

The email body contains the following text:

[freedns]: Welcome new member! Activation instructions enclosed.

Dit bericht is geïdentificeerd als spam. Het wordt na 30 dagen verwijderd. [Het bericht is geen spam](#)

Retentie: Junk Email (30 dagen) Verloopt: Wo 2/03/2022 9:52

FreeDNS <dnsadmin@afraid.org>
Ma 31/01/2022 9:52
Aan: Gert Van Waeyenberg

Your signup to FreeDNS.afraid.org has been received.

To enable/activate your account into an operational status, you must visit this activation URL:

-> <https://eur01.safelinks.protection.outlook.com/?url=http%3A%2F%2Ffreedns.afraid.org%2Fsignup%2Factivate.php%3FBCKg4C5rG0fVi9d4f008d9e496ea70%7C0bfff66c545db46ed8b8187959e069b90%7C0%7C637792LCJBtil6lk1haWwiLCJXCI6Mn0%3D%7C2000&sdata=6WywxIUr6Ke9Rqgqg18kC>

Your signup credentials are:

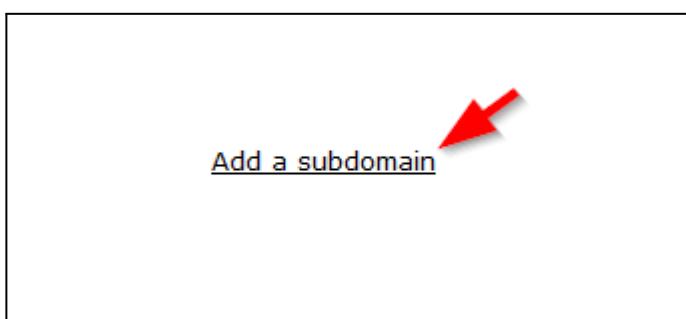
Name: Gert Van Waeyenberg

FreeDNS - Free subdomain AND

The screenshot shows the FreeDNS website interface. On the left, there's a sidebar with two sections: "For Members:" and "For Everybody:". The "For Members:" section contains links for Main Menu, Domains, Subdomains (which has a red arrow pointing to it), Web Forward, Dynamic DNS, IPv6 Reverse, Backup DNS, Preferences, Registry, and Logout. The "For Everybody:" section contains links for Home, About Us, FAQ, News, DNS Stats, AUP/TOS, Contact, Router Setup, and Guide. To the right of the sidebar is the main content area. At the top of the content area is a "FreeDNS Login!" form with fields for Email (containing "hidden") and Password (containing a series of dots). Below the form are links for "Remember Me!", "Login" (which has a red arrow pointing to it), "Recover your password here", and a note about cookies. At the bottom of the content area are two buttons: "Sign up Free" and "Premium Plans".

Log in met de login die je zonet hebt aangemaakt.

Klik op Add a subdomain (indien niet zichtbaar, klik in linkermenu op "Subdomains")



Add a new subdomain

Type:	A	explanation
Subdomain:	<input type="text"/>	
Domain:	chickenkiller.com (public)	
Destination:	chickenkiller.com (public)	
TTL:	crabdance.com (public) optional	
Wildcard:	ignorelist.com (public) more info	
	jumpingcrab.com (public)	
	mooo.com (public)	
	strangled.net (public)	
	twilightparadox.com (public)	
Many many more available ...		
		Save!

Klik bij Subdomain op "Many many more available...". Je ziet dan dat je dit moet doen via "Registry" in het linkermenu. Klik hier op.

For Members:	
[Main Menu] [Domains] [Subdomains] [Web Forward] [Dynamic DNS] [IPv6 Reverse] [Backup DNS] [Preferences] [Registry] [Logout]	<p>2 errors</p> <ul style="list-style-type: none"> You can choose from the other available domains by browsing through the S labeled Registry where you can choose from 10's of thousands of domains. <p>You can also choose to customize your default available domains dropdown box domains I am using, or show domains owned by afraid.org admin (default), or y selectable domains!</p> <p>Also, if you're already using some domains, you can use a shortcut by clicking</p> <ul style="list-style-type: none"> The security code was incorrect, please try again.
For Everybody:	
[Home] [About Us] [FAQ] [News] [DNS Stats] [AUP/TOS] [Contact]	

Showing 1-1 of 1 total			
Domain	Status	Owner	Age
Sorted by: Popularity			
generi.cc (73 hosts in use) website	public	uniquelygeneric	2819 days ago (04/05/2014)

Zoek naar een leuk domain (**best iets anders dan "generi.cc"**) en klik op de rode link van een leuke naam

Add a new subdomain

Type:	A	explanation
Subdomain:	gert	
Domain:	generi.cc (public)	
Destination:	3.231.186.123	
TTL:	For our premium supporter seconds (optional)	
Wildcard:	<input type="checkbox"/> Enabled for all subscribers (more info)	
 FOOP [Different Image]		
<input style="float: right;" type="button" value="Save!"/>		

Vul bij Subdomain **jouw voornaam** in. Dit vormt bij mij naderhand de url: gert.generi.cc.

Bij Destination vul je het publiek IP-adres in van je Webserver.

Ik kan dus naar mijn webserver surfen met:

<http://gert.generi.cc>

Klik op Save!

If you could place a small text link somewhere on your site to <https://freedns.afraid.org/> named "Free DNS" it would be greatly appreciated, to help raise search engine rankings and bring more users to the site, even if you don't think your site gets much traffic it would still help! - Josh

Want to update multiple records? Check out the [Mass Mod](#) utility.

4 subdomains	
generi.cc	[add]
<input type="checkbox"/> gert.generi.cc A 3.231.186.123	
delete selected	Add

De DNS-entry is aangemaakt!

Probeer eens te surfen naar jouw publieke URL.

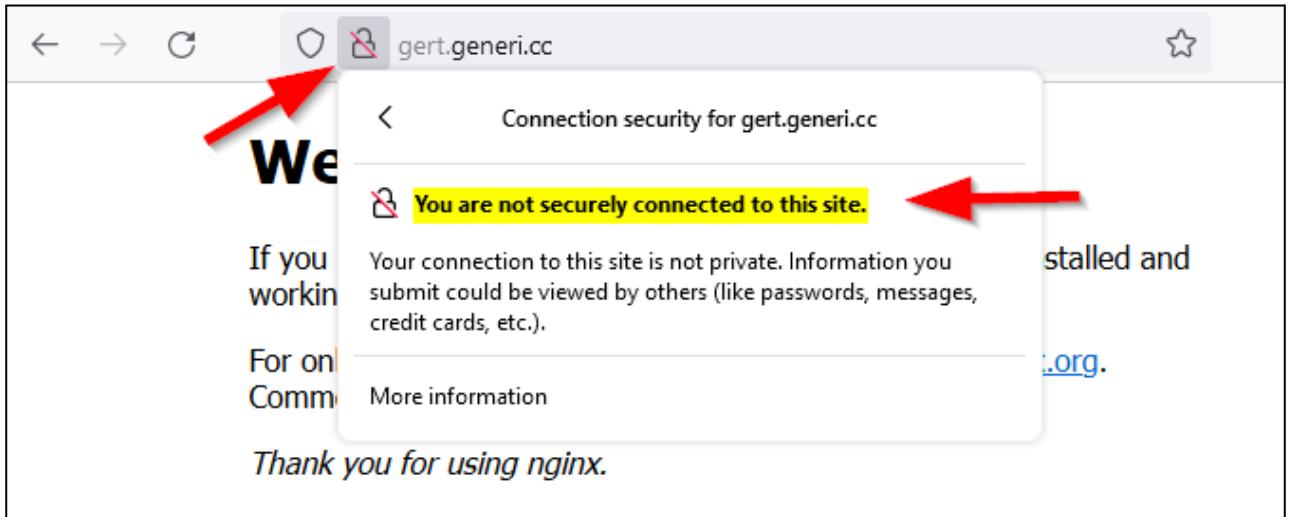


Het kan eventjes duren vooraleer dit over alle DNS servers gekend is.

- Indien het te lang duurt, kan je de informatie ook zetten in de hosts-file (op windows).

q. HTTPS met Let's Encrypt en publieke DNS

Indien we naar de website surfen krijgen we wel de waarschuwing dat het niet veilig is. Dit is omdat we over http gaan en niet over https. De data die over de lijn loopt is dan niet geëncrypteerd en daarom zouden hackers kunnen meekijken.



We gaan de website beveiligen met een certificaat. Dit kunnen Self-signed certificates zijn. Deze zijn gratis en iedereen kan ze lokaal aanmaken. Maar dan krijgen de eindgebruikers nog altijd een veiligheidswaarschuwing. Maar buiten deze waarschuwing is alle data wel geëncrypteerd!

Indien we geen Self-signed certificates willen gebruiken kunnen we er kopen.

Er is echter een mogelijkheid om toch gratis certificates te bekomen die geen waarschuwing meer geven. Dat gaan we doen met "Let's Encrypt".

Eerst het https verkeer toelaten

Op dezelfde manier als we voor http het verkeer hebben doorgelaten via onze Security Group op AWS zal je dit nu ook moeten doen voor https-verkeer.

- Voeg in jouw VPC aan jouw Security Group een regel toe om https-verkeer toe te laten

Let's Encrypt certificate implementeren

De procedure staat hieronder uitgeschreven

- We installeren de Certbot software en zijn nginx-plugin :
 - sudo apt install certbot python3-certbot-nginx

```
ubuntu@web-webserver1:~$ sudo apt install certbot python3-certbot-nginx
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-acme python3-certbot python3-configargparse python3-future python3-icu python3-josepy python3-mock
  python3-parsedatetime python3-nbr python3-pyparsing python3-requests-toolbelt python3-rfc3339 python3-tz
  python3-units
```

- We passen de Default-website aan:
 - sudo nano /etc/nginx/sites-enabled/default
 - verander de directive server_name als volgt
 - server_name **jouw_url**;

```
server_name gert.generi.cc;
```

- check de syntax
 - sudo nginx -t

```
ubuntu@ip-10-0-0-6:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

- herstart de service
 - sudo systemctl restart nginx

```
ubuntu@web-webserver1:~$ sudo systemctl restart nginx
```

- Controleer of je nog altijd naar je website kan surfen



- Vraag het certificaat aan
 - sudo certbot --nginx -d jouw.url.be

```
ubuntu@ip-10-0-0-6:~$ sudo certbot --nginx -d gert.generi.cc
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): gert.vanwaeyenberg@pxl.be
```

```
-----  
Please read the Terms of Service at  
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must  
agree in order to register with the ACME server. Do you agree?
```

```
-----  
(Y)es/(N)o: Y
```

```
-----  
Would you be willing, once your first certificate is successfully issued, to  
share your email address with the Electronic Frontier Foundation, a founding  
partner of the Let's Encrypt project and the non-profit organization that  
develops Certbot? We'd like to send you email about our work encrypting the web,  
EFF news, campaigns, and ways to support digital freedom.
```

```
-----  
(Y)es/(N)o: N
```

```
Account registered.
```

```
Requesting a certificate for gert.generi.cc
```

```
Successfully received certificate.
```

```
Certificate is saved at: /etc/letsencrypt/live/gert.generi.cc/fullchain.pem
```

```
Key is saved at: /etc/letsencrypt/live/gert.generi.cc/privkey.pem
```

```
This certificate expires on 2023-04-20.
```

```
These files will be updated when the certificate renews.
```

```
Certbot has set up a scheduled task to automatically renew this certificate in the background.
```

```
Deploying certificate
```

```
Successfully deployed certificate for gert.generi.cc to /etc/nginx/sites-enabled/default
```

```
Congratulations! You have successfully enabled HTTPS on https://gert.generi.cc
```

```
-----  
If you like Certbot, please consider supporting our work by:
```

```
* Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate
```

```
* Donating to EFF: https://eff.org/donate-le
```

We zien dat het certificaat maar een 90 dagen geldig zal blijven. We moeten dus voor die tijd een nieuwe aanvraag doen. De procedure van het opnieuw aanvragen gebeurt echter automatisch op de achtergrond via een Systemd-timer, genaamd "certbot.timer". Deze timer controleert tweemaal per dag of er certificaten zijn die nog slechts 30 geldig zijn. Indien dit het geval is zal dat certificaat vernieuwd worden.

```
ubuntu@ip-10-0-0-6:~$ systemctl status certbot.timer
● certbot.timer - Run certbot twice daily
   Loaded: loaded (/lib/systemd/system/certbot.timer; enabled; vendor preset: enabled)
   Active: active (waiting) since Fri 2023-01-20 12:02:50 UTC; 34min ago
     Trigger: Sat 2023-01-21 06:35:26 UTC; 17h left
  Triggers: ● certbot.service

Jan 20 12:02:50 ip-10-0-0-6 systemd[1]: Started Run certbot twice daily.
```

Testen van de aanpassingen

We kunnen nu testen of het werkt.

Surf via de DNS-naam naar je website over http (niet https)

OF

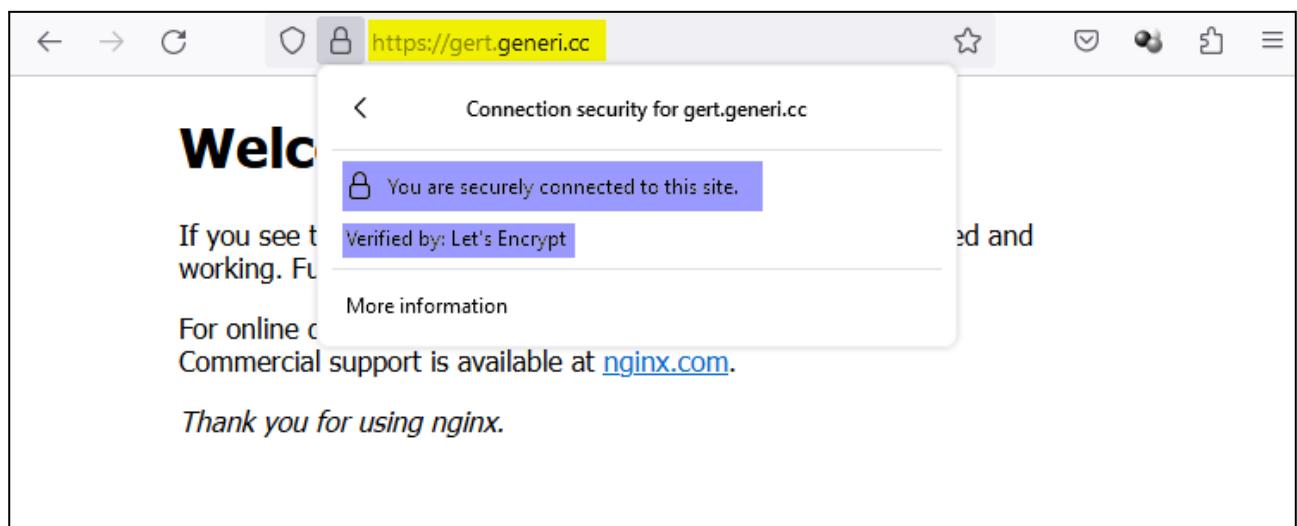
druk op CTRL-F5 indien je website nog open staat

Je ziet dat er automatisch geredirect wordt naar HTTPS en dat er geen veiligheidswaarschuwing meer wordt gegeven.



Je kan natuurlijk ook onmiddellijk surfen over https.

Je ziet nu ook dat er een certificaat is uitgereikt door "Let's Encrypt".



Klik op *More Information* als je meer informatie wilt over het certificaat.

The screenshot shows the Firefox 'Page Info' dialog for the URL <https://gert.generi.cc/>. The 'Security' tab is selected, displaying information about the website's identity, privacy history, and technical details. A 'View Certificate' button is present. To the right, a separate window titled 'Certificate' displays detailed information about the SSL/TLS certificate for gert.generi.cc, issued by R3. The certificate details include:

Subject Name	
Common Name	gert.generi.cc
Issuer Name	
Country	US
Organization	Let's Encrypt
Common Name	R3
Validity	
Not Before	Fri, 20 Jan 2023 11:11:42 GMT
Not After	Thu, 20 Apr 2023 11:11:41 GMT
Subject Alt Names	
DNS Name	gert.generi.cc
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	F5:78:73:25:84:6C:61:AD:5F:AE:84:B9:AF
Miscellaneous	
Serial Number	03:11:0F:DE:B2:15:1A:3F:42:61:66:D1:A3
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

Opkijken van de config

Indien je nu surft over https naar jouw Publiek **IP-adres** krijg je een waarschuwing. Dit omdat het certificaat gekoppeld is aan de DNS-naam en niet aan het IP-adres.

Je kan wel doorklikken om de website te bezoeken.

The screenshot shows a Firefox browser window with the following details:

- Address Bar:** Shows the URL <https://3.231.186.123>.
- Content Area:**
 - An orange warning icon with an exclamation mark is displayed.
 - The text "Warning: Potential Security Risk Ahead" is shown.
 - A detailed message states: "Firefox detected a potential security threat and did not continue to **3.231.186.123**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details."
 - A section titled "What can you do about it?" contains the text: "The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem." Below this is a link "Learn more...".
 - At the bottom of the warning area are two buttons: "Go Back (Recommended)" (blue) and "Advanced..." (grey).
- Bottom Panel:**
 - The text "Websites prove their identity via certificates. Firefox does not trust this site because it uses a certificate that is not valid for 3.231.186.123. The certificate is only valid for gert.generi.cc." is displayed.
 - The error code "Error code: SSL_ERROR_BAD_CERT_DOMAIN" is shown.
 - A link "View Certificate" is present.
 - At the bottom are two buttons: "Go Back (Recommended)" (blue) and "Accept the Risk and Continue" (grey).

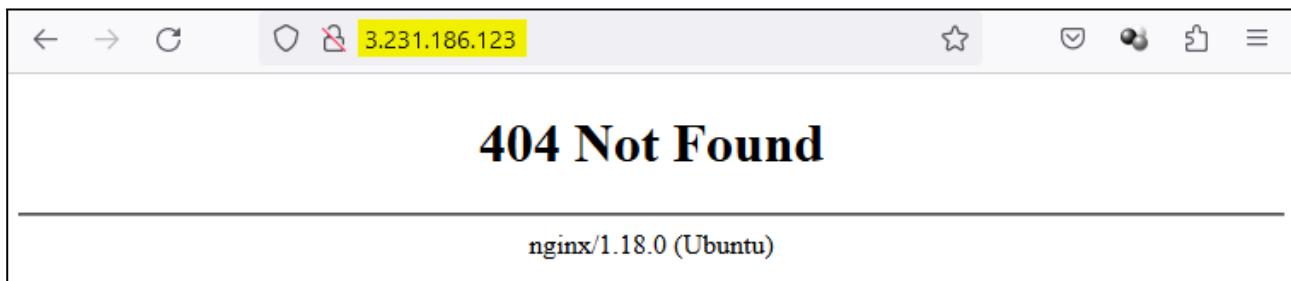
Two red arrows point to specific buttons:

- Arrow 1 points to the "Advanced..." button in the first warning panel.
- Arrow 2 points to the "Accept the Risk and Continue" button in the bottom panel.

De Webbrowser zal dus enkel niet klagen als we met de Website verbinden via de common-name binnen het certificaat.

Certificate		
gert.generi.cc	R3	ISRG Root X1
Subject Name		
Common Name	gert.generi.cc	
Issuer Name		
Country	US	
Organization	Let's Encrypt	
Common Name	R3	

Indien we surfen over http naar het Publiek **IP-adres** van onze website krijgen we een 404.



Dit komt omdat Let's Encrypt dit in de config van onze website (/etc/nginx/sites-enabled/default) heeft toegevoegd.

```
ubuntu@ip-10-0-0-6:~$ tail -15 /etc/nginx/sites-enabled/default
server {
    if ($host = gert.generi.cc) {
        return 301 https://$host$request_uri;
    } # managed by Certbot

    listen 80 default_server;
    listen [::]:80 default_server;

    server_name gert.generi.cc;
    return 404; # managed by Certbot

}
```

Indien je dit toch wilt toelaten en tegelijkertijd altijd wilt redirecten van http naar https, dan moet je de hieronder aangegeven regels in commentaar plaatsen en de nginx-service herstarten.

```
ubuntu@ip-10-0-0-6:~$ tail -15 /etc/nginx/sites-enabled/default
server {
    # if ($host = gert.generi.cc) {
    #     return 301 https://$host$request_uri;
    # } # managed by Certbot

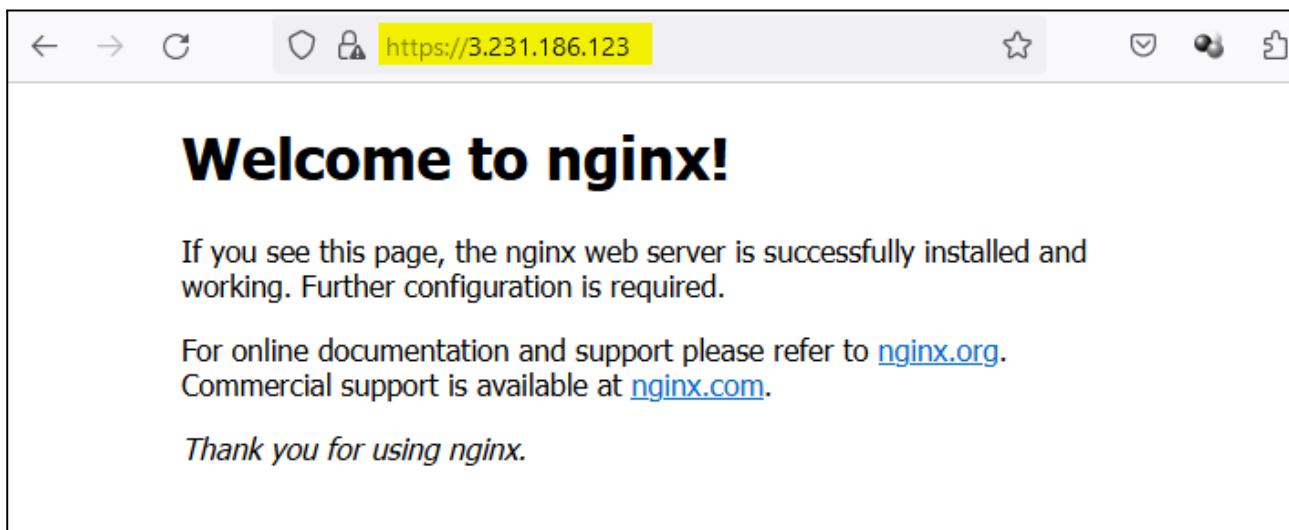
    listen 80 default_server;
    listen [::]:80 default_server;

    server_name gert.generi.cc;
    # return 404; # managed by Certbot

}
```

PS: De return 404 in commentaar zetten is eigenlijk niet echt nodig, omdat er toch steeds wordt geredirect van HTTP naar HTTPS.

Surf opnieuw over http naar het Publiek **IP-adres** van onze website of druk CTRL-F5. Zoals je ziet wordt er nu wel automatisch geredirect naar HTTPS.



Eindpresentatie

In een filmpje van **maximum** 5 minuten leg je technisch uit hoe je tot het eindresultaat bent gekomen.

- Begin het filmpje door te zeggen wie je bent.
- Toon kort de webserver-instance in AWS Cloud met zijn DNS naam
 - Zorg dat je loginnaam in de rechterbovenhoek zichtbaar is
- Toon de SSH-keys die je hebt gemaakt in de Cloud-shell en waar deze staan op je laptop, en dat de verbinding werkt.
- Toon dat je website werkt door via de door jouw gekozen browser te surfen over http, vanaf je laptop, naar het publiek IP-adres van uw website.
- Leg ook uit in het filmpje hoe het juist zit met de gebruiker ubuntu waarmee je connecteert naar de Server over SSH. Volgende vragen dienen beantwoord :
 - Heeft deze gebruiker een wachtwoord?
 - Waarom kan je sudo doen zonder een wachtwoord op te geven?
- Toon de DNS-entry op freedns.afraid.org.
 - Toon dat je naar je Webserver kan surfen via de DNS-naam.
- Toon je certificaat op je Webserver.
 - Toon dat je kan surfen over https naar je Webserver
 - Toon het certificaat in je webbrowser als je naar uw website surft.
 - Toon aan dat je certificaat automatisch opnieuw zal aangevraagd worden binnen de 90 dagen.
- Als laatste probeer je op een supervlotte manier uit te leggen hoe het komt dat jouw Webserver aan een IP-adres en DNS-naam komt binnen AWS en hoe dat je protocollen en poorten hebt doorgelaten zodanig dat de website mag benaderd worden over http en https.
- Plaats het filmpje op youtube.
 - Zet de Visibility van het youtube-filmpje op Unlisted.
 - Je zal de Video link van dit filmpje moeten doorgeven ter evaluatie van deze taak
 - kijk terug naar de Takenlijst voor een link naar het upload-formulier.
- **Waar houden we nog rekening mee bij de evaluatie**
 - De video moet ingesproken zijn.
 - Enthousiast en niet te eentonig.
 - Gebruik professioneel taalgebruik.
 - Je moet jezelf ook in beeld hebben via de webcam

- De video moet voorbereid zijn
 - Zet reeds de nodige websites open in tabbladen
 - ...
- Knip fouten uit de video en zorg dat dit niet opvalt.
- Toon aan dat je weet wat je gedaan hebt en dat je dit alles begrijpt zodat een minder technisch geschoold persoon toch zeer goed de uitleg kan begrijpen om tot het gepubliceerde resultaat te komen.

Je moet dus zelf zorgen dat wij alles zien in het filmpje op een enthousiaste en correcte manier. Hoe beter, zelfzekerder en duidelijker, hoe hoger de punten.