

CAPACITACIÓN
usach



UNIVERSIDAD DE SANTIAGO DE CHILE

Servicios web de Amazon

Solución de Actividad Cloudformation

Marzo 2022

Table of Contents

Objetivos de la actividad:	3
References:	4
Actualiza el Stack de la solución:	4
Appendix:	8

Objetivos de la actividad:

Modificar la plantilla

Lab_Initial_CloudFormation_Module_General_ImmersionDay.json (Siga las instrucciones en la sección del apéndice para obtener la plantilla) con los siguientes objetivos:

Agregar parámetros de restricción (Parameter Constraint) :

- Vpccidr
 - La longitud mínima debe establecerse en 9
 - La longitud máxima debe establecerse en 18
 - El patrón permitido debe ser:
"(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})/(\d{1,2})"
 - Agregar una descripción de restricción
- Psharedacidr
 - La longitud mínima debe establecerse en 9
 - La longitud máxima debe establecerse en 18
 - El patrón permitido debe ser:
"(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})/(\d{1,2})"
 - Agregar una descripción de restricción
- Psharedbcidr
 - La longitud mínima debe establecerse en 9
 - La longitud máxima debe establecerse en 18
 - El patrón permitido debe ser:
"(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})/(\d{1,2})"
 - Agregar una descripción de restricción

Agregar restricción de política de eliminación:

- Cree una política de eliminación para que su depósito de S3 se conserve en el momento de la eliminación

Agregue la sección Salidas para mostrar el valor en la pestaña Salida:

- Vpc id
 - Crea una descripción de tu salida
 - Haga referencia a su VPC como el valor usando !Ref
- NATGWA
 - Crea una descripción de tu salida
 - Haga referencia a su puerta de enlace NAT A como el valor usando !Ref
- NATGWB
 - Crea una descripción de tu salida

- Haga referencia a su puerta de enlace NAT B como el valor usando !Ref
- App bucket URL
 - Crea una descripción de tu salida
 - Haga referencia a la URL de su depósito S3 como el valor usando !Ref

References:

Parameters:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html>

Intrinsic functions:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/intrinsic-function-reference.html>

Outputs and Export:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/outputs-section-structure.html>

Mappings:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/mappings-section-structure.html>

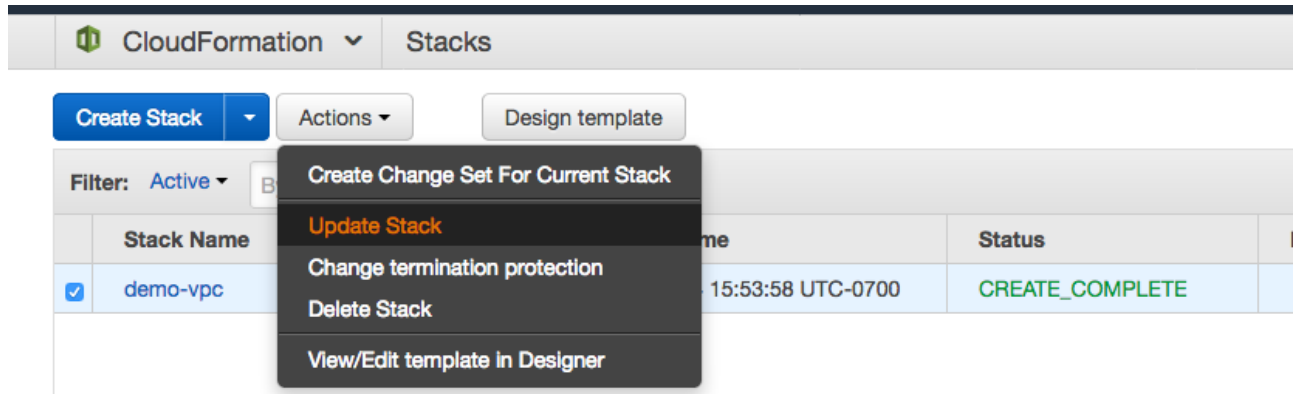
Deletion policy:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-attribute-deletionpolicy.html>

Actualiza el Stack de la solución:

Build VPC with AWS CloudFormation Lab

Una vez que modificó su plantilla existente, puede usar la opción Actualizar pila para actualizar su pila. Para actualizar, seleccione su pila y haga clic en el menú desplegable Acciones y encontrará la opción Actualizar pila.



En la pantalla Actualizar, Apilar, seleccione buscar su plantilla actualizada. Si aún no ha encontrado una solución, siga las instrucciones en la sección del apéndice para obtener la plantilla.

Lab_Solution_CloudFormation_Module_General_ImmersionDay.json.

Update demo-vpc stack

Select Template

Specify Details

Options

Review

Select Template

To update an existing stack, provide a template that specifies the changes for the resources and properties that you want to update. AWS CloudFormation updates only the resources that have changed. [Learn more.](#)

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

☐ Use current template

☒ Upload a template to Amazon S3

Lab_Solution_CloudFormation_Module_General_ImmersionDay.yaml

☐ Specify an Amazon S3 template URL

[Cancel](#)

[Next](#)

Build VPC with AWS CloudFormation Lab

Ahora los pasos restantes son los mismos que siguió en Crear pila. Haga clic en Siguiente par de veces y aterrizará en la pantalla de resumen de revisión, donde debe hacer clic en el botón Actualizar:

[Select Template](#)
[Specify Details](#)
[Options](#)
Review

Review

Review the information that AWS CloudFormation will use to update your stack. If you need to change a value, return to the page that contains the value that you want to change.

Template

Template URL https://s3-external-1.amazonaws.com/cf-templates-ta7yfdqq9l4-us-east-1/2018144zmU-Lab_Solution_CloudFormation_Module_General_ImmersionDay.yaml
Description

Details

Stack name:	demo-vpc
psharedacidr	10.20.0.0/22
psharedbcidr	10.20.4.0/22
vpccidr	10.20.0.0/16

Options

Tags
No tags provided

Rollback Triggers
No monitoring time provided
No rollback triggers provided

Advanced
Notification

Preview your changes

Based on your input, CloudFormation will change the following resources. For more information, choose [View change set details](#).

No values found

[Cancel](#) [Previous](#) [Update](#)

Ahora encontrará el estado de su pila cambiado a UPDATE_IN_PROGRESS y la pestaña Eventos que muestra la actividad realizada usando la pila de actualización.

Build VPC with AWS CloudFormation Lab

The screenshot shows the AWS CloudFormation console interface. At the top, there are buttons for 'Create Stack', 'Actions', and 'Design template'. Below these, a filter dropdown is set to 'Active' and a search box contains 'By Stack Name'. The main table lists one stack: 'demo-vpc', created on 2018-05-24 at 15:53:58 UTC-0700, with a status of 'UPDATE_IN_PROGRESS'. Below the table, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', 'Stack Policy', 'Change Sets', and 'Rollback Triggers'. The 'Events' tab is selected, showing a list of events for the stack 'demo-vpc' on 2018-05-24. The events include 'UPDATE_COMPLETE', 'UPDATE_COMPLETE_CLEANUP_IN_PROGRESS', 'UPDATE_COMPLETE', 'UPDATE_IN_PROGRESS', 'CREATE_COMPLETE', and 'CREATE_COMPLETE'.

Stack Name	Created Time	Status	Description
demo-vpc	2018-05-24 15:53:58 UTC-0700	UPDATE_IN_PROGRESS	

Filter by: Status	Search events			
2018-05-24	Status	Type	Logical ID	Status Reason
16:32:13 UTC-0700	UPDATE_COMPLETE	AWS::CloudFormation::Stack	demo-vpc	
16:32:12 UTC-0700	UPDATE_COMPLETE_CLEANUP_IN_PROGRESS	AWS::CloudFormation::Stack	demo-vpc	
16:32:06 UTC-0700	UPDATE_COMPLETE	AWS::S3::Bucket	S3AppBucket	
16:32:01 UTC-0700	UPDATE_IN_PROGRESS	AWS::CloudFormation::Stack	demo-vpc	User Initiated
15:57:42 UTC-0700	CREATE_COMPLETE	AWS::CloudFormation::Stack	demo-vpc	
15:57:40 UTC-0700	CREATE_COMPLETE	AWS::EC2::Route	RouteDefaultPrivateA	

Una vez que el estado de la pila cambió a UPDATE_COMPLETE, puede navegar a la pestaña Salidas y descubrir que nuestros cambios se han reflejado ahora. La pestaña Salidas tiene cuatro valores en comparación con antes, estaba vacía:

The screenshot shows the AWS CloudFormation console interface. At the top, there are buttons for 'Create Stack', 'Actions', and 'Design template'. Below these, a filter dropdown is set to 'Active' and a search box contains 'By Stack Name'. The main table lists one stack: 'demo-vpc', created on 2018-05-24 at 15:53:58 UTC-0700, with a status of 'UPDATE_COMPLETE'. Below the table, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', 'Stack Policy', 'Change Sets', and 'Rollback Triggers'. The 'Outputs' tab is selected, showing a list of outputs for the stack 'demo-vpc'. The outputs include 'appbucketurl', 'vpcid', 'natgatewayaid', and 'natgatewaybid'.

Stack Name	Created Time	Status	Description
demo-vpc	2018-05-24 15:53:58 UTC-0700	UPDATE_COMPLETE	

Key	Value	Description	Export Name
appbucketurl	http://demo-vpc-s3appbucket-1tpko9hqotzl.s3-website-us-east-1.amazonaws.com	Shared Infrastructure App Bucket	sharedinf-appbucketurl
vpcid	vpc-95370fee	ID of Shared Infrastructure VPC	sharedinf-vpcid
natgatewayaid	nat-0f1ac3f564cbad943	ID of NAT Gateway A	
natgatewaybid	nat-07cf630f543cf33f8	ID of NAT Gateway B	

Además, haga clic en el ícono de CloudFormation en la esquina superior derecha de la pantalla y seleccione la opción Exportar, encontrará dos valores exportados que se muestran aquí que se pueden utilizar como referencia entre pilas.

Build VPC with AWS CloudFormation Lab

CloudFormation ^ Exports			
<div>Stacks</div> <div>Exports</div> <div>StackSets</div>			
Showing 2 exports			
Export Value	Stack Name	Stack ID	
sharedinf-appbucketurl	http://demo-vpc-s3appbucket-1tpiko9hqotzl.s3...	demo-vpc	arn:aws:cloudformation:us-east-1:789211807855:stack/demo-vpc/58064a90-...
sharedinf-vpcid	vpc-95370fee	demo-vpc	arn:aws:cloudformation:us-east-1:789211807855:stack/demo-vpc/58064a90-...

Para crear una referencia de pila cruzada, use el campo Exportar salida para marcar el valor de una salida de recursos para exportar. Luego, use la función intrínseca Fn:: ImportValue para importar el valor.

Appendix:

Initial AWS CloudFormation Template for lab exercise:

Create a file Lab_Initial_CloudFormation_Module_General_ImmersionDay.yaml and copy paste following code :

```
AWSTemplateFormatVersion: '2010-09-09'
Parameters:
  vpccidr:
    Type: String
    Default: 10.20.0.0/16
  psharedacidr:
    Type: String
    Default: 10.20.0.0/22
  psharedbcidr:
    Type: String
    Default: 10.20.4.0/22

Resources:
  VPC:
    Type: "AWS::EC2::VPC"
    Properties:
      CidrBlock: !Ref vpccidr
  IGW:
    Type: "AWS::EC2::InternetGateway"
  S3AppBucket:
    Type: "AWS::S3::Bucket"
    Properties:
      AccessControl: PublicRead
      WebsiteConfiguration:
        ErrorDocument: index.html
        IndexDocument: index.html
  BucketPolicyApp:
    Type: "AWS::S3::BucketPolicy"
    Properties:
      Bucket: !Ref S3AppBucket
      PolicyDocument:
        Statement:
```


Build VPC with AWS CloudFormation Lab

```
-
  Sid: "ABC123"
  Action:
    - "s3:GetObject"
  Effect: Allow
  Resource: !Join [ "", [ "arn:aws:s3:::", !Ref S3AppBucket, "/"* ]]
  Principal:
    AWS:
      - "*"

GatewayAttach:
  Type: "AWS::EC2::VPCGatewayAttachment"
  Properties:
    InternetGatewayId: !Ref IGW
    VpcId: !Ref VPC
SubnetPublicSharedA:
  Type: "AWS::EC2::Subnet"
  Properties:
    AvailabilityZone: !Select [ 0, !GetAZs ]
    CidrBlock: !Ref psharedacidr
    MapPublicIpOnLaunch: true
    VpcId: !Ref VPC
SubnetPublicSharedB:
  Type: "AWS::EC2::Subnet"
  Properties:
    AvailabilityZone: !Select [ 1, !GetAZs ]
    CidrBlock: !Ref psharedbcidr
    MapPublicIpOnLaunch: true
    VpcId: !Ref VPC
SubnetRouteTableAssociatePublicA:
  Type: "AWS::EC2::SubnetRouteTableAssociation"
  Properties:
    RouteTableId: !Ref RouteTablePublic
    SubnetId: !Ref SubnetPublicSharedA
SubnetRouteTableAssociatePublicB:
  Type: "AWS::EC2::SubnetRouteTableAssociation"
  Properties:
    RouteTableId: !Ref RouteTablePublic
    SubnetId: !Ref SubnetPublicSharedB
RouteDefaultPublic:
  Type: "AWS::EC2::Route"
  DependsOn: GatewayAttach
  Properties:
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref IGW
    RouteTableId: !Ref RouteTablePublic
RouteDefaultPrivateA:
  Type: "AWS::EC2::Route"
  Properties:
    DestinationCidrBlock: 0.0.0.0/0
    NatGatewayId: !Ref NatGatewayA
    RouteTableId: !Ref RouteTablePrivateA
RouteDefaultPrivateB:
  Type: "AWS::EC2::Route"
  Properties:
    DestinationCidrBlock: 0.0.0.0/0
    NatGatewayId: !Ref NatGatewayB
    RouteTableId: !Ref RouteTablePrivateB
RouteTablePublic:
  Type: "AWS::EC2::RouteTable"
  Properties:
    VpcId: !Ref VPC
```

Build VPC with AWS CloudFormation Lab

```
RouteTablePrivateA:
  Type: "AWS::EC2::RouteTable"
  Properties:
    VpcId: !Ref VPC
RouteTablePrivateB:
  Type: "AWS::EC2::RouteTable"
  Properties:
    VpcId: !Ref VPC
EIPNatGWA:
  DependsOn: GatewayAttach
  Type: "AWS::EC2::EIP"
  Properties:
    Domain: vpc
EIPNatGWB:
  DependsOn: GatewayAttach
  Type: "AWS::EC2::EIP"
  Properties:
    Domain: vpc
NatGatewayA:
  Type: "AWS::EC2::NatGateway"
  Properties:
    AllocationId: !GetAtt EIPNatGWA.AllocationId
    SubnetId: !Ref SubnetPublicSharedA
NatGatewayB:
  Type: "AWS::EC2::NatGateway"
  Properties:
    AllocationId: !GetAtt EIPNatGWB.AllocationId
    SubnetId: !Ref SubnetPublicSharedB
```