AMIS | CONCLUSION TECHNOLOGY BLOG

Getting value from IoT, Integration and Data Analytics

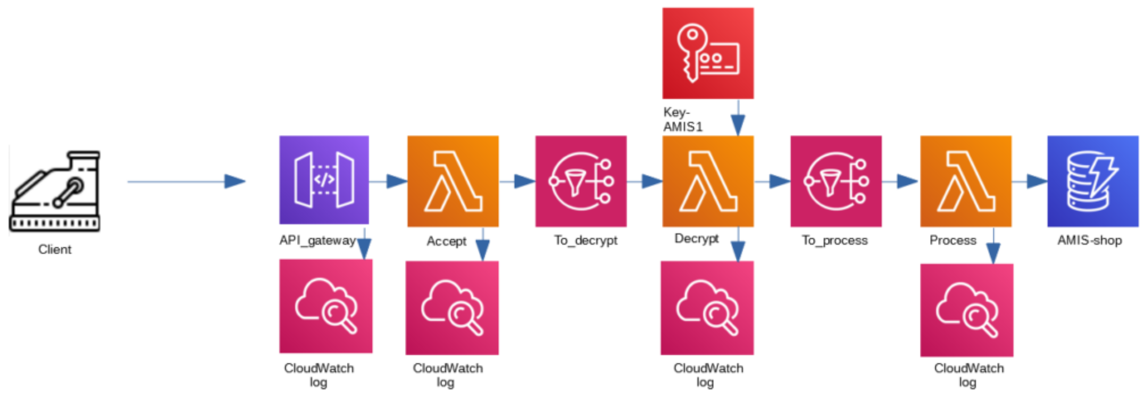
AWS Cloud

AWS Shop example: API Gateway (2)

Frederique Retsema *May 13, 2020*

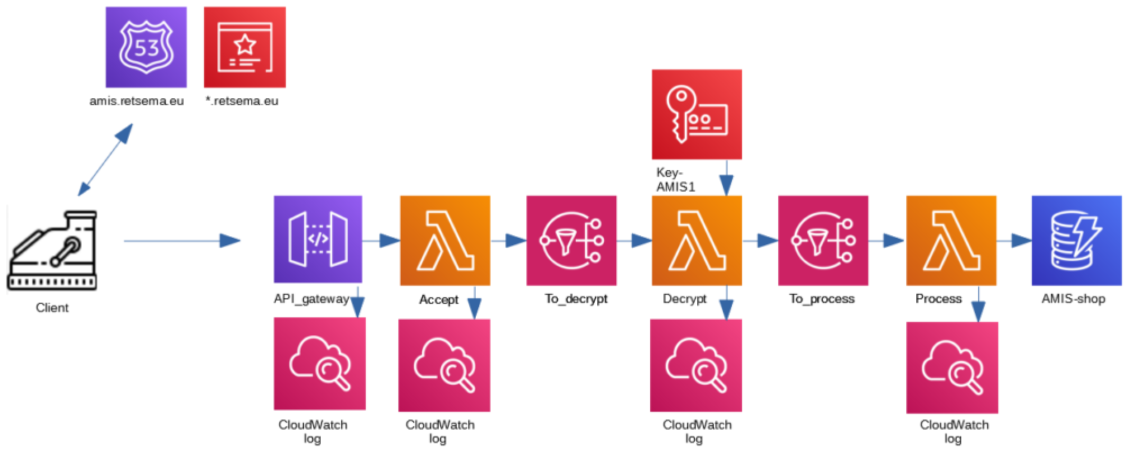
Introduction

Last time, I talked about the API Gateway [1]. The URL that we used last time has randomness in it: it looks like https://54dwcigu3a.execute-api.eu-west-1.amazonaws.com/prod/shop. When you destroy the API Gateway objects and redeploy them, you will get another URL. That's not nice: we don't want to change the URL in all our cashing machines when we deploy a new version of our software… The objects we used in the last blog are shown in the next image:



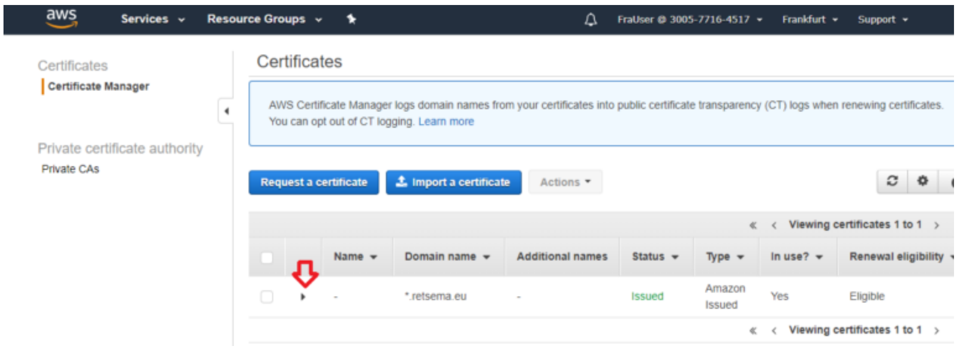
Today, I will use the domain retsema.eu (which is running in Route53, the DNS of AWS) to show you what you need to configure to get the nicely formed url (like https://amis.retsema.eu/shop). When I really would own a shop, I would most probably call it something like https://api.retsema.eu/shop. But well, in this example I added AMIS as a prefix for everything, so I will use it for my URL as well.

Here's the image that shows the objects that we will look at today:



Certificate

First, we need to have a certificate for our domain. Go to the certificate manager service, and click on the arrow next to the checkbox of the certificate.

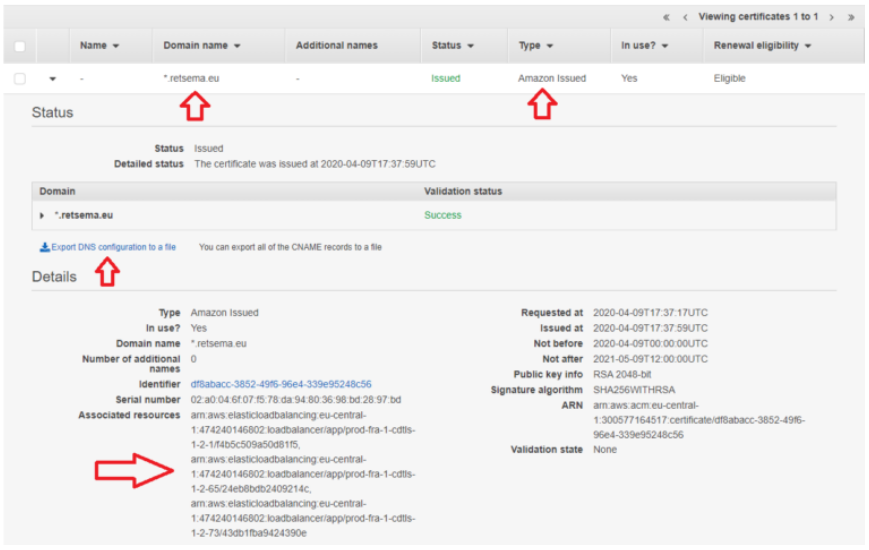


Certificates

AWS Certificate Manager logs domain names from your certificates into public certificate transparency (CT) logs when renewing certificates. You can opt out of CT logging. Learn more

Name	Domain name	Additional names	Status	Type	In use?	Renewal eligibility
-	*.retsema.eu	-	Issued	Amazon Issued	Yes	Eligible

You can now see the details of the certificate:


Viewing certificates 1 to 1
Export DNS configuration to a file

Name	Domain name	Additional names	Status	Type	In use?	Renewal eligibility
-	*.retsema.eu	-	Issued	Amazon Issued	Yes	Eligible

Status

Status Issued
Detailed status The certificate was issued at 2020-04-09T17:37:59UTC

Domain	Validation status
*.retsema.eu	Success

You can export all of the CNAME records to a file

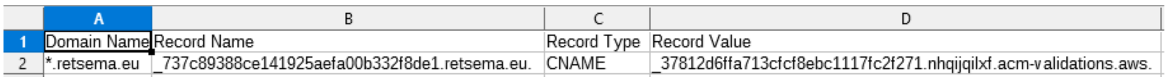
Details

Type	Amazon Issued
In use?	Yes
Domain name	*.retsema.eu
Number of additional names	0
Identifier	df8abacc-3852-49f6-96e4-339e95248c56
Serial number	02:a0:04:6f:07:f5:78:da:94:80:36:98:bd:28:97:bd
Associated resources	arn:aws:elasticloadbalancing:eu-central-1:474240146802:loadbalancer/app/prod-fra-1-cdtls-1-2-1/f4b5c509a50d81f5, arn:aws:elasticloadbalancing:eu-central-1:474240146802:loadbalancer/app/prod-fra-1-cdtls-1-2-65/24eb8bdb2409214c, arn:aws:elasticloadbalancing:eu-central-1:474240146802:loadbalancer/app/prod-fra-1-cdtls-1-2-73/43db1fba9424390e
Requested at	2020-04-09T17:37:17UTC
Issued at	2020-04-09T17:37:59UTC
Not before	2020-04-09T00:00:00UTC
Not after	2021-05-09T12:00:00UTC
Public key info	RSA 2048-bit
Signature algorithm	SHA256WITHRSA
ARN	arn:aws:acm:eu-central-1:300577164517:certificate/df8abacc-3852-49f6-96e4-339e95248c56
Validation state	None

The name of the certificate is *.retsema.eu, which means that I can use this certificate for any name that ends with retsema.eu. The certificate is issued by Amazon (I also could have uploaded a certificate that is issued by someone else).

When you request a certificate from Amazon, there are two ways that Amazon can verify that you really are the owner of the domain. The first way, is to verify by e-mail. The disadvantage is that this is slow: you are dependent on people to read the e-mail, press a link etc.

A much faster way, is to check via DNS. Amazon asks you to add an alias (CNAME) record to your domain, which will point to an AWS address. You can see how this works, by clicking on the "Export DNS configuration to a file" link.



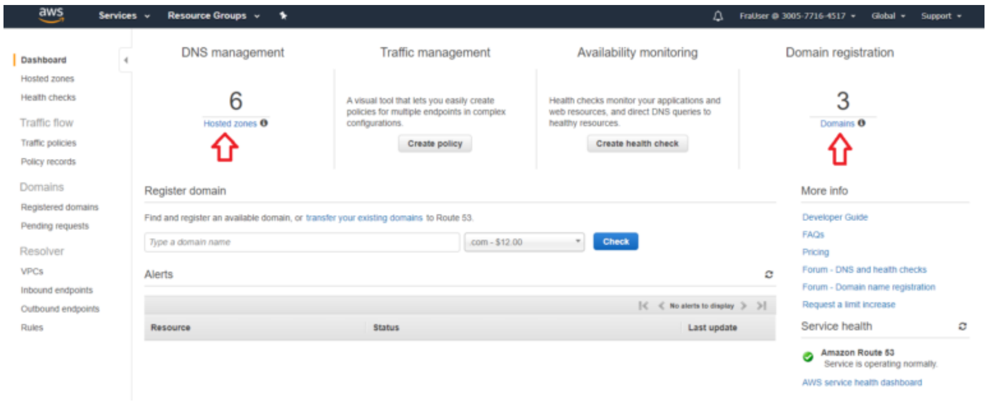
	A	B	C	D
1	Domain Name	Record Name	Record Type	Record Value
2	*.retsema.eu	_737c89388ce141925aefa00b332f8de1.retsema.eu.	CNAME	_37812d6ffa713cfcf8ebc1117fc2f271.nhqijqilxf.acm-validations.aws.

When you open the file, you can see that there has to be a record in the DNS with the name "_737c89388ce141925aefa00b332f8de1.retsema.eu." and that record has to point at "_37812d6ffa713cfcf8ebc1117fc2f271.nhqijqilxf.acm-validations.aws." When AWS verifies the domain (sometimes this is done within minutes, sometimes it takes more then two days), they will use the url _737c89388ce141925aefa00b332f8de1.retsema.eu. to check if they are routed to _37812d6ffa713cfcf8ebc1117fc2f271.nhqijqilxf.acm-validations.aws.

Before we go and look at Route53, I'd like to point to a nice detail in this screen. You see, that when the certificate is in use, this screen will show you where it is used ("Associated resources"). Though I never implemented a load balancer anywhere (see the architecture image), my certificate is used in three load balancers. It seems that the API Gateway uses multiple load balancers to do its job…

Route 53

Let's look at the CNAME record: go to the Route53 service. In the dashboard, you can see that I have three public domain names, and six hosted zones. That means that I use three private zones and three public zones.



DNS management: 6 Hosted zones

Traffic management: A visual tool that lets you easily create policies for multiple endpoints in complex configurations.

Availability monitoring: Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.

Domain registration: 3 Domains

Register domain

Find and register an available domain, or transfer your existing domains to Route 53.

Type a domain name | .com - $12.00

Alerts

No alerts to display

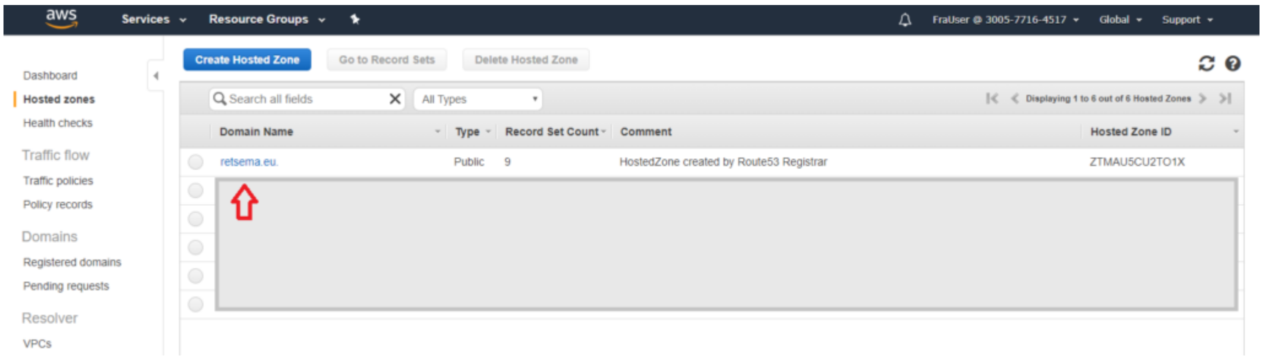
Resource	Status	Last update

More info

Service health

Amazon Route 53
Service is operating normally.

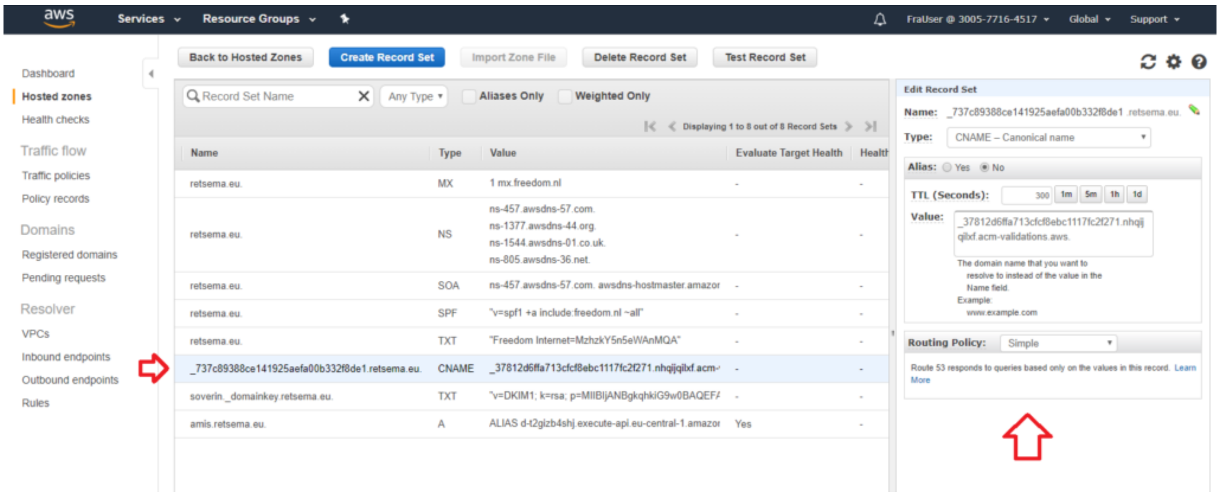
Click on the “Hosted zones” link, you will see the retsema.eu domain name in this list (normally you would see all six domain names here, I removed the other domain names from the image because they are not used in the shop example and some of them can be confusing). Click on the link with your domain name (in this case: retsema.eu):



Displaying 1 to 6 out of 6 Hosted Zones

Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
retsema.eu.	Public	9	HostedZone created by Route53 Registrar	ZTMAU5CU2TO1X

In this screen, you see all the DNS records for the retsema.eu domain. When you click on the CNAME record that we talked about, then the details are shown on the right part of the screen:



Displaying 1 to 8 out of 8 Record Sets

Name	Type	Value	Evaluate Target Health	Healtl
retsema.eu.	MX	1 mx.freedom.nl	-	-
retsema.eu.	NS	ns-457.awsdns-57.com. ns-1377.awsdns-44.org. ns-1544.awsdns-01.co.uk. ns-805.awsdns-36.net.	-	-
retsema.eu.	SOA	ns-457.awsdns-57.com. awsdns-hostmaster.amazor	-	-
retsema.eu.	SPF	"v=spf1 +a include:freedom.nl ~all"	-	-
retsema.eu.	TXT	"Freedom Internet=MzhzkY5n5eWAnMQA"	-	-
_737c89388ce141925aefa00b332f8de1.retsema.eu.	CNAME	_37812d6ffa713cfcf8ebc1117fc2f271.nhqijqilxf.acm-	-	-
soverin._domainkey.retsema.eu.	TXT	"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEF/	-	-
amis.retsema.eu.	A	ALIAS d-t2gizb4shj.execute-api.eu-central-1.amazor	Yes	-

Edit Record Set

Name: _737c89388ce141925aefa00b332f8de1 .retsema.eu.

Type: CNAME – Canonical name

Alias: Yes [✓ No]

TTL (Seconds): 300 1m 5m 1h 1d

Value: _37812d6ffa713cfcf8ebc1117fc2f271.nhqijqilxf.acm-validations.aws.

The domain name that you want to resolve to instead of the value in the Name field.
Example:
www.example.com

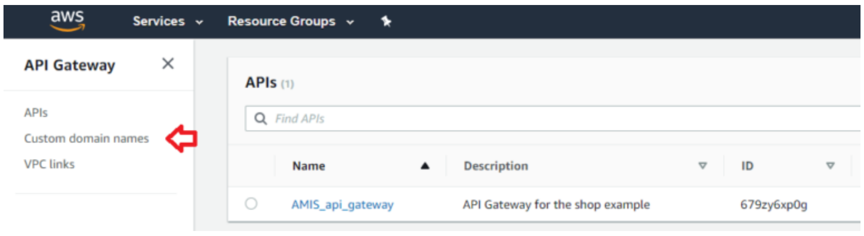
Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. Learn More

You can already see the amis.retsema.eu entry. But before we look into that, we have to change the configuration of the API Gateway.

API Gateway

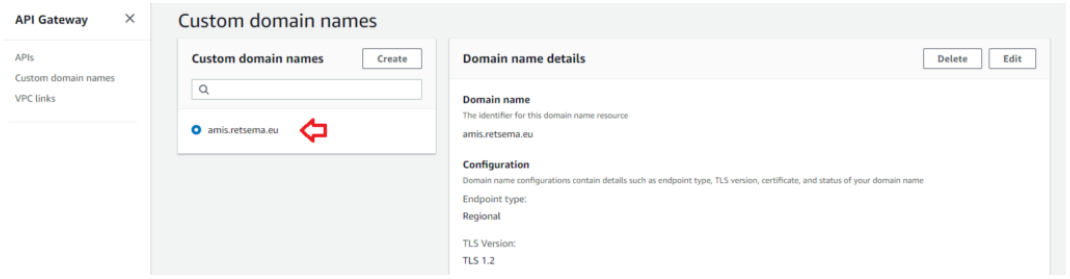
Go to the API Gateway, and choose Custom domain names in the left menu:



APIs (1)

Name	Description	ID
AMIS_api_gateway	API Gateway for the shop example	679zy6xp0g

Click on the domain name amis.retsema.eu:



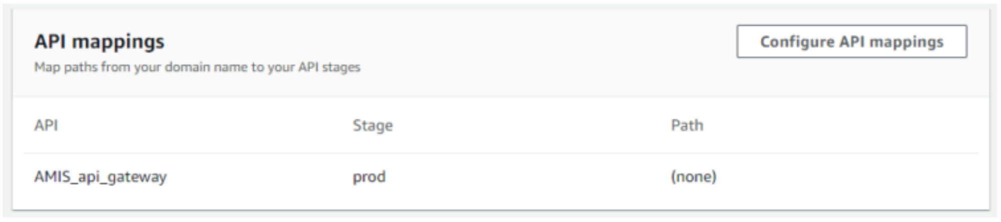
Domain name details

Domain name
The identifier for this domain name resource
amis.retsema.eu

Configuration
Domain name configurations contain details such as endpoint type, TLS version, certificate, and status of your domain name
Endpoint type:
Regional

TLS Version:
TLS 1.2

This might be confusing: we need to specify the full domain name (including the amis part) here, where only retsema.eu is a domain name. When you scroll down, you see API mappings:

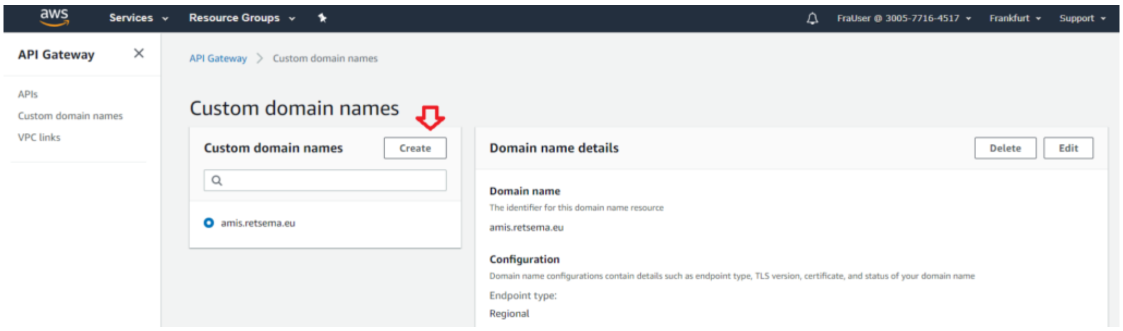


API mappings
Map paths from your domain name to your API stages

API	Stage	Path
AMIS_api_gateway	prod	(none)

You can see that amis.retsema.eu will use the prod stage, and that it will not have a path. This means that when 1we use amis.retsema.eu/shop, we always will use the prod stage and that we will have to specify the /shop resource when we use this URL.

It is possible to have multiple "nice URL's" to the same API Gateway. Let's try this out: let's make a new URL api.retsema.eu that points to the same API Gateway. Click on Create:

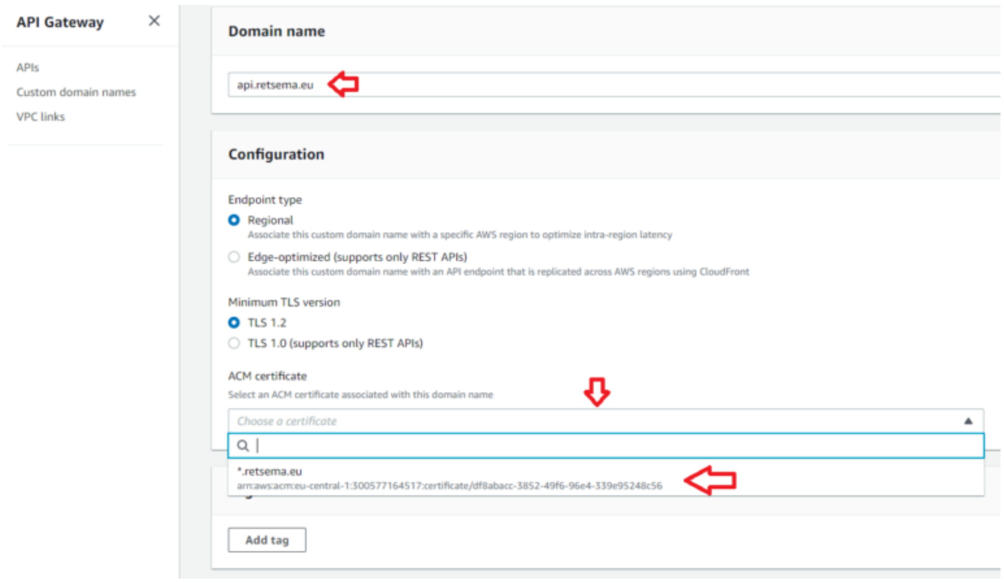


Domain name details

Domain name
The identifier for this domain name resource
amis.retsema.eu

Configuration
Domain name configurations contain details such as endpoint type, TLS version, certificate, and status of your domain name
Endpoint type:
Regional

Enter the name of the end point (in our case: api.retsema.eu) and add the certificate:



Domain name
api.retsema.eu

Configuration

Endpoint type
● Regional
Associate this custom domain name with a specific AWS region to optimize intra-region latency
○ Edge-optimized (supports only REST APIs)
Associate this custom domain name with an API endpoint that is replicated across AWS regions using CloudFront

Minimum TLS version
● TLS 1.2
○ TLS 1.0 (supports only REST APIs)

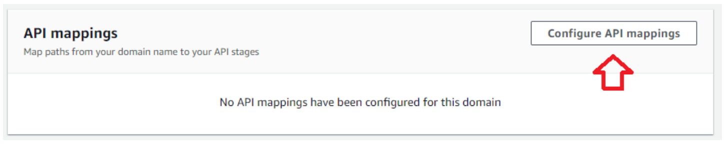
ACM certificate
Select an ACM certificate associated with this domain name
Choose a certificate
*.retsema.eu
arn:aws:acm:eu-central-1:300577164517:certificate/df8abacc-3852-49f6-96e4-339e95248c56

You also see the option to create a regional endpoint or an edge-optimized endpoint. A regional endpoint assumes that the people who use this URL will be in the neighborhood of the AWS region that this solution is deployed in (in my case: Frankfurt, AWS region eu-central-1).

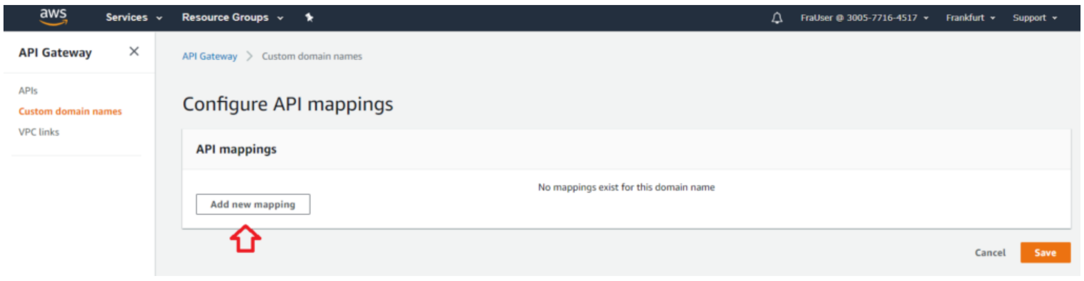
When you would use an API Gateway to provide information (REST GET requests) and your company is a global company, then you could use the edge locations of AWS. These edge locations are in the neighborhood of your clients, and will cache the results of the API calls. This will speed up the process. In our case, Regional is good.

Now, scroll to the bottom of the screen and press save.

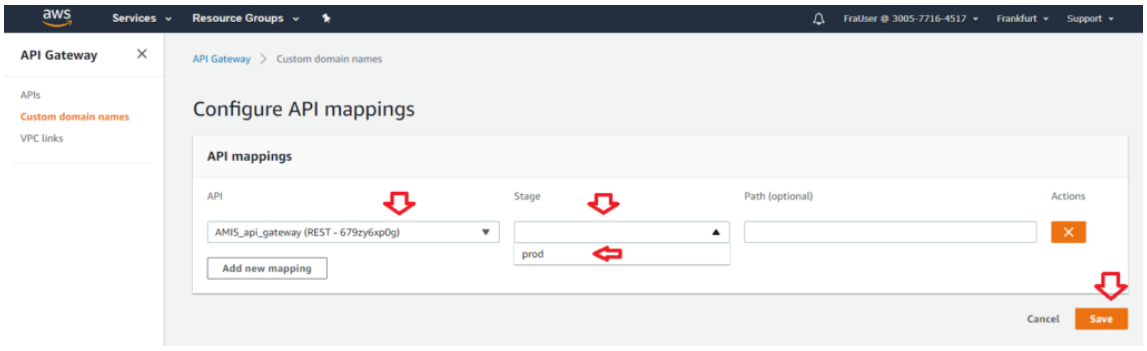
We have to do one more thing: scroll down, and look at the API mappings: they are empty now. Press on Configure API mappings:


API mappings
Map paths from your domain name to your API stages
Configure API mappings
No API mappings have been configured for this domain

In this screen, click on Add new mapping:

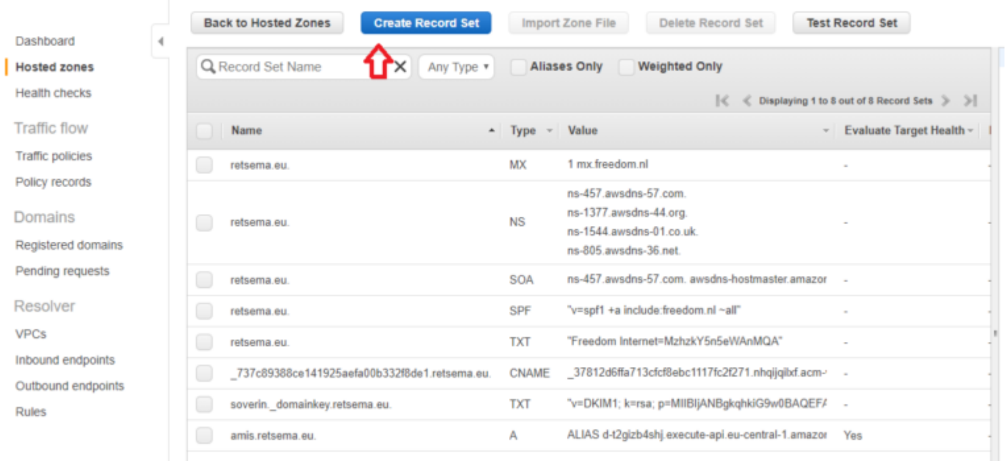


Click on the drop down windows for API and Stage, and choose the AMIS_api_gateway for API and prod for Stage. Leave the path empty. After that, press Save.



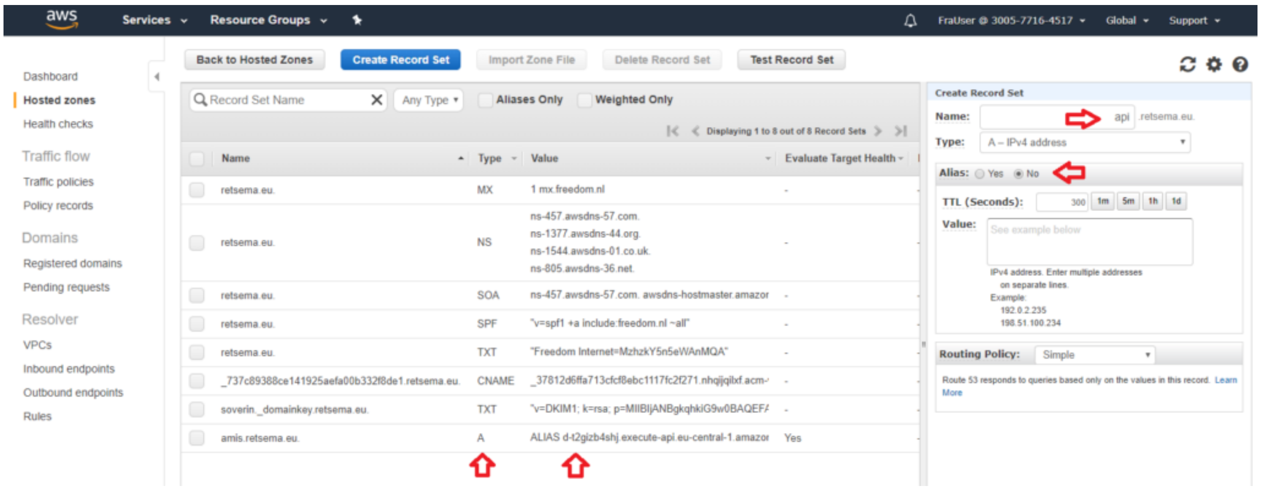
Route53

Now we have configured api.retsema.eu in the API gateway, we can configure the DNS entry: go back to the Route53 screen, and click on Create record set:



Name	Type	Value	Evaluate Target Health
retsema.eu.	MX	1 mx.freedom.nl	-
retsema.eu.	NS	ns-457.awsdns-57.com. ns-1377.awsdns-44.org. ns-1544.awsdns-01.co.uk. ns-805.awsdns-36.net.	-
retsema.eu.	SOA	ns-457.awsdns-57.com. awsdns-hostmaster.amazor	-
retsema.eu.	SPF	"v=spf1 +a include:freedom.nl ~all"	-
retsema.eu.	TXT	"Freedom Internet=MzhzkY5n5eWAnMQA"	-
_737c89388ce141925aefa00b332f8de1.retsema.eu.	CNAME	_37812d6ffa713cfcf8ebc1117fc2f271.nhqijqilxf.acm-	-
soverin._domainkey.retsema.eu.	TXT	"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEF/	-
amis.retsema.eu.	A	ALIAS d-t2gizb4shj.execute-api.eu-central-1.amazor	Yes

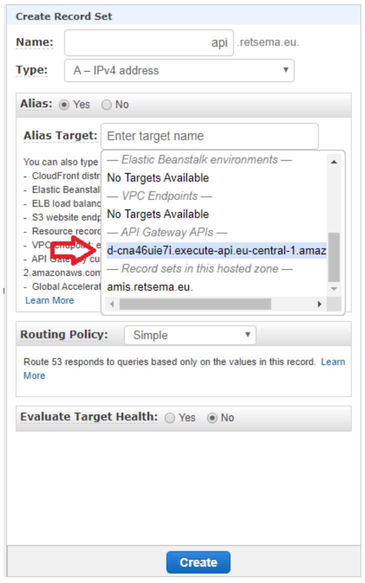
You might get confused here. We will need to create an A record. An A record in the DNS points to an IP address. But in the main screen, you see that amis.retsema.eu has an A record that points to an AWS address. That magic is done by clicking on the “Yes” radio button from the Alias:



Name	Type	Value	Evaluate Target Health
retsema.eu.	MX	1 mx.freedom.nl	-
retsema.eu.	NS	ns-457.awsdns-57.com. ns-1377.awsdns-44.org. ns-1544.awsdns-01.co.uk. ns-805.awsdns-36.net.	-
retsema.eu.	SOA	ns-457.awsdns-57.com. awsdns-hostmaster.amazor	-
retsema.eu.	SPF	"v=spf1 +a include:freedom.nl ~all"	-
retsema.eu.	TXT	"Freedom Internet=MzhzkY5n5eWAnMQA"	-
_737c89388ce141925aefa00b332f8de1.retsema.eu.	CNAME	_37812d6ffa713cfcf8ebc1117fc2f271.nhqjjqilxf.acm-	-
soverin._domainkey.retsema.eu.	TXT	"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEF/	-
amis.retsema.eu.	A	ALIAS d-t2gizb4shj.execute-api.eu-central-1.amazor	Yes

Create Record Set
Name: api .retsema.eu.
Type: A – IPv4 address
Alias: Yes [✓ No]
TTL (Seconds): 300 1m 5m 1h 1d
Value: See example below
IPv4 address. Enter multiple addresses on separate lines.
Example:
192.0.2.235
198.51.100.234
Routing Policy: Simple
Route 53 responds to queries based only on the values in this record. Learn More

You now can choose the Alias Target. When you scroll down, you see the API Gateway API. Choose it:

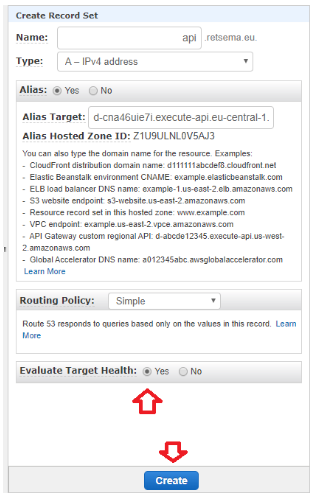


Create Record Set
Name: api .retsema.eu.
Type: A – IPv4 address
Alias: [✓ Yes] No
Alias Target: Enter target name
You can also type
- CloudFront distr
- Elastic Beanstal
- ELB load balanc
- S3 website endp
- Resource record
- VPC endpoint: e
- API Gateway cu
2.amazonaws.com
- Global Accelerat
Learn More

— Elastic Beanstalk environments —
No Targets Available
— VPC Endpoints —
No Targets Available
— API Gateway APIs —
d-cna46uie7i.execute-api.eu-central-1.amaz
— Record sets in this hosted zone —
amis.retsema.eu.

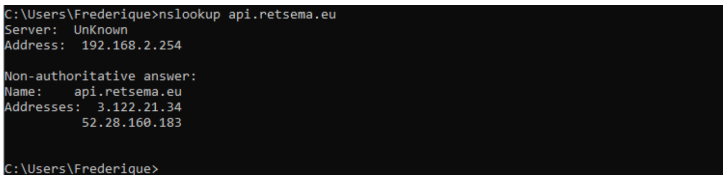
Routing Policy: Simple
Route 53 responds to queries based only on the values in this record. Learn More
Evaluate Target Health: Yes [✓ No]
Create

You can select Evaluate yes for Target Health: in that way, AWS will check regularly if the target (the load balancers of the API Gateway) are present and only point to healthy load balancers. After that, click Create:



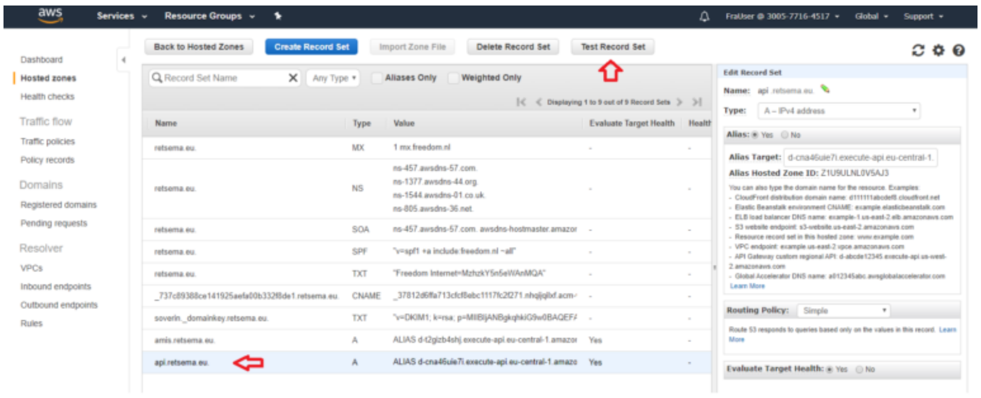
Create Record Set
Name: api .retsema.eu.
Type: A – IPv4 address
Alias: [✓ Yes] No
Alias Target: d-cna46uie7i.execute-api.eu-central-1.
Alias Hosted Zone ID: Z1U9ULNL0V5AJ3
You can also type the domain name for the resource. Examples:
- CloudFront distribution domain name: d111111abcdef8.cloudfront.net
- Elastic Beanstalk environment CNAME: example.elasticbeanstalk.com
- ELB load balancer DNS name: example-1.us-east-2.elb.amazonaws.com
- S3 website endpoint: s3-website.us-east-2.amazonaws.com
- Resource record set in this hosted zone: www.example.com
- VPC endpoint: example.us-east-2.vpce.amazonaws.com
- API Gateway custom regional API: d-abcde12345.execute-api.us-west-2.amazonaws.com
- Global Accelerator DNS name: a012345abc.awsglobalaccelerator.com
Learn More
Routing Policy: Simple
Route 53 responds to queries based only on the values in this record. Learn More
Evaluate Target Health: [✓ Yes] No
Create

But wait… We are talking about an A record. A records point to IP adresses, they are not supposed to point to other services. Is api.retsema.eu really an A record? Let's wait a few minutes and then find out by checking the DNS:



```
C:\Users\Frederique>nslookup api.retsema.eu
Server:  UnKnown
Address:  192.168.2.254

Non-authoritative answer:
Name:    api.retsema.eu
Addresses:  3.122.21.34
          52.28.160.183

C:\Users\Frederique>
```

You see that it is indeed a normal A record, giving back only IP addresses. Route53 has put the IP addresses from the load balancers of the API Gateway in this DNS record. We could also check this from within AWS: click on the api.retsema.eu record, and then on Test record set:



Displaying 1 to 9 out of 9 Record Sets

Name	Type	Value	Evaluate Target Health	Health
retsema.eu.	MX	1 mx.freedom.nl	-	-
retsema.eu.	NS	ns-457.awsdns-57.com. ns-1377.awsdns-44.org. ns-1544.awsdns-01.co.uk. ns-805.awsdns-36.net.	-	-
retsema.eu.	SOA	ns-457.awsdns-57.com. awsdns-hostmaster.amazor	-	-
retsema.eu.	SPF	"v=spf1 +a include:freedom.nl ~all"	-	-
retsema.eu.	TXT	"Freedom Internet=MzhzkY5n5eWAnMQA"	-	-
_737c89388ce141925aefa00b332f8de1.retsema.eu.	CNAME	_37812d6ffa713cfcf8ebc1117fc2f271.nhqjjqlbf.acm-	-	-
soverin._domainkey.retsema.eu.	TXT	"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEF/	-	-
amis.retsema.eu.	A	ALIAS d-t2glzb4shj.execute-api.eu-central-1.amazor	Yes	-
api.retsema.eu.	A	ALIAS d-cna46uie7i.execute-api.eu-central-1.amazo	Yes	-

Edit Record Set

Name: api .retsema.eu.

Type: A – IPv4 address

Alias: [✓ Yes] No

Alias Target: d-cna46uie7i.execute-api.eu-central-1.

Alias Hosted Zone ID: Z1U9ULNL0V5AJ3

You can also type the domain name for the resource. Examples:
- CloudFront distribution domain name: d111111abcdef8.cloudfront.net
- Elastic Beanstalk environment CNAME: example.elasticbeanstalk.com
- ELB load balancer DNS name: example-1.us-east-2.elb.amazonaws.com
- S3 website endpoint: s3-website.us-east-2.amazonaws.com
- Resource record set in this hosted zone: www.example.com
- VPC endpoint: example.us-east-2.vpce.amazonaws.com
- API Gateway custom regional API: d-abcde12345.execute-api.us-west-2.amazonaws.com
- Global Accelerator DNS name: a012345abc.awsglobalaccelerator.com

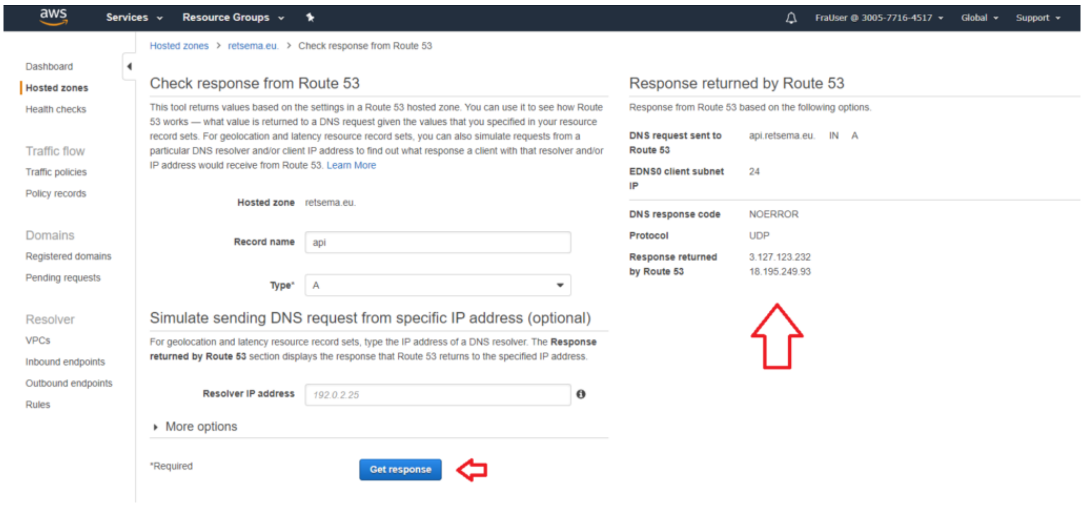
Learn More

Routing Policy: Simple

Route 53 responds to queries based only on the values in this record. Learn More

Evaluate Target Health: [✓ Yes] No

In the next screen, you can simulate to check from another location than you are now, by specifying an IP address to test from. In our case, this isn't necessary, so we will leave the Resolver IP address as it is and press the Get response button, you will see the response on the right part of the screen:



Check response from Route 53

This tool returns values based on the settings in a Route 53 hosted zone. You can use it to see how Route 53 works — what value is returned to a DNS request given the values that you specified in your resource record sets. For geolocation and latency resource record sets, you can also simulate requests from a particular DNS resolver and/or client IP address to find out what response a client with that resolver and/or IP address would receive from Route 53. Learn More

Hosted zone: retsema.eu.

Record name: api

Type*: A

Simulate sending DNS request from specific IP address (optional)

For geolocation and latency resource record sets, type the IP address of a DNS resolver. The **Response returned by Route 53** section displays the response that Route 53 returns to the specified IP address.

Resolver IP address: 192.0.2.25

*Required

Response returned by Route 53

Response from Route 53 based on the following options.

DNS request sent to Route 53: api.retsema.eu. IN A

EDNS0 client subnet IP: 24

DNS response code: NOERROR

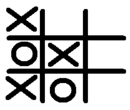
Protocol: UDP

Response returned by Route 53: 3.127.123.232, 18.195.249.93

And, because the proof of the pudding is in the eating, let's use our new api.retsema.eu record to send a message to the API gateway:

```
[vagrant@localhost client]$ ./encrypt_and_send.py AMIS1 https://api.retsema.eu/shop

Shop id = AMIS1

Key alias = alias/KeyL-AMIS1

URL = https://api.retsema.eu/shop

Data = {“shop_id”: “AMIS1”, “content_base64”:
“KW4JaTQy3R4kOvJsK669coHgPspVuTUwBve5v9D4m2OpsXWTx+u3adAR7OOi8CCEMA+Tits7PzjuBNQBwNZg0IynOyMW4LeEFrcaJh84+m8DOECmVuYLdmyHmpKzVOl4XkiQ

request_number = 1

Status code = 200

Content = b'”OK”‘

[vagrant@localhost client]$
```

Play along



I scripted the solution [2]. You can follow along and create this solution in your own environment, see the README.md file in the vagrant directory and see the introduction blog for more information. For this specific blog, you need your own domain. Replace retsema.eu by your own domain name. A domain name for .nl in AWS costs about $10 per year.

Links

[1] This is the fifth blog about this shop. Links to the previous blogs:

– Introduction: https://technology.amis.nl/2020/04/26/example-application-in-aws-using-lambda/

– Lambda and IAM: https://technology.amis.nl/2020/04/29/aws-shop-example-lambda/

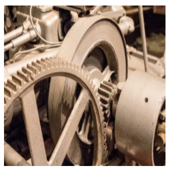
– SNS: https://technology.amis.nl/2020/05/02/aws-shop-about-the-aws-simple-notification-service-sns/

– DynamoDB: https://technology.amis.nl/2020/05/05/aws-shop-dynamodb-the-aws-nosql-database/

– API Gateway (1): https://technology.amis.nl/2020/05/09/aws-shop-api-gateway-1/

[2] https://github.com/FrederiqueRetsema/AMIS-Blog-AWS , directory shop-1

Related Posts:

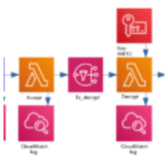

Differences between

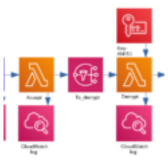
aws

Creating policy's, groups

aws

Policies in AWS (2)


AWS Shop: about the AWS


AWS Shop: DynamoDB, the

Leave a Reply

Enter your comment here...

This site uses Akismet to reduce spam. Learn how your comment data is processed.

Next Post ›

Databases DBA Oracle Oracle Cloud

A Quick how-to RMAN backup to OCI Object Storage

Wed May 13 , 2020

Facebook 0 Twitter Linkedin This is a quick how-to article on setting up RMAN to backup to Object Storage on OCI. This is applicable when you build your on Oracle database on an OCI instance, or when you have a database on-premise you wish to backup to the (OCI) cloud. [...]

ORACLE® Cloud Infrastructure

You May Like

APEX Cloud Database