

Final Project Solution

Network

Network could be deployed as it was in course example project

```
slava@LAPTOP-LJS1DSMA ~  
$ aws s3 ls  
2020-03-22 16:49:50 cf-templates-1yjelzdl46bm-us-east-2  
2020-03-15 08:37:39 elasticbeanstalk-us-east-2-980543251014  
2020-03-21 19:53:40 udacity-website-123456
```

```
slava@LAPTOP-LJS1DSMA ~  
$ cd d:
```

```
slava@LAPTOP-LJS1DSMA /cygdrive/d  
$ cd YandexDisk/udacity_cloud_devops/Project_3_IAC/
```

```
slava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC  
$ ./create.sh Project2_IAC network.yml network-parameters.json
```

An error occurred (ValidationError) when calling the CreateStack operation: 1 validation error detected: Value 'Project2_IAC' at 'stackName' failed to satisfy constraint: Member must satisfy regular expression pattern: [a-zA-Z][-a-zA-Z0-9]*

```
slava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC  
$ ./create.sh Project2_IAC network.yml network-parameters.json
```

An error occurred (ValidationError) when calling the CreateStack operation: 1 validation error detected: Value 'Project2_IAC' at 'stackName' failed to satisfy constraint: Member must satisfy regular expression pattern: [a-zA-Z][-a-zA-Z0-9]*

```
slava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC  
$ ./create.sh UdacityProject2IAC network.yml network-parameters.json
```

An error occurred (ValidationError) when calling the CreateStack operation: Template format error: YAML not well-formed. (line 2, column 1)

```
slava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC  
$ ./create.sh UdacityProject2IAC network.yml network-parameters.json  
{  
  "stackId": "arn:aws:cloudformation:us-west-2:980543251014:stack/UdacityProject2IAC/96709ce0-  
8154-11ea-91d6-02e34c33f014"  
}
```

```
slava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC
```

The screenshot shows the AWS CloudFormation console interface. On the left, the 'Stacks' section is expanded, and 'UdacityProject2IAC' is selected. The main panel displays the 'UdacityProject2IAC' stack details, including the 'Events' tab. The events list shows the following details:

Timestamp	Logical ID	Status	Status reason
2020-04-18 12:13:18 UTC+0300	NatGateway2	CREATE_IN_PROGRESS	Resource creation Initiated
2020-04-18 12:13:17 UTC+0300	NatGateway2	CREATE_IN_PROGRESS	-
2020-04-18 12:13:17 UTC+0300	NatGateway1	CREATE_IN_PROGRESS	Resource creation Initiated
2020-04-18 12:13:17 UTC+0300	NatGateway1	CREATE_IN_PROGRESS	-
2020-04-18 12:13:16 UTC+0300	PublicSubnet2RouteTableAssociation	CREATE_COMPLETE	-
2020-04-18 12:13:16 UTC+0300	PrivateSubnet2RouteTableAssociation	CREATE_COMPLETE	-
2020-04-18 12:13:15 UTC+0300	PrivateSubnet1RouteTableAssociation	CREATE_COMPLETE	-
2020-04-18 12:13:15 UTC+0300	PublicSubnet1RouteTableAssociation	CREATE_COMPLETE	-
2020-04-18 12:13:15 UTC+0300	NatGateway1EIP	CREATE_COMPLETE	-
2020-04-18 12:13:15 UTC+0300	NatGateway2EIP	CREATE_COMPLETE	-

CloudFormation

Stacks

Stack details

Drifts

StackSets

Exports

Designer

CloudFormation registry

Resource types

Feedback

CloudFormation > Stacks > UdacityProject2IAC

Stacks (2)

Filter by stack name

Active View nested

UdacityProject2IAC

2020-04-18 12:12:19 UTC+0300

CREATE_COMPLETE

ourfirsttest

2020-03-23 14:24:34 UTC+0300

CREATE_COMPLETE

UdacityProject2IAC

Delete Update Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets

Outputs (10)

Search outputs

Key	Value	Description	Export name
PrivateSubnet1	subnet-0c5212e9a706ca695	A reference to the private subnet in the 1st Availability Zone	UdacityProject2IAC-PR1-SN
PrivateSubnet2	subnet-06e305bf0d309165e	A reference to the private subnet in the 2nd Availability Zone	UdacityProject2IAC-PR2-SN
PrivateSubnets	subnet-0c5212e9a706ca695,subnet-06e305bf0d309165e	A list of the private subnets	UdacityProject2IAC-PRIV-NETS
PublicSubnet1	subnet-0e933bc4fafe283ed	A reference to the public subnet in the 1st Availability Zone	UdacityProject2IAC-PUB1-SN
PublicSubnet2	subnet-0a9c022a31587e942	A reference to the public subnet in the 2nd Availability Zone	UdacityProject2IAC-PUB2-SN
PublicSubnets	subnet-0e933bc4fafe283ed,subnet-0a9c022a31587e942	A list of the public subnets	UdacityProject2IAC-PUB-NETS
VPC	vpc-0928cebd6f72d8b7e	A reference to the created VPC	UdacityProject2IAC-VPCID
VPCPrivateRouteTable1	rtb-01399d9f95a2caed6	Private Routing AZ1	UdacityProject2IAC-PR1-RT
VPCPrivateRouteTable2	rtb-0afe088cbe316d1	Private Routing AZ2	UdacityProject2IAC-PR2-RT
VPCPublicRouteTable	rtb-031e927cfce1b8e43	Public Routing	UdacityProject2IAC-PUB-RT

https://us-west-2.console.aws.amazon.com/cloudformation/home?region=us-west-2

© 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Create VPC Actions

Filter by tags and attributes or search by keyword

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR (Network Border Group)	DHCP options set	Main Route table	Main Network ACL	Tenancy	Default VPC
UdacityProj...	vpc-0928cebd6f72d8b7e	available	10.0.0.0/16	-	dopt-0c808899c4d2a6390	rtb-01f5a2962e44c0ce	acl-01f143e5c4bc2e04b	default	No
	vpc-00f8482c7c4af19bc	available	10.0.0.0/16	-	dopt-0c808899c4d2a6390	rtb-0a53b70da090edc64	acl-024077c0f76744cdc	default	No

VPC: vpc-0928cebd6f72d8b7e

Description CIDR Blocks Flow Logs Tags

VPC ID

State

IPv4 CIDR

IPv6 CIDR (Network Border Group)

DNS resolution

DNS hostnames

ClassicLink DNS Support

Owner

Tenancy

Default VPC

Classic link

IPv6 Pool

Network ACL

DHCP options set

Route table

aws

Services

Resource Groups

slava.lion25

Oregon

Support

VPC Dashboard

Filter by VPC:

Select a VPC

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

SECURITY

Network ACLs

Security Groups

VIRTUAL PRIVATE NETWORK (VPN)

Customer Gateways

Virtual Private Gateways

Site-to-Site VPN Connections

Client VPN Endpoints

TRANSIT GATEWAYS

Transit Gateways

Transit Gateway Attachments

Create subnet Actions

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Network Border Gro	Route table
UdacityProj...	subnet-06e305bf0d309165e	available	vpc-0928cebd6f72d8b7e	10.0.3.0/24	251	-	us-west-2b	usw2-az2	us-west-2	rtb-0afe088cbe6
UdacityProj...	subnet-0a9c022a31587e942	available	vpc-0928cebd6f72d8b7e	10.0.1.0/24	250	-	us-west-2b	usw2-az2	us-west-2	rtb-031e927cfce1
UdacityProj...	subnet-0c5212e9a706ca695	available	vpc-0928cebd6f72d8b7e	10.0.2.0/24	251	-	us-west-2a	usw2-az1	us-west-2	rtb-01399d9f95a2
UdacityProj...	subnet-0e933bc4fafe283ed	available	vpc-0928cebd6f72d8b7e	10.0.0.0/24	250	-	us-west-2a	usw2-az1	us-west-2	rtb-031e927cfce1
	subnet-1bb07d46	available	vpc-45caac3d	172.31.0.0/20	4091	-	us-west-2c	usw2-az3	us-west-2	rtb-d4efacaf
	subnet-767c8f0e	available	vpc-45caac3d	172.31.16.0/20	4091	-	us-west-2a	usw2-az1	us-west-2	rtb-d4efacaf
	subnet-d8001c93	available	vpc-45caac3d	172.31.32.0/20	4091	-	us-west-2b	usw2-az2	us-west-2	rtb-d4efacaf
	subnet-ed9f2ac6	available	vpc-45caac3d	172.31.48.0/20	4091	-	us-west-2d	usw2-az4	us-west-2	rtb-d4efacaf

Subnet: subnet-0e933bc4fafe283ed

Description Flow Logs Route Table Network ACL Tags Sharing

Edit route table association

Route Table: rtb-031e927cfce1b8e43 | UdacityProject2IAC Public Routes

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-0e34cd1571da6e79a

aws

Services

Resource Groups

slava.lion25

Oregon

Support

Servers

WebServerSecGroup

WebServerSecGroup change 8080 port to 80

WebAppLaunchConfig

Copy from starter code

```
Fn::Base64: !Sub |
    #!/bin/bash
    apt-get update -y
    apt-get install apache2 -y
    systemctl start apache2.service
    cd /var/www/html
    echo "Udacity Demo Web Server Up and Running!" > index.html
```

and choose ami with ubuntu 18 in us-west-2

The screenshot shows the AWS Management Console interface for selecting an Amazon Machine Image (AMI). The page is titled "Step 1: Choose an Amazon Machine Image (AMI)". A search bar at the top allows searching for an AMI by entering a search term like "Windows". Below the search bar, there is a "Quick Start" sidebar with options like "My AMIs", "AWS Marketplace", and "Community AMIs". The main content area displays a list of AMIs. The "Ubuntu Server 18.04 LTS (HVM), SSD Volume Type" is highlighted with a red box, showing its AMI ID: ami-0d1cd67c26f5fca19. Other AMIs listed include Amazon Linux 2, Amazon Linux 2018.03.0, Red Hat Enterprise Linux 8, and SUSE Linux Enterprise Server 15 SP1.

ImageId: ami-0d1cd67c26f5fca19

I will test with free t2.micro, but for the Server specs we need t2.medium with two vCPUs and at least 4GB of RAM

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 types Current generation Show/Hide Columns

Currently selected: t2.medium (Variable ECUs, 2 vCPUs, 2.3 GHz, Intel Broadwell E5-2686v4, 4 GiB memory, EBS only)								
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.micro	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

InstanceType: t2.medium

To be able access S3 bucket with static resources we should add IAM Role

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-as-launchconfig.html#cfn-as-launchconfig-iaminstanceprofile>

S3 Role


first we should create a role


<https://console.aws.amazon.com/iam/>


Create role


1 2 3 4

Select type of trusted entity

 **AWS service**
EC2, Lambda and others

 **Another AWS account**
Belonging to you or 3rd party

 **Web identity**
Cognito or any OpenID provider

 **SAML 2.0 federation**
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway	CodeDeploy	EMR	KMS	RoboMaker
AWS Backup	CodeGuru	ElastiCache	Kinesis	S3
AWS Chatbot	CodeStar Notifications	Elastic Beanstalk	Lambda	SMS
AWS Support	Comprehend	Elastic Container Service	Lex	SNS
Amplify	Config	Elastic Transcoder	License Manager	SWF
AppStream 2.0	Connect	ElasticLoadBalancing	Machine Learning	SageMaker
AppSync	DMS	Forecast	Macie	Security Hub
Application Auto Scaling	Data Lifecycle Manager	Global Accelerator	MediaConvert	Service Catalog

Create role

▼ Attach permissions policies

Choose one or more policies to attach to your new role.




Create policy

↺

Filter policies ▼

Q S3

Showing 5 results

	Policy name ▼	Used as
<input type="checkbox"/>	▶  AmazonDMSRedshiftS3Role	None
<input type="checkbox"/>	▶  AmazonS3FullAccess	None
<input checked="" type="checkbox"/>	▼  AmazonS3ReadOnlyAccess	None

AmazonS3ReadOnlyAccess

Provides read only access to all buckets via the AWS Management Console.

Policy summary

{ } JSON

1 {

2 "Version": "2012-10-17",

3 "Statement": [

▶ Set permissions boundary

Create role

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<div>name</div>	<div>EC2 Role with S3 read only rights</div>	✕
<div>Add new key</div>	<div></div>	

You can add 49 more tags.

Create role



Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+=, @-_' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+=, @-_' characters.

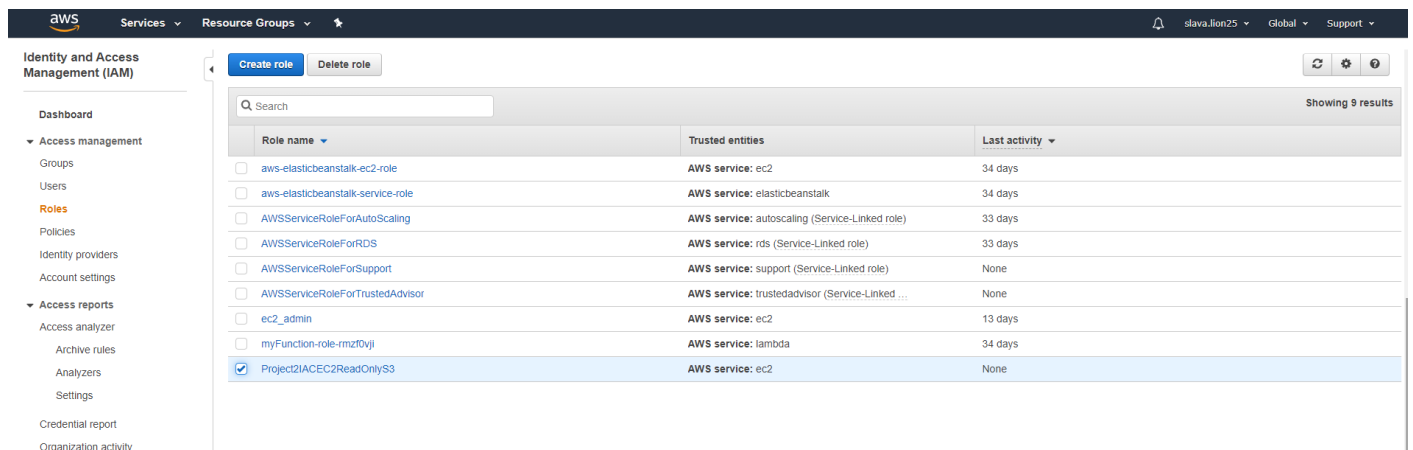
Trusted entities AWS service: ec2.amazonaws.com

Policies  AmazonS3ReadOnlyAccess 

Permissions boundary Permissions boundary is not set

The new role will receive the following tag

Key	Value
name	EC2 Role with S3 read only rights



The screenshot shows the AWS IAM console interface. On the left, there is a navigation menu with options like Dashboard, Access management, Groups, Users, Roles (highlighted), Policies, Identity providers, Account settings, Access reports, Access analyzer, Archive rules, Analyzers, Settings, Credential report, and Organization activity. The main area displays a table of roles. The table has columns for Role name, Trusted entities, and Last activity. The role 'Project2IACEC2ReadOnlyS3' is selected and highlighted in blue. Other roles listed include aws-elasticbeanstalk-ec2-role, aws-elasticbeanstalk-service-role, AWSServiceRoleForAutoScaling, AWSServiceRoleForRDS, AWSServiceRoleForSupport, AWSServiceRoleForTrustedAdvisor, ec2_admin, and myFunction-role-rmzt0vj.

So back to our WebAppLaunchConfig

We should create AWS::IAM::InstanceProfile

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-iam-instanceprofile.html>

adding

```
EC2UbuntuWithAccessToS3InstanceProfile:
  Type: AWS::IAM::InstanceProfile
  Properties:
    Roles:
      - Project2IACEC2ReadOnlyS3
```

To WebAppLaunchConfig adding

```
IamInstanceProfile:
  Ref: EC2UbuntuWithAccessToS3InstanceProfile
```

WebAppGroup

Set min and max size to 4

```
MinSize: '4'
MaxSize: '4'
```

WebAppTargetGroup

As we changed all ports to 80, we should also change it here

```
Port: 80
```

Outputs

As we need url to load balancer

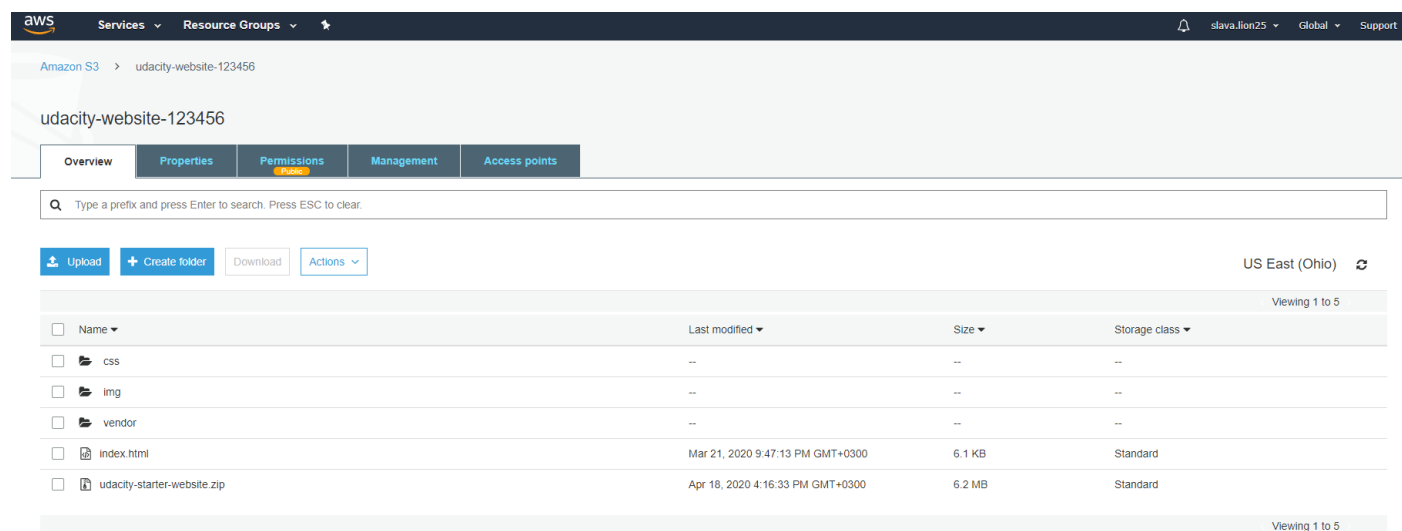
<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-elasticloadbalancingv2-loadbalancer.html>

Fn::GetAtt - DNSName

The DNS name for the load balancer. For example, my-load-balancer-424835706.us-west-2.elb.amazonaws.com.

S3 prepare

Upload static web site from the previous lesson to S3



The screenshot shows the AWS S3 console interface for a bucket named 'udacity-website-123456'. The 'Overview' tab is active, showing a list of objects. The objects are:

Name	Last modified	Size	Storage class
css	--	--	--
img	--	--	--
vendor	--	--	--
index.html	Mar 21, 2020 9:47:13 PM GMT+0300	6.1 KB	Standard
udacity-starter-website.zip	Apr 18, 2020 4:16:33 PM GMT+0300	6.2 MB	Standard

```
aws s3 cp s3://udacity-website-123456/udacity-starter-website.zip .
```

```
unzip -o udacity-starter-website.zip
```

Script launch

```
s1ava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC
$ ./create.sh UdacityProject2IAC servers.yml server-parameters.json

An error occurred (AlreadyExistsException) when calling the CreateStack operation: Stack
[UdacityProject2IAC] already exists

s1ava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC
$ ./update.sh UdacityProject2IAC servers.yml server-parameters.json

An error occurred (ValidationError) when calling the UpdateStack operation: Template format
error: YAML not well-formed. (line 2, column 1)

s1ava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC
$ ./update.sh UdacityProject2IAC servers.yml server-parameters.json

An error occurred (ValidationError) when calling the UpdateStack operation: Template format
error: YAML not well-formed. (line 2, column 1)

s1ava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC
$ ./update.sh UdacityProject2IAC servers.yml server-parameters.json

An error occurred (ValidationError) when calling the UpdateStack operation: Template format
error: YAML not well-formed. (line 7, column 1)

s1ava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC
$ ./update.sh UdacityProject2IAC servers.yml server-parameters.json

An error occurred (ValidationError) when calling the UpdateStack operation: Template format
error: YAML not well-formed. (line 8, column 1)

s1ava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC
$ ./update.sh UdacityProject2IAC servers.yml server-parameters.json
{
  "StackId": "arn:aws:cloudformation:us-west-2:980543251014:stack/UdacityProject2IAC/96709ce0-
8154-11ea-91d6-02e34c33f014"
}

s1ava@LAPTOP-LJS1DSMA /cygdrive/d/YandexDisk/udacity_cloud_devops/Project_3_IAC
$ ./update.sh UdacityProject2IAC network_and_servers.yml network-parameters.json
{
  "StackId": "arn:aws:cloudformation:us-west-2:980543251014:stack/UdacityProject2IAC/96709ce0-
8154-11ea-91d6-02e34c33f014"
}
```


CloudFormation > Stacks > UdacityProject2IAC

Stacks (1)

Filter by stack name

Active View nested

UdacityProject2IAC

2020-04-18 12:12:19 UTC+0300

UPDATE_COMPLETE

UdacityProject2IAC

Delete

Update

Stack actions

Create stack

Stack info

Events

Resources

Outputs

Parameters

Template

Change sets

Outputs (11)

Search outputs

Key	Value	Description	Export name
PrivateSubnet1	subnet-0c5212e9a706ca695	A reference to the private subnet in the 1st Availability Zone	UdacityProject2IAC-PR1-SN
PrivateSubnet2	subnet-06e305bf0d309165e	A reference to the private subnet in the 2nd Availability Zone	UdacityProject2IAC-PR2-SN
PrivateSubnets	subnet-0c5212e9a706ca695,subnet-06e305bf0d309165e	A list of the private subnets	UdacityProject2IAC-PRIV-NETS
PublicSubnet1	subnet-0e933bc4fae283ed	A reference to the public subnet in the 1st Availability Zone	UdacityProject2IAC-PUB1-SN
PublicSubnet2	subnet-0a9c022a31587e942	A reference to the public subnet in the 2nd Availability Zone	UdacityProject2IAC-PUB2-SN
PublicSubnets	subnet-0e933bc4fae283ed,subnet-0a9c022a31587e942	A list of the public subnets	UdacityProject2IAC-PUB-NETS
VPC	vpc-0928cebd6f72d8b7e	A reference to the created VPC	UdacityProject2IAC-VPCID
VPCPrivateRouteTable1	rtb-01399d9f95a2caed6	Private Routing AZ1	UdacityProject2IAC-PR1-RT
VPCPrivateRouteTable2	rtb-0afe088cbe6316d1	Private Routing AZ2	UdacityProject2IAC-PR2-RT
VPCPublicRouteTable	rtb-031e927cfe1b8e43	Public Routing	UdacityProject2IAC-PUB-RT
WebAppLB	http://Udaci-WebAp-6KOE5FC5ARW9-1982102900.us-west-2.elb.amazonaws.com	A reference to the created Load balancer	UdacityProject2IAC-WebAppLB-Url

<http://udaci-webap-6koesfc5arw9-1982102900.us-west-2.elb.amazonaws.com/index3.html>