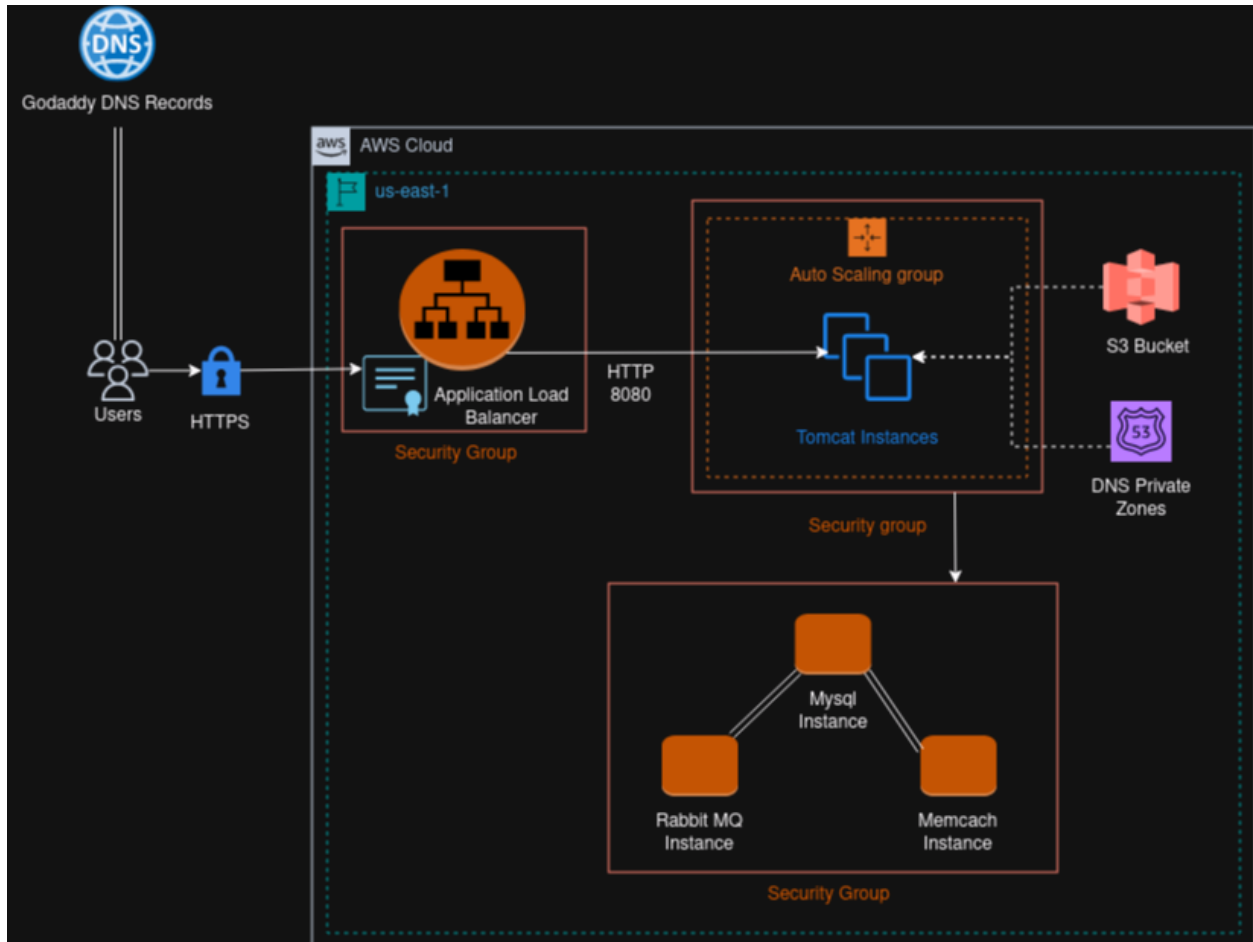


Lift & Shift from local to cloud

project overview



1) create security groups

Load Balancer SG:

allow all http/https traffic from anywhere

Inbound rules Info				
Type Info	Protocol Info	Port range Info	Source Info	
HTTP	TCP	80	Anywhere-...	0.0.0.0/0 X
HTTP	TCP	80	Anywhere-...	::/0 X
HTTPS	TCP	443	Anywhere-...	0.0.0.0/0 X
HTTPS	TCP	443	Anywhere-...	::/0 X

Tomcat SG:

allow traffic from elb sg on 8080

allow ssh from myip

allow 8080 access from my ip (for troubleshooting, to access the web app without the ELB)

Inbound rules Info				
Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info
sgr-09dc83014b651e095	SSH	TCP	22	Custom 87.89.70.237/32 X
sgr-0307a05ff5217b5c	Custom TCP	TCP	8080	Custom sg-0330b5334332dac51 X
sgr-0dec6f2b3928fa8a3	Custom TCP	TCP	8080	Custom 87.89.70.237/32 X

Backend services SG (allow only tomcat SG):

allow mysql 3306

allow Memcach 11211

allow rabbitMQ 5672

allow all traffic to its own SG (services can communicate with eachother)

allow ssh from my ip

Inbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info
sgr-001e06a7e52d553b	SSH	TCP	22	Custom 87.89.70.237/32
sgr-0e06e5ce74f06ed09	Custom TCP	TCP	5672	Custom sg-02fd0647b407b503b
sgr-0aace0ca8861199b2	Custom TCP	TCP	11211	Custom sg-02fd0647b407b503b
sgr-00a45aa088e9d53a3	MYSQL/Aurora	TCP	3306	Custom sg-02fd0647b407b503b
-	All traffic	All	All	Custom sg-0b6d3892149efa6ef sg-0b6d3892149efa6ef

2) create the ssh Key (one for all instances)

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

vprofile-keypair

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

Key pair type [Info](#)

☒ RSA

☐ ED25519

Private key file format

☒ .pem

For use with OpenSSH

☐ .ppk

For use with PuTTY

Tags - optional

Key

Q project

Value - optional

Q vprofile

Remove

3) start instances

create vprofile-db01 instance:

os: almalinux 9

set the key and the sg

copy the mysql script in the provisioning section

create vprofile-mc01

copy the memcach script

create vprofile-rmq01

copy the rapidmq script

create vprofile-app01 (tomcat)

os: ubuntu

set the key and sg

copy the toomcat script

search how to retrieve user data

login to tomcat and check if it is running

```
● tomcat9.service - Apache Tomcat 9 Web Application Server
   Loaded: loaded (/lib/systemd/system/tomcat9.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-01-17 21:43:42 UTC; 4min 59s ago
     Docs: https://tomcat.apache.org/tomcat-9.0-doc/index.html
   Process: 11442 ExecStartPre=/usr/libexec/tomcat9/tomcat-update-policy.sh (code=exited, status=0/SUCCESS)
  Main PID: 11446 (java)
    Tasks: 28 (limit: 1121)
   Memory: 87.8M
      CPU: 8.200s
   CGroup: /system.slice/tomcat9.service
           └─11446 /usr/lib/jvm/java-11-openjdk-amd64/bin/java -Djava.util.logging.config.file=/var/lib/tomcat
```

login to account database

mysql -u admin -padmin123 accounts

show tables

```
MariaDB [accounts]> show tables;
+-----+
| Tables_in_accounts |
+-----+
| role                |
| user                |
| user_role           |
+-----+
3 rows in set (0.000 sec)

MariaDB [accounts]> 
```

login to memcash instance

`ss -tunlp | grep 11211`

```
[ec2-user@ip-172-31-30-60 ~]$ ss -tunlp | grep 11211
tcp    LISTEN 0      1024      0.0.0.0:11211  0.0.0.0:*
tcp    LISTEN 0      1024      :::11211    :::*
[ec2-user@ip-172-31-30-60 ~]$ 
```

login to rabbitmq

check the service status

```
[ec2-user@ip-172-31-26-209 ~]$ systemctl status rabbitmq-server
● rabbitmq-server.service - RabbitMQ broker
   Loaded: loaded (/usr/lib/systemd/system/rabbitmq-server.service; enabled; preset: disabled)
   Active: active (running) since Wed 2024-01-17 21:36:14 UTC; 21min ago
     Main PID: 21100 (beam.smp)
        Tasks: 21 (limit: 5736)
      Memory: 85.8M
         CPU: 11.003s
       CGroup: /system.slice/rabbitmq-server.service
```

Instances (4) Info									Connect	
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>										
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone			
<input type="checkbox"/>	vprofile-app	i-0605316f3f7df14ed	Running	t2.micro	2/2 checks passed	View alarms	us-east-1c			
<input type="checkbox"/>	vprofile-db	i-0543d0b14c4410363	Running	t2.micro	2/2 checks passed	View alarms	us-east-1c			
<input type="checkbox"/>	vprofile-mc	i-090a9e6ec76fe2646	Running	t2.micro	2/2 checks passed	View alarms	us-east-1c			
<input type="checkbox"/>	vprofile-rmq	i-0c3e6a17c1d0f4d16	Running	t2.micro	2/2 checks passed	View alarms	us-east-1c			

4) set up DNS Records with Route 53

1- create a hosted zone:

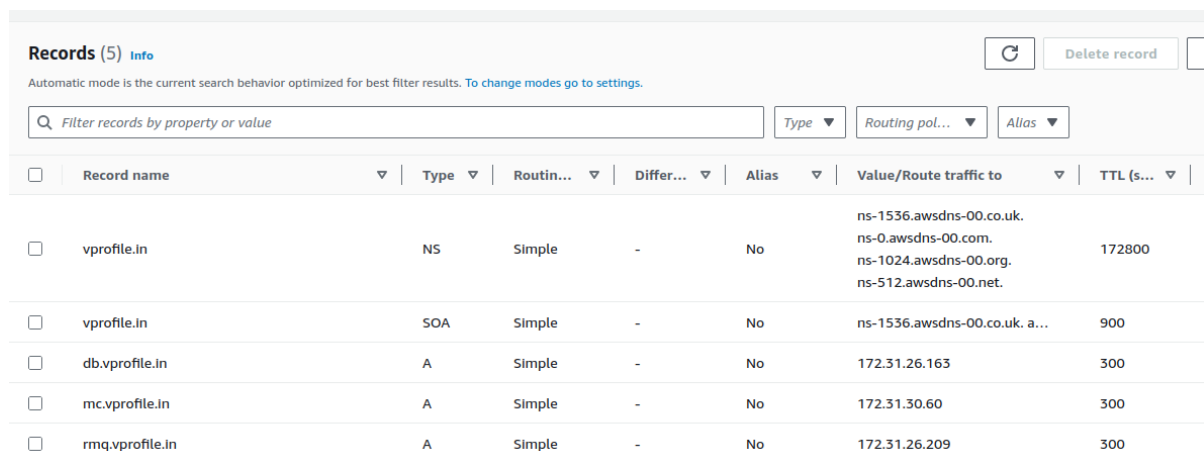
name: vprofile.in

make it private (only accessed from the its subnet / VPC) (records can be resolved only inside

the VPC)

2- create records inside the zone, chose simple routing

for each instance create a record with the name of the instance name.vprofile.in that resolves to its private ip



The screenshot shows the AWS Route 53 console interface for a hosted zone named 'vprofile.in'. At the top, there's a header 'Records (5) Info' with a refresh button and a 'Delete record' button. Below this is a search bar with the placeholder 'Filter records by property or value' and three dropdown menus for 'Type', 'Routing pol...', and 'Alias'. The main part of the image is a table listing five DNS records. The first record is of type 'NS' (Name Server) with a 'Simple' routing policy, pointing to four AWS managed NS records (ns-1536.awsdns-00.co.uk, ns-0.awsdns-00.com, ns-1024.awsdns-00.org, ns-512.awsdns-00.net) with a TTL of 172800. The other four records are of type 'A' (Address) with a 'Simple' routing policy, pointing to specific private IP addresses (172.31.26.163, 172.31.30.60, 172.31.26.209) with a TTL of 300. Each record has a checkbox on the left for selection.

<input type="checkbox"/>	Record name	Type	Routin...	Differ...	Alias	Value/Route traffic to	TTL (s...)
<input type="checkbox"/>	vprofile.in	NS	Simple	-	No	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	172800
<input type="checkbox"/>	vprofile.in	SOA	Simple	-	No	ns-1536.awsdns-00.co.uk. a...	900
<input type="checkbox"/>	db.vprofile.in	A	Simple	-	No	172.31.26.163	300
<input type="checkbox"/>	mc.vprofile.in	A	Simple	-	No	172.31.30.60	300
<input type="checkbox"/>	rmq.vprofile.in	A	Simple	-	No	172.31.26.209	300

5) create the artifact

build the artifact:

go to src/main/ressources/application.properties, and replace the host names with name.vprofile.in

run "mvn install" to build the artifact

create S3 IAM User:

username: s3admin

give it the policy: amazones3fullaccess

create an access key for the CLI

Retrieve access keys [Info](#)

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIARIWCMYSZ2ZX6NG4V	***** Show

Access key best practices

go to terminal and configure the cli with the downloaded creds "aws configure"
past the key id, and the secret, region: us-east-1, format: json

```
riad@power:~/devops/aws/lift-shift/vprofile-project$ aws configure
AWS Access Key ID [*****LW4W]: AKIARIWCMYSZ2ZX6NG4V
AWS Secret Access Key [*****lgtk]: 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
Default region name [us-east-1]: us-east-1
Default output format [json]: json
```

create s3 bucket from aws:

```
aws s3 mb s3://bucket_name
```

copy the artifact to the aws bucket

```
aws s3 cp target/vprofile-v2.war s3://bucket_name
```

<input type="checkbox"/>	Name	Type	Last modified
<input type="checkbox"/>	vprofile-v2.war	war	January 17, 2024, 23:3 (UTC+01:00)

6) get the artifact to the tomcat instance:

create a role to connect to the s3 bucket from the ec2 instance without
configuring the aws cli

```
aws service, ec2
```

```
policy: amzones3fullaccess
```

```
name: vprofile-s3
```

vprofile-s3-admin-role [Info](#) Delete

allow access to vprofile s3 bucket

Summary Edit

Creation date January 17, 2024, 23:40 (UTC+01:00)	ARN arn:aws:iam::087380772019:role/vprofile-s3-admin-role	Instance profile ARN arn:aws:iam::087380772019:instance-profile/vprofile-s3-admin-role
Last activity -	Maximum session duration 1 hour	

Permissions | Trust relationships | Tags | Access Advisor | Revoke sessions

Permissions policies (1) [Info](#) Refresh Simulate Remove Add permissions

You can attach up to 10 managed policies.

Search Filter by Type All types < 1 > Refresh

<input type="checkbox"/>	Policy name Info	Type	Attached entities
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	?

go to the instance actions, security, modify role and set the role

connect to the instance:

```
apt install awscli -y
```

```
aws s3 ls
```

```
aws s3 cp s3://bucketname/vprofile-v2.war /tmp/
```

replace the artifact:

```
systemctl stop tomcat9
rm -rf /var/lib/tomcat9/webapps/ROOT
cp /tmp/vprofile-v2.war /var/lib/tomcat9/webapps/ROOT.war
systemctl start tomcat9
ls /var/lib/tomcat9/webapps
# should see ROOT and ROOT.war
cat /var/lib/tomcat9/webapps/ROOT/WEB-INF/classes/application.p
# check if th
```

7) TG & ELB & DNS

create a target group for tomcat instance.

port 8080, health check override with 8080

Details					
arn:aws:elasticloadbalancing:us-east-1:087380772019:targetgroup/vprofile-app-tg/9bc098d07e6dcb63					
Target type	Protocol : Port		Protocol version		VPC
Instance	HTTP: 8080		HTTP1		vpc-0b50bf8cac6eaf8e1
IP address type	Load balancer				
IPv4	None associated				
0	0	0	0	0	0
Total targets	Healthy	Unhealthy	Unused	Initial	Draining
	0 Anomalous				

create the application load balancer

set http and https to the target group

select the certificat (ACM) in the security settings

▼ Details

Load balancer type

Application

Scheme

Internet-facing

Status

⌵ Provisioning

Hosted zone

Z355XD0TRQ7X7K

VPC

[vpc-0b50bf8cac6eaf8e1](#)

Availability Zones

[subnet-094fb95a6c6683766](#) us-east-1b (use1-az2)
[subnet-0e57cc1dcb8346589](#) us-east-1c (use1-az4)

IP address type

IPv4

Date created

January 18, 2024, 00:02 (UTC+01:00)

Load balancer ARN

arn:aws:elasticloadbalancing:us-east-1:087380772019:loadbalancer/app/vprofile-app-elb/04554cee46078151

DNS name

[Info](#)

vprofile-app-elb-1603699535.us-east-1.elb.amazonaws.com (A Record)

Listeners and rules

Network mapping

Security

Monitoring

Integrations

Attributes

Tags

Listeners and rules (2) [Info](#)

A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

🔍 Filter listeners

⌵

Protocol:Port

⌵

⌵

Default action

⌵

⌵

Rules

⌵

⌵

ARN

⌵

⌵

Security policy

⌵

⌵

Default SSL/TLS certificate

⌵

⌵

mTLS

⌵

⌵

[HTTP:443](#)

Forward to target group

[vprofile-app-tg](#) 1 (100%)

• Group-level stickiness: Off

[1 rule](#)

ARN

ELBSecurityPolicy-TLS13-1-2-...

[*.riadprojects.xyz \(Certificate I...](#)

Off

⌵

[HTTP:80](#)

Forward to target group

[vprofile-app-tg](#) 1 (100%)

• Group-level stickiness: Off

[1 rule](#)

ARN

Not applicable

Not applicable

Not applicable

create a CNAME DNS record in godaday domain: paste the ELB DNS name as a cname record (vproapp → dns name)

<input type="checkbox"/>	CNAME	vproapp	vprofile-app-elb-1603699535.us-east-1.elb.amazonaws.com.	1 heure
--------------------------	-------	---------	--	---------

8) autoscalling group for the APP:

create an AMI for the EC2 app machine.

create a template using the AMI (don't forget to give the s3 role to the template)

Launch template details

Launch template ID

lt-05a6f8eb04af55271

Launch template name

vprofile-app-template

Default version

1

Details

Versions

Template tags

Launch template version details

Version

1 (Default)

Description

-

Date created

2024-01-17T23:14:49.000Z

Instance details

Storage

Resource tags

Network interfaces

Advanced details

AMI ID

ami-049fb5a247dae9d

Instance type

t2.micro

Availability Zone

-

Security groups

-

Security group IDs

sg-02fd0647b407b503b

create the auto scalling group

Group details

Auto Scaling group name

vprofile-app-asg

Desired capacity

1

Desired capacity type

Units (number of instances)

Date created

Thu Jan 18 2024 00:22:22 GMT+0100 (Central European Standard Time)

Minimum capacity

1

Status

Updating capacity

Maximum capacity

3

configure the stickiness on the target group (requests from a user sticks two one instance)

Target selection configuration

Stickiness

On

Stickiness duration

4 days

Stickiness type

Load balancer generated cookie

Cross-zone load balancing

Inherit settings from load balancer attributes

know the moment of truth: let try navigating to <https://vproapp.riadprojects.xyz>
and voila: the website is live

