



INHOUDSTAFEL

1	Doelstelling.....	3
2	Ubuntu EC2 aanmaken.....	3
2.1	Kies een Amazone Machine Image (AMI)	3
2.2	Keuze van het type van virtuele server.....	4
2.3	Configuratie van de virtuele server.....	4
2.4	Opslagruimte toevoegen.....	5
2.5	Je virtuele machine benoemen	5
2.6	Veiligheidsgroep configureren	6
2.7	Overzicht en validatie.....	6
3	Mysql server opmaken.....	8
4	Database opmaken	10
5	Dynamic DNS aanmaken.....	11
6	Https beveiligen.....	11
7	Https endpoint action toevoegen aan Aws	12

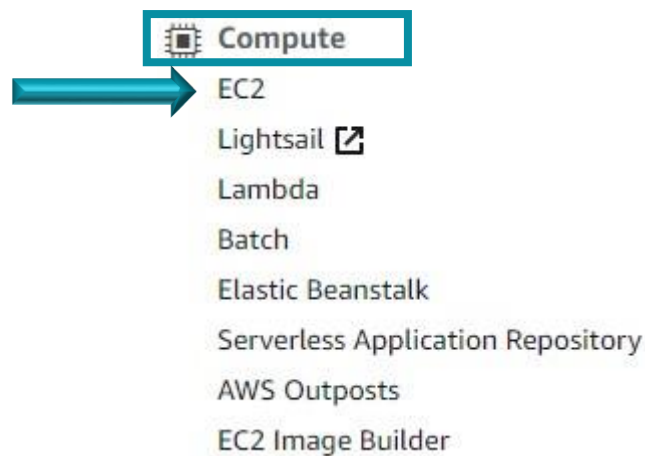
1 DOELSTELLING

Dit document beschrijft hoe de communicatie tussen AWS IoT Thing en EC2 tot stand moet gebracht worden.

2 UBUNTU EC2 AANMAKEN

Nadat je bent ingelogd op de AWS-website kan je de EC2 aanmaken.

- Ga naar het gedeelte "Compute"
- Klik op EC2



- Ga naar "Instances"
- Klik op "Instances New"

▼ Instances

Instances New

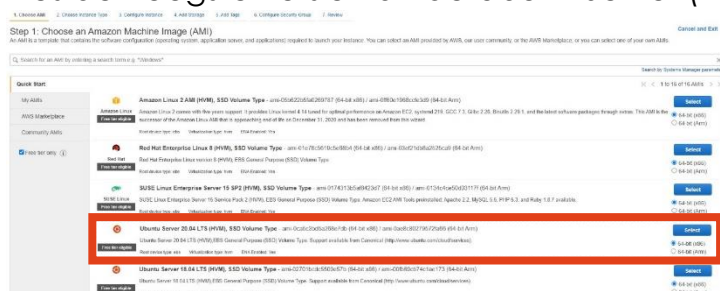
- Klik op "Launch Instances"

Launch Instances ▼

Je moet 7 stappen doorlopen om de Ubuntu EC2 aan te maken :

2.1 Kies een Amazon Machine Image (AMI)

- Kies de hoogste versie van de Ubuntu Server (20.04)



- Klik op "Next: Configure Instance Details"

Next: Configure Instance Details

2.2 Keuze van het type van virtuele server

Kies voor een GRATIS virtuele server (anders moet je maandelijks betalen om een virtuele server te mogen gebruiken)

- Kies "t2.micro free tier eligible" door het vakje in de eerste kolom aan te klikken
- Klik op "Next: Configure Instance Details"

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more about instance types and how they can meet your computing needs.](#)

Filter by: All instance families Current generation Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, -, 1 GB memory, EBS only)

	Family	Type	vCPUs	Memory (GB)	Instance Storage (GB)	EBS Optimized Available	Network Performance	IPv6 Support
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t2	t2.xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.small	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.medium	2	4	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.large	2	8	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	t3	t3.xlarge	4	16	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

2.3 Configuratie van de virtuele server

Je moet niets aanpassen. De standaard instelling zijn voldoende.

- Klik op "Next: Add Storage"

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details
Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 1 Launch into Auto Scaling Group

Purchasing option ☐ Request Spot instances

Network vpc-757a200d (default) Create new VPC

Subnet No preference (default subnet in any Availability Zone) Create new subnet

Auto-assign Public IP Use subnet setting (Enable)

Placement group ☐ Add instance to placement group

Capacity Reservation Open

Domain join directory No directory Create new directory

IAM role None Create new IAM role
Select an IAM role that has read access to Secrets Manager, and that has the following AWS managed policies attached to it: AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess. [Learn more](#)

CPU options ☐ Specify CPU options

Shutdown behavior Stop

Stop - Hibernate behavior ☐ Enable hibernation as an additional stop behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Elastic inference ☐ Add an Elastic Inference accelerator

Cancel Previous Review and Launch Next: Add Storage

2.4 Opslagruimte toevoegen

Je geeft mee over hoeveel opslagruimte je wenst te beschikken. De standaard instellingen zijn voldoende.

- Klik op “Next: Add Tags”

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Volume Type (1)	Device (1)	Snapshot (1)	Size (GiB) (1)	Volume Type (1)	IOPS (1)	Throughput (MB/s) (1)	Delete on Termination (1)	Encryption (1)
Root	/dev/sda1	snap-09d3a0caf6c20b475	8	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GiB of EBS General Purpose (SSD) or Magnetic storage. Learn more about free usage tier eligibility and usage restrictions.

Cancel Previous **Review and Launch** **Next: Add Tags**

2.5 Je virtuele machine benoemen

- Klik op “Add Tag”

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances (1)	Volumes (1)	Network Interfaces (1)
This resource currently has no tags.				
Choose the Add tag button or click to add a Name tag.				
Make sure your IAM policy includes permissions to create tags.				

Add Tag (Up to 50 tags maximum)

- Je kan een sleutel en een waarde ingeven. Als waarde kies je best je eigen naam zodat je weet dat het om jouw virtuele machine gaat.

Key (128 characters maximum)	Value (256 characters maximum)	Instances (1)	Volumes (1)	Network Interfaces (1)
name	cedric	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- Klik op “Next: Configure Security Group”

Cancel Previous **Review and Launch** **Next: Configure Security Group**

2.6 Veiligheidsgroep configureren

Je moet een veiligheidsregel toevoegen voor :

- De SSH-connectie
- De HTTP-connectie
- De HTTPS-connectie

Omdat je dus 3 regels moet aanmaken, zal je 2 keer op de knop “Add Rule” moeten klikken.

Je kiest uit het keuzemenu voor welke connectie je een regel wilt aanmaken.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:
Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

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

- Klik op “Next: Preview and Launch”

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group
A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:
Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

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

Cancel Previous **Review and Launch**

2.7 Overzicht en validatie

Je krijgt een overzicht van hoe de virtuele machine werd opgezet.
Indien je akkoord gaat met de verschillende instellingen.

- Klik je op de knop “Launch” om te bevestigen

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

AMI Details

Ubuntu Server 20.04 LTS (HVM), SSD Volume Type - ami-0ca5c3bd5a268e7db

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups

launch-sg-14

Description

launch-sg-14 created 2021-03-22T10:26:13.490+01:00

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	
HTTP	TCP	80	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	

Instance Details

Storage

Tags

Cancel Previous Launch

- Je moet een sleutelpaar (publieke en private sleutel) kiezen of aanmaken. Door op het pijltje te klikken kan je kiezen uit een keuzelijst. Kies "Create a new key pair"

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Create a new key pair
Choose an existing key pair
Create a new key pair
Proceed without a key pair

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. Store it in a **secure and accessible location**. You will not be able to download the file again after it's created.

Cancel Launch Instances

- Geef een naam aan de sleutel [1]
- Download de sleutel door op de knop "Download Key Pair" te klikken [2]
- Klik op "Launch Instances" [3]

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Create a new key pair

Key pair name

r0804148

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. Store it in a **secure and accessible location**. You will not be able to download the file again after it's created.

Cancel Launch Instances

- Als je op “View Instances” klikt, krijg je een overzicht van alle virtuele servers die werden aangemaakt.

Launch Status

Your instances are now launching
The following instance launches have been initiated: i-010e25f81be5369 View launch log

Get notified of estimated charges
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances. Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. Find out how to connect to your instances.

▼ Here are some helpful resources to get you started

- How to connect to your Linux instance
- Amazon EC2: User Guide
- Learn about AWS Free Usage Tier
- Amazon EC2: Discussion Forum

While your instances are launching you can also

- Create status check alarms to be notified when these instances fail status checks. (Additional charges may apply)
- Create and attach additional EBS volumes. (Additional charges may apply)
- Manage security groups

[View instances](#)

Instances (1/15) info

Filter instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4	Elastic IP
r0640239	i-03e429223328c2691	Stopped	t2.micro	–	No alarms	us-west-2c	–	–	–
r0704309	i-008b7722fb8e89786	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	ec2-18-237-153-198.us...	18.237.153.198	–
Quinten	i-0aa6c45912898ad80	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	ec2-34-216-92-153.us...	34.216.92.153	–
Lander	i-0e39649b691f54ee6	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	ec2-34-212-40-255.us...	34.212.40.255	–
r0781287	i-0c0e4e05f0c1ffa7c	Stopped	t2.micro	–	No alarms	us-west-2c	–	–	–
r0781787	i-0a3074152b9c237c8	Stopped	t2.micro	–	No alarms	us-west-2c	–	–	–
--	i-04bd6447566a0996d	Stopped	t2.micro	–	No alarms	us-west-2c	–	–	–
r0787887	i-07446eefda725ec5d	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	ec2-54-202-56-131.us...	54.202.56.131	–
stefwelleman	i-0914e603f19bdc886	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	ec2-34-211-112-251.us...	34.211.112.251	–
r0671598	i-036fbac1a8b5b0fda	Stopped	t2.micro	–	No alarms	us-west-2b	–	–	–
r0759090	i-03a11d1ca85d6c6f8	Running	t2.micro	2/2 checks passed	No alarms	us-west-7b	ec2-52-26-208-94.us-w...	52.26.208.94	–
<input checked="" type="checkbox"/> r0804148_cedric	i-010e25f81be5369	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-54-203-137-181.us...	54.203.137.181	–
JoachimP	i-08c00f40a35fc623	Stopped	t2.micro	–	No alarms	us-west-2a	–	–	–
r0802087	i-0594e051d14dc852c	Stopped	t2.micro	–	No alarms	us-west-2a	–	–	–
r0781530	i-094708411357ef2b2	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	ec2-54-184-202-204.us...	54.184.202.204	–

3 MYSQL SERVER OPMAKEN

- Open je Putty
- Voer onder “Host Name” het IP-adres in dat je op de EC2-server onder “Public IPv4” terugvindt

Putty Configuration

Category: Session

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) **54.203.137.181** Port 22

Connection type: ☐ Raw ☐ Telnet ☒ SSH ☐ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Load Save Delete

Close window on exit: ☐ Always ☐ Never ☒ Only on clean exit

Open Cancel

Public IPv4 ...

18.237.153.198

34.216.92.153

34.212.40.255

–

–

–

54.202.56.131

34.211.112.251

–

52.26.208.94

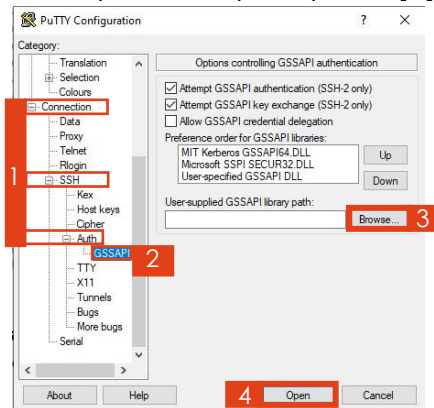
54.203.137.181

–

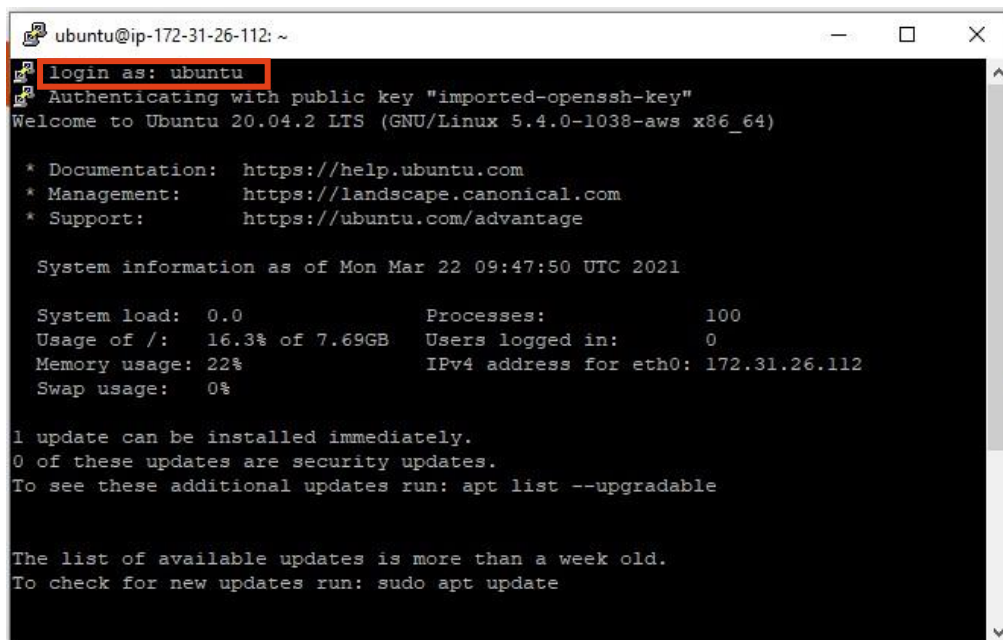
–

54.184.202.204

- Klap de volgende folders onder "Category" open : Connection – SSH – Auth [1]
- Klik op GSSAPI [2]
- Klik op de knop "Browse" om de Key Pair die je downloade op te halen [3]
- Klik op de knop "Open" [4]



- Voer je login in : "Ubuntu"



- Je moet volgende commando's intypen om onderdelen, bibliotheken en certificaten te installeren :
 - `Sudo apt install apache 2`
Installeert apache
 - `Sudo apt install mysql-server`
Installeert mysql

- `Sudo apt install php libapache2-mod-php php-mysql`
Installeert php met mysql module
- `Sudo systemctl restart apache2`
Heropstarten van apache
- `Sudo chmod 777/var/www/html`
Geeft schrijfrechten voor iedereen op html
- `Sudo apt install certbot`
Installeert certbot
- `Sudo apt install python-3-certbot-apache`
Installeert de nodige bibliotheken
- `Sudo certbot—apache`
Vraagt certificaat aan
- `Sudo tail/var/log/apache2/access.log`
Gaat token zoeken voor activatielink AWS IoT

4 DATABASE OPMAKEN

- Voer het commando "InfluxDB" in
- Ga naar de website van Github via volgende link :
<https://github.com/cedric-carels/Cloud-and-Security/tree/main/Assignment%203/ubuntu>
- Open "sql.txt"
- Voer de commando's uit die in dit txt-document staan
- Sluit af door het commando "exit" in te voeren
- Voer het commando "cd/var/www/html" in
- Voer het commando "nano secrets.php" in
- Ga naar de website van github (zie puntje 2 onder dit hoofdstuk)
- Open "secrets.example.php"
- Voer de commando's uit die in dit document staan
- Vergeet niet te bewaren
- Volg dezelfde stappen (zie 1) voor "test.php" en "mysql_connect.php"



5 DYNAMIC DNS AANMAKEN

- Ga naar de website van NOIP (zie hieronder) en maak een account aan.
<https://www.noip.com/support/knowledgebase/installing-the-linux-dynamic-update-client-on-ubuntu/>
- Log in
- Maak een nieuwe hostname aan **Create Hostname**
 - [1] Hostnaam : naam die je wenst te gebruiken. Als de naam al bestaat, krijg je een melding en moet je dus een nieuwe naam kiezen
 - [2] Record Type : DNS Host (A) = staat standaard zo ingesteld
 - [3] Domein : je kiest "hopto.org" uit de keuzelijst
 - [4] IPv4 Adres : is het IP-adres van je EC2-instance
 - [5] Klik op de knop "Create Hostname"

Create a Hostname

Hostname ¹

Domain ³

Record Type ²

☒ DNS Host (A) ²

☐ AAAA (IPv6) ²

☐ DNS Alias (CNAME) ²

☐ Web Redirect ²

[Manage your Round Robin, TXT, SRV and DKIM records.](#)

Wildcard ²

[Upgrade to Enhanced](#)
to enable wildcard hostnames.

MX Records

[+ Add MX Records](#)

IPv4 Address ⁴

Public IPv4 ...

18.237.153.198
34.216.92.153
34.212.40.255
54.202.56.131
34.211.112.251
52.26.208.94
54.203.137.181
54.184.202.204

5

6 HTTPS BEVEILIGEN

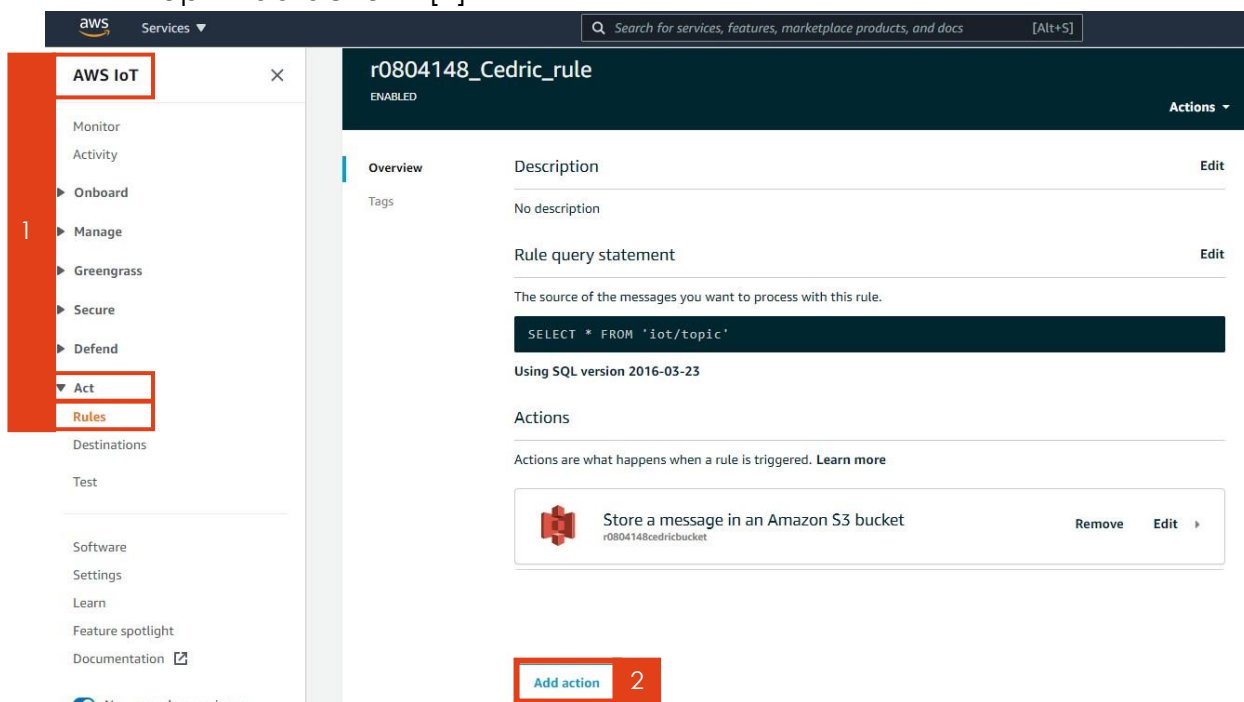
- Open of activeer "Putty". Moest je Putty hebben afgesloten moet je terug inloggen op Ubuntu
- Voer het commando "cd/var/www/html" in
- Voer het commando "nano api.php" in
- Ga naar de website van github (zie hoofdstuk 4)
- Open "api.php"
- Voer de commando's uit die in dit document staan
- Vergeet niet te bewaren
- Volg dezelfde stappen (zie 1) voor "lijst.php"



7 HTTPS ENDPOINT ACTION TOEVOEGEN AAN AWS

Je gaat een https endpoint action toevoegen aan de AWS IoT regel (rule) die je aanmaakte (zie taak 2) en verwijzen naar je api.php pagina.

- Open AWS website of activeer hem mocht deze nog open staan
- Ga naar “AWS IoT” door hierop te klikken [1]
- Ga naar “Act” door hierop te klikken [1]
- Klik op “Rules” [1]
- Klik op “Add action” [2]



- Kies “Send a message to downstream https endpoint” uit de keuzelijst door het bolletje aan te klikken




- Klik op de knop “Configure action”



- Vul de configuratie gegevens in :
 - [1] HTTPS Endpoint : dit is het hostname die je invulde bij het aanmaken van een Dynamic DNS (zie punt 5)
 - [2] Bevestiging van de url mag blanco gelaten worden
 - Hoofdingen (headers) :
 - [3] Key : Je moet 3 sleutels aanmaken. Je krijgt in het begin maar één vak, om vakken toe te voegen moet je op de knop "add another" [5] klikken. Je moet volgende sleutels aanmaken door de text in te typen :
 - Een voor de ID van je apparaat
 - Een voor de temperatuur
 - Een voor de vochtigheidsgraad
 - [4] Value (waarde) : je moet aan elke sleutel een waarde meegeven door de text in te typen

AWS IoT > Rules > r0804148_Cedric_rule

Configure action


 Send a message to a downstream HTTPS endpoint
HTTPS

Endpoint

Provide the HTTPS endpoint to receive messages, as well as the confirmation URL associated with the endpoint. The confirmation URL is used to confirm your ownership of the endpoint, and must be the prefix of the endpoint. [Learn more about destinations](#)

HTTPS Endpoint

1

Confirmation URL 

2

Headers

Add headers to your HTTP request to pass additional information with your request. A header consists of a key-value pair.

Key	Value	
<input type="text" value="Device_id"/>	<input type="text" value="\${device_id}"/>	3
<input type="text" value="Temperature"/>	<input type="text" value="\${temperature}"/>	
<input type="text" value="Humidity"/>	<input type="text" value="\${humidity}"/>	

4

5

Authentication

Add request authentication (optional).