



Workbook de Implementación de Proyecto:

## **Separación de Ambientes para Alamo**

Ingeniero: Roberto Castro Barrios

## Definición y creación de la estructura de red

Como primer paso, iniciaremos especificando las características de la VPC a generar con el fin de formar un proceso claro y consiso para llevar a cabo dicha separación de ambientes y seguir el proceso definido dentro del plan de trabajo.

### VPC Original Producción

Nombre de la VPC: VPC-Produccion

Ipv4 CIDR: 192.168.0.0/16

Número de subredes: 3 **segmentos públicos**.

- SB-Prod-BD
  - IPv4 CIDR: 192.168.2.0/24
- SB-Prod-Aplicaciones-I
  - IPv4 CIDR: 192.168.1.0/24
- SB-Prod-Aplicaciones-II
  - IPv4 CIDR: 192.168.3.0/24

Tabla de rutas: RT-Produccion

- S3 Endpoint
- 0.0.0.0/0 hacia Internet Gateway
- 192.168.0.0/16 hacia local

### VPC Propuesta Producción

Nombre de la VPC: Alamo-Prod

Ipv4 CIDR: 10.0.0.0/20

Número de subredes: 2 **segmentos públicos** y 2 **segmentos privados**.

- **alamo-prod-public-1a**
  - IPv4 CIDR: 10.0.0.0/24
- **alamo-prod-public-1b**
  - IPv4 CIDR: 10.0.1.0/24
- **alamo-prod-private-1a**
  - IPv4 CIDR: 10.0.2.0/24
- **alamo-prod-private-1b**
  - IPv4 CIDR: 10.0.3.0/24

Tabla de rutas:

- RT-Public-Prod
  - S3 Endpoint

- 0.0.0.0/0 hacia Internet Gateway
- 10.0.0.0/20 hacia local
- RT-Private-Prod
  - S3 Endpoint\* (Sólo si es necesario comunicar el segmento privado hacia S3)
  - 0.0.0.0/0 hacia NAT Gateway
  - 192.168.0.0/16 hacia local

## VPC Propuesta QA

Nombre de la VPC: Alamo-QA

Ipv4 CIDR: 172.168.0.0/20

Número de subredes: 2 segmentos públicos y 2 segmentos privados.

- alamo-qa-public-1a
  - IPv4 CIDR: 172.168.0.0/24
- alamo-qa-public-1b
  - IPv4 CIDR: 172.168.1.0/24
- alamo-qa-private-1a
  - IPv4 CIDR: 172.168.2.0/24
- alamo-qa-private-1b
  - IPv4 CIDR: 172.168.3.0/24

Tabla de rutas:

- RT-Public-QA
  - S3 Endpoint
  - 0.0.0.0/0 hacia Internet Gateway
  - 172.168.0.0/20 hacia local
- RT-Private-QA
  - S3 Endpoint\* (Sólo si es necesario comunicar el segmento privado hacia S3)
  - 0.0.0.0/0 hacia NAT Gateway
  - 172.168.0.0/20 hacia local

## VPC Propuesta Dev

Nombre de la VPC: Alamo-Dev

Ipv4 CIDR: 172.16.0.0/20

Número de subredes: 2 segmentos públicos y 2 segmentos privados.

- alamo-dev-public-1a
  - IPv4 CIDR: 172.16.0.0/24

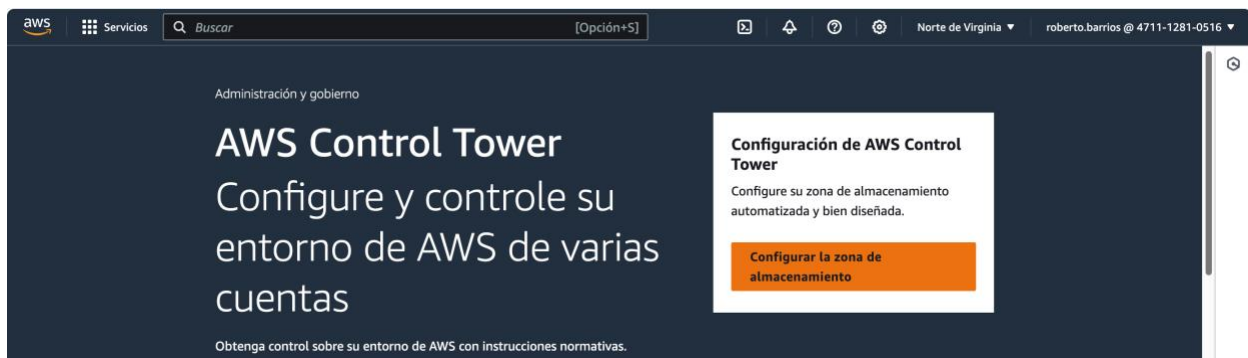
- **alamo-dev-public-1b**
  - IPv4 CIDR: 172.16.1.0/24
- **alamo-dev-private-1a**
  - IPv4 CIDR: 172.16.2.0/24
- **alamo-dev-private-1b**
  - IPv4 CIDR: 172.16.3.0/24

Tabla de rutas:

- **RT-Public-Dev**
  - S3 Endpoint
  - 0.0.0.0/0 hacia Internet Gateway
  - 172.168.0.0/20 hacia local
- **RT-Private-Dev**
  - S3 Endpoint\* (Sólo si es necesario comunicar el segmento privado hacia S3)
  - 0.0.0.0/0 hacia NAT Gateway
  - 172.168.0.0/20 hacia local

## Configuración de Control Tower

Como primer paso, nos dirigimos al servicio de control Tower en la región US-EAST-1 y hacemos click en el recuadro naranja “Configurar la zona de almacenamiento”:



Posteriormente, seleccionamos nuestra región principal donde será desplegado el servicio de Control Tower:

## Región principal

Para elegir una región principal para AWS Control Tower, seleccione una región del selector de regiones de AWS o del menú desplegable que aparece a continuación. Esta será la región predeterminada donde se aprovisionarán los recursos de las cuentas compartidas.

**No puede cambiar la región principal después de establecer la zona de almacenamiento.**

EE.UU. Este (Norte de Virginia) ▼

Seleccionamos regiones adicionales donde se desee desplegar la solución de Control Tower, en este caso todos nuestros recursos estarán en EE.UU. Este (Norte de Virginia) por lo que no será necesario agregar otra región:

## Seleccione regiones adicionales para la gobernanza (1/29) [Información](#)

Seleccione las regiones de AWS que regirán para su entorno. **Revise las regiones adicionales para la gobernanza [panel de ayuda](#)**, porque algunos controles de AWS Control Tower no están disponibles en todas las regiones. No se puede anular la selección de la región principal.

**i** Le recomendamos que amplíe su zona de aterrizaje de AWS Control Tower únicamente a las regiones de AWS en las que necesite ejecutar cargas de trabajo.


<input type="text"/> <span>&lt; 1 2 3 4 &gt; ⚙</span>				
<input type="checkbox"/>	Nombre de la región ▼	Código de la región ▼	Estado de AWS Control Tower ▼	Estado de la región de AWS ▼
<input checked="" type="checkbox"/>	EE.UU. Este (Norte de Virginia) Región principal	us-east-1	⊖ No controlado	✅ Activa de forma pre determinada

Habilitamos la denegación de regiones para aplicar un control que prohíbe el acceso a los servicios y operaciones de AWS, por región. Esta configuración es revertible y en este caso, sólo estará disponible la región EE.UU. Este (Norte de Virginia) para la creación y operación de servicios:

## Seleccione regiones adicionales para la gobernanza (1/29) [Información](#)



Seleccione las regiones de AWS que regirán para su entorno. **Revise las regiones adicionales para la gobernanza [panel de ayuda](#)**, porque algunos controles de AWS Control Tower no están disponibles en todas las regiones. No se puede anular la selección de la región principal.

 Le recomendamos que amplíe su zona de aterrizaje de AWS Control Tower únicamente a las regiones de AWS en las que necesite ejecutar cargas de trabajo.

<1234>

Nombre de la región

Código de la región

Estado de AWS Control Tower

Estado de la región de AWS

EE.UU. Este (Norte de Virginia)

Región principal

us-east-1

No controlado

Activa de forma pre determinada

Damos click en el recuadro naranja “Siguiente” y procedemos con la configuración de la nomenclatura de las Unidades Organizacionales a levantar para los temas de Seguridad y Auditoría, así como para ambientes de Producción, QA y Desarrollo:

## Configurar OU [Información](#)

### OU fundamental

Para iniciar una estructura de OU bien planificada en la zona de destino, AWS Control Tower configura una OU de seguridad por usted. Esta OU contiene dos cuentas compartidas: la cuenta de archivo de registro y la cuenta de auditoría de seguridad (también conocida como cuenta de auditoría).

Cambiar el nombre de la OU: *opcional*

“Seguridad” es el nombre predeterminado de la OU (organizational unit, OU) para las cuentas compartidas. Los nombres de las OU deben ser únicos y se pueden editar después de configurar la zona de almacenamiento.

### OU adicional

Para ayudar a configurar un sistema de varias cuentas, AWS Control Tower recomienda crear una OU secundaria al configurar la zona de almacenamiento. Esta OU se puede utilizar para almacenar cualquier cuenta de producción o desarrollo. Puede crear más unidades organizativas después de configurar la zona de almacenamiento.

Cambiar el nombre de la OU: *opcional*

“Sandbox” es el nombre de OU predeterminado para la OU adicional. Los nombres de las OU deben ser únicos y se pueden editar después de configurar la zona de almacenamiento.

Hacemos click en “Siguiente” y procedemos con la configuración del correo y nombre de las cuentas a crear para las unidades organizacionales anteriormente definidas:

## Configurar cuentas compartidas [Información](#)

### Cuenta de administración

La cuenta de administración proporciona la facturación y la administración de las cuentas y la zona de aterrizaje. Depende de la dirección de correo electrónico de la cuenta de AWS existente.

### Cuenta de archivo de registro

La cuenta de archivos de registro es un repositorio de registros inmutables de actividades de la API y configuraciones de recursos de todas las cuentas.

☒ **Crear cuenta nueva**

Cree una nueva dirección de correo electrónico para cuenta de archivo de registro. Esta no debe estar en uso para una cuenta de AWS existente.

☐ **Usar cuenta existente**

Escribir el ID de cuenta de una cuenta de archivo de registro que existe en la organización

#### Crear cuenta

alamo.log-archive@myappsoftware.com

La dirección de correo electrónico de la cuenta de archivo de registro no debe estar en uso para una cuenta de AWS existente. Debe tener entre 6 y 64 caracteres.

**Cambiar el nombre de la cuenta: *opcional***

El nombre de cuenta del archivo de registro debe ser único con respecto al nombre de la otra cuenta. **No podrá editar el nombre después de configurar la zona de almacenamiento.**

Alamo-LogArchive

### Cuenta de auditoría

La cuenta de auditoría es una cuenta restringida. Permite a los equipos de seguridad y cumplimiento obtener acceso a todas las cuentas de la organización.

☒ **Crear cuenta nueva**

Cree una nueva dirección de correo electrónico para cuenta de auditoría. Esta no debe estar en uso para una cuenta de AWS existente.

☐ **Usar cuenta existente**

Escribir el ID de cuenta de una cuenta de auditoría que existe en la organización

#### Crear cuenta

alamo.audit@myappsoftware.com

La dirección de correo electrónico de la cuenta de auditoría no debe estar en uso para una cuenta de AWS existente. Debe tener entre 6 y 64 caracteres.

**Cambiar el nombre de la cuenta: *opcional***

El nombre de la cuenta de auditoría debe ser único con respecto al nombre de la otra cuenta. **No podrá editar el nombre después de configurar la zona de almacenamiento.**

Alamo-Audit

Procedemos con las configuraciones adicionales como la habilitación de Identity Center, CloudTrail, retención default para los buckets de registros en S3:



## Configuraciones adicionales

### Configuración de acceso a la cuenta de AWS [Información](#)

Seleccione cómo administrar el acceso a las cuentas de AWS registradas en AWS Control Tower. Podrá modificar esto posteriormente.

- ☐ AWS Control Tower configura el acceso a la cuenta de AWS con IAM Identity Center.  
Se recomienda si acaba de comenzar a utilizar AWS o si la estructura de administración del acceso funciona con [Grupos y conjuntos de permisos de AWS Control Tower](#) . Más adelante podrá conectar el proveedor de identidades (IdP) externo en IAM Identity Center.

- ☒ Acceso autoadministrado a la cuenta de AWS con IAM Identity Center u otro método.  
La mejor opción si existen requisitos personalizados para administrar el acceso a las cuentas de AWS. AWS Control Tower no administrará el acceso a las cuentas. Es necesario configurar IAM Identity Center u otro método de acceso.

## Configuraciones adicionales

### Configuración de acceso a la cuenta de AWS [Información](#)

Seleccione cómo administrar el acceso a las cuentas de AWS registradas en AWS Control Tower. Podrá modificar esto posteriormente.

- ☒ AWS Control Tower configura el acceso a la cuenta de AWS con IAM Identity Center.  
Se recomienda si acaba de comenzar a utilizar AWS o si la estructura de administración del acceso funciona con [Grupos y conjuntos de permisos de AWS Control Tower](#) . Más adelante podrá conectar el proveedor de identidades (IdP) externo en IAM Identity Center.

- ☐ Acceso autoadministrado a la cuenta de AWS con IAM Identity Center u otro método.  
La mejor opción si existen requisitos personalizados para administrar el acceso a las cuentas de AWS. AWS Control Tower no administrará el acceso a las cuentas. Es necesario configurar IAM Identity Center u otro método de acceso.

### Configuración de registros para Amazon S3 - *opcional* [Información](#)

En estos dos campos, introduzca números que representen los tiempos de retención del ciclo de vida del bucket de registro de Amazon S3 y del bucket de registro de acceso.

#### Retención de bucket de Amazon S3 para registro

Default: 1

Los años deben expresarse como números enteros del 1 al 15, con valores de hasta 2 decimales. Las duraciones inferiores a 1 año se expresan en días.

#### Formato para el registro

years ▼

#### Retención de bucket de Amazon S3 para registro de acceso


Default: 10

Los años deben expresarse como números enteros del 1 al 15, con valores de hasta 2 decimales. Las duraciones inferiores a 1 año se expresan en días.

#### Formato para el registro de acceso

years ▼

### Cifrado KMS - *opcional* [Información](#)

AWS Key Management Service (KMS) le ayuda a crear y administrar claves criptográficas y controlar sus recursos en AWS Control Tower. Para seleccionar una clave, marque la casilla. La clave KMS debe tener permisos para AWS CloudTrail y AWS Config. No se admiten claves de varias regiones. [Obtenga más información sobre KMS](#) 

☐ Habilitar y personalizar la configuración de cifrado

Para desactivar la configuración de cifrado, desactive esta casilla.

Revisamos y confirmamos las configuraciones generadas, permisos de servicio por crear e instrucciones del servicio:

## Permisos de servicio

AWS Control Tower necesita su permiso para administrar los recursos de AWS y aplicar reglas en su nombre.

### ▼ Obtenga más información sobre los permisos

#### Permiso para administrar políticas de control de servicios (SCP) en la organización

AWS Control Tower utiliza SCP para aplicar controles preventivos en las unidades organizativas (OU) y, por lo tanto, requiere permiso para crear, modificar y asociar SCP. Además, AWS Control Tower puede leer el contenido de las SCP creadas por AWS Control Tower periódicamente para verificar que los controles preventivos estén habilitados en la cuenta. AWS Control Tower no lee el contenido de las SCP que no fueron creadas por AWS Control Tower.

#### Roles de IAM

AWS Control Tower requiere la creación de cuatro roles para lanzar una zona de destino. AWS Control Tower divide los permisos en cuatro roles como una práctica recomendada para restringir el acceso a los conjuntos mínimos de acciones y recursos.

**Nombre de rol:** AWSControlTowerAdmin

**Finalidad:** Este rol le proporciona a AWS Control Tower acceso a una infraestructura fundamental para el mantenimiento de la zona de almacenamiento.

**Política insertada:**

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Action": "ec2:DescribeAvailabilityZones",
7        "Resource": "*"
8      }
9    ]
10 }
```

**Política administrada de AWS adicional asociada:**[AWSControlTowerServiceRolePolicy](#)**Nombre de rol:** AWSControlTowerStackSetRole**Finalidad:** AWS CloudFormation asume este rol para implementar conjuntos de pilas en cuentas creadas por AWS Control Tower.**Política insertada:**

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Action": [
6          "sts:AssumeRole"
7        ],
8        "Resource": [
9          "arn:aws:iam::*:role/AWSControlTowerExecution"
10       ],
11       "Effect": "Allow"
12     }
13   ]
14 }
```

**Nombre de rol:** AWSControlTowerCloudTrailRole**Finalidad:** AWS Control Tower habilita a CloudTrail como práctica recomendada y proporciona este rol a AWS CloudTrail. AWS CloudTrail asume este rol para crear y publicar registros de CloudTrail.**Política insertada:**

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Action": "logs:CreateLogStream",
6        "Resource": "arn:aws:logs::*:log-group:aws-controltower/CloudTrailLog",
7        "Effect": "Allow"
8      },
9      {
10       "Action": "logs:PutLogEvents",
11       "Resource": "arn:aws:logs::*:log-group:aws-controltower/CloudTrailLog",
12       "Effect": "Allow"
13     }
14   ]
15 }
```

**Nombre de rol:** AWSControlTowerConfigAggregatorRoleForOrganizations

**Finalidad:** Para que el agregador de AWS Config funcione con AWS Organizations, AWS Control Tower debe crear un nuevo rol, denominado AWSControlTowerConfigAggregatorRoleForOrganizations, que tiene los permisos necesarios para describir la organización y enumerar las cuentas que contiene.

AWSControlTowerConfigAggregatorRoleForOrganizations requiere la política administrada

AWSConfigRoleForOrganizations y una relación de confianza con config.amazonaws.com.

**Política insertada:**

```
1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Effect": "Allow",
6        "Principal": {
7          "Service": "config.amazonaws.com"
8        },
9        "Action": "sts:AssumeRole"
10     }
11   ]
12 }
```

**Política administrada de AWS adicional asociada:**

[AWSConfigRoleForOrganizations](#)

## Instrucciones

Le recomendamos encarecidamente que siga las instrucciones que se ofrecen a continuación cuando utilice AWS Control Tower. Dichas instrucciones pueden cambiar a medida que actualizamos el servicio.

### 1. Instrucciones generales

- No modifique ni elimine recursos creados por AWS Control Tower en la cuenta de administración o en las cuentas compartidas. La modificación de estos recursos puede requerir una actualización de su zona de almacenamiento.
- No modifique ni elimine los roles de AWS Identity and Access Management (IAM) creados en las cuentas compartidas de la OU principal. La modificación de estos recursos puede requerir una actualización de su zona de almacenamiento.
- Para obtener más información sobre los recursos creados por AWS Control Tower, consulte [Recursos](#) en la Guía del usuario de AWS Control Tower.

### 2. Instrucciones de AWS Organizations

- No utilice AWS Organizations para actualizar políticas de control de servicios (SCP) que AWS Control Tower asocia a una OU administrada por AWS Control Tower. Si lo hace, los controles podrían adoptar un estado desconocido, lo que requeriría volver a habilitar los controles afectados en AWS Control Tower.
- Si utiliza AWS Organizations para crear, invitar o mover cuentas dentro de una organización creada por AWS Control Tower, esas cuentas externas no serán administradas por medio de AWS Control Tower y no aparecerán en la tabla de cuentas.
- Si utiliza AWS Organizations para crear, invitar o mover OU dentro de una organización creada por AWS Control Tower, esas OU externas no serán administradas por medio de AWS Control Tower y no aparecerán en la tabla de unidades organizativas.
- Si utiliza AWS Organizations para eliminar una OU creada por AWS Control Tower o para cambiarle el nombre, AWS Control Tower seguirá mostrando esa OU con su nombre original. No podrá aprovisionar una nueva cuenta para esa OU utilizando la creación de cuentas de AWS Tower.

### 3. Guía del Centro de identidades de IAM

- Si se reconfigura el directorio en el Centro de identidades de IAM en Active Directory, se eliminarán todos los usuarios y grupos preconfigurados en el Centro de identidades.

### 4. Instrucciones de creación de cuentas

- Cuando utilice la creación de cuentas para aprovisionar cuentas nuevas en AWS Service Catalog, no defina TagOptions, no habilite las notificaciones y no cree un plan de producto aprovisionado. De lo contrario, se puede producir un error al aprovisionar una cuenta nueva.

Para obtener más información, consulte la [Guía del usuario de AWS Control Tower](#).

- ☒ **Comprendo los permisos que utilizará AWS Control Tower para administrar los recursos de AWS y aplicar reglas en mi nombre. También comprendo las instrucciones sobre el uso de AWS Control Tower y los recursos de AWS subyacentes.**

Cancelar

Anterior

Configurar la zona de almacenamiento

Esperamos al rededor de 60 min. para que se levanten y configuren las tareas automatizadas de Control Tower, finalmente observaremos una ventana de confirmación como la siguiente:

[AWS Control Tower](#) > Panel



**Su zona de almacenamiento ya está disponible.**



AWS Control Tower ha configurado lo siguiente:

- 2 unidades organizativas, una para sus cuentas compartidas y otra para las cuentas que aprovisionarán sus usuarios.
- 3 cuentas compartidas, que son la cuenta de administración y las cuentas aisladas para el archivo de registro y la auditoría de seguridad.
- La configuración de Identity and Access Management seleccionada.
- 20 controles preventivos para aplicar políticas y 3 controles de detección para detectar infracciones en la configuración.

**Inscribir cuentas existentes en AWS Control Tower**

Puede inscribir cuentas existentes de su organización de AWS Organizations en AWS Control Tower y administrarlas de la misma forma que administra las cuentas creadas con la creación de cuentas. Para la inscripción, es necesario realizar trabajo adicional.

[Más información sobre cómo inscribir cuentas existentes en AWS Control Tower](#)

## Creación de Cuentas de Producción / QA / Desarrollo

Creación de Cuenta Productiva.

Como primer paso nos dirigimos al menú lateral izquierdo y seleccionamos el servicio de **Account Factory**:



Posteriormente, nos aseguramos de generar los cambios definidos para el ambiente productivo dentro de la configuración de red:



### Configuración de red

[Editar](#)

Las siguientes opciones de configuración de la VPC estarán disponibles para los usuarios cuando aprovisionen cuentas nuevas. Puede modificar la configuración en cualquier momento.

Subred accesible por medio de Internet  
Permitir

Número máximo de subredes privadas  
2

Intervalo de direcciones (CIDR) para las VPC  
de la cuenta  
10.0.0.0/20

Regiones para la creación de la VPC  
EE.UU. Este (Norte de Virginia)

Hacemos click en el recuadro “Crear cuenta” y configuramos el correo y nombre de la cuenta productiva:

### Detalles de la cuenta

#### Correo electrónico de la cuenta

Especifique un correo electrónico para crear una nueva cuenta en su zona de aterrizaje.

Debe tener entre 6 y 64 caracteres. El email no distingue entre mayúsculas y minúsculas.

#### Nombre de visualización

Nombre de la cuenta tal como aparece en AWS Control Tower

Solo debe contener letras, números, puntos, guiones, guiones bajos y espacios. Debe comenzar por una letra o un número.

Configuramos un usuario administrador inicial para el acceso a la cuenta a generar, así como la unidad organizativa:

### Configuración de acceso

#### Correo electrónico del usuario de IAM Identity Center

Designa un usuario del Centro de identidades de IAM.

Debe tener entre 6 y 64 caracteres.

#### Nombre de usuario del Centro de identidades de IAM

Nombre y apellido previstos para la creación de un usuario del Centro de identidades de IAM

### Unidad organizativa

#### Unidad organizativa

Seleccione una unidad organizativa para habilitar todos los controles que se configurarán en esta cuenta.



Creamos la cuenta y posteriormente, esperamos a que el servicio de AWS Control Tower provisione los recursos conforme a la configuración especificada:

**① Solicitud de creación enviada** ×  
AWS Control Tower está aprovisionando la cuenta. Para obtener más información sobre la solicitud, consulte Alamo-Produccion en [AWS Service Catalog](#) 🔗  
· [Información](#)

Adicionalmente, el proceso de creación de cuentas es llevado a cabo a por el servicio de AWS Service Catalog el cual...

### Creación de Cuenta Dev

[AWS Control Tower](#) > [Account factory](#) > Create account

## Create account [Info](#)

**①** AWS Control Tower cannot create an account if you are signed in as root. You can create 5 accounts at a time. ×

**①** As you increase the number of Regions with resources, account operations may take longer to complete. ×

### Account details

#### Account email

Specify an email in order to create a new account in your landing zone.

Must be from 6 to 64 characters long. Email is not case sensitive.

#### Display name

Name for account as it appears in AWS Control Tower

Must contain only letters, numbers, periods, dashes, underscores, spaces. Must begin with a letter or number.

**① Creation request submitted** ×  
AWS Control Tower is provisioning your account. For more information about your request, see Alamo-Dev in [AWS Service Catalog](#) 🔗. [Info](#)

Alamo-QA

### Account details

#### Account email

Specify an email in order to create a new account in your landing zone.

Must be from 6 to 64 characters long. Email is not case sensitive.

#### Display name

Name for account as it appears in AWS Control Tower

Must contain only letters, numbers, periods, dashes, underscores, spaces. Must begin with a letter or number.

### Access configuration

#### IAM Identity Center user email

Designate an IAM Identity Center user.

Must be from 6 to 64 characters long.

#### IAM Identity Center user name

First and last name intended for creating an IAM Identity Center user



## Configuración en IAM

### Configuración de Políticas de Contraseñas en IAM

#### Política de contraseñas [Información](#)

[Editar](#)

Configure los requisitos de contraseña para los usuarios de IAM.

Esta cuenta de AWS utiliza la siguiente política de contraseñas personalizadas:

##### Longitud mínima de la contraseña

8 caracteres

##### Seguridad de la contraseña

- Exigir al menos un carácter en mayúscula del alfabeto latino (A-Z)
- Exigir al menos un carácter en minúscula del alfabeto latino (a-z)
- Exigir al menos un número
- Exija al menos un carácter que no sea alfanumérico

##### Otros requisitos

- La contraseña caduca en 90 días
- Permitir que los usuarios cambien sus propias contraseñas

### Roles y Políticas para los diversos ambientes

#### Prod

- *Rol-Alamo-Prod-EC2-conexionSSM*
  - **Política:** AmazonSSMManagedInstanceCore

- **Descripción:** Rol empleado para la conexión con Systems Manager para el acceso a una instancia de EC2.
- *Rol-Alamo-Prod-Lambda-Backend*
  - **Política:**
  - **Descripción:**
- *Rol-Alamo-Prod-...*
  - **Política:**
  - **Descripción:**

## QA

- *Rol-Alamo-QA-EC2-conexionSSM*
  - **Política:** AmazonSSMManagedInstanceCore
  - **Descripción:** Rol empleado para la conexión con Systems Manager para el acceso a una instancia de EC2.
- *Rol-Alamo-QA-Lambda-Backend*
  - **Política:**
  - **Descripción:**
- *Rol-Alamo-QA-...*
  - **Política:**
  - **Descripción:**

## Dev

- *Rol-Alamo-Dev-EC2-conexionSSM*
  - **Política:** AmazonSSMManagedInstanceCore
  - **Descripción:** Rol empleado para la conexión con Systems Manager para el acceso a una instancia de EC2.
- *Rol-Alamo-Dev-Lambda-Backend*
  - **Política:**
  - **Descripción:**
- *Rol-Alamo-Dev-...*
  - **Política:**
  - **Descripción:**

## Configuración de MFA en cuenta Root

## Configuración de Identity Center

Conjuntos de permisos

- ps-admin
  - **Política:** AdministratorAccess
  - **Cuentas:**
    - Alamo-Prod
    - Alamo-QA
    - Alamo-Dev
    - Alamo-Management
    - Alamo-Securit
    - Alamo-ArchiveLog
- ps-qa
  - **Política:** AmazonRDSFullAccess
  - **Política:** AWSLambda\_FullAccess
  - **Política:** AmazonAPIGatewayAdministrator
  - **Política:** AmazonEC2FullAccess
  - **Política:** AWSCloudFormationFullAccess
  - **Política:** CloudWatchFullAccessV2
  - **Política:** AmazonEventBridgeFullAccess
  - **Política:** AmazonSSMFullAccess
  - **Política:** SecretsManagerReadWrite
  - **Política:** AmazonS3FullAccess
  - **Cuentas:**
    - Alamo-QA
- ps-dev
  - **Política:** AmazonRDSFullAccess
  - **Política:** AWSLambda\_FullAccess
  - **Política:** AmazonAPIGatewayAdministrator
  - **Política:** AmazonEC2FullAccess
  - **Política:** AWSCloudFormationFullAccess
  - **Política:** CloudWatchFullAccessV2
  - **Política:** AmazonEventBridgeFullAccess
  - **Política:** AmazonSSMFullAccess
  - **Política:** SecretsManagerReadWrite
  - **Política:** AmazonS3FullAccess
  - **Política:** ReadOnlyAccess
  - **Cuentas:**
    - Alamo-Dev
- ps-readonly
  - **Política:** ReadOnlyAccess
  - **Cuentas:**
    - Alamo-Prod
    - Alamo-QA
    - Alamo-Dev
    - Alamo-Management
    - Alamo-Security

- Alamo-Archive Log
- ps-billing
  - **Política:** Billing
  - **Cuentas:**
    - Alamo-Management

## Configuración de VPCs

### Configuración de VPC Peering

Es necesario establecer una conexión de tipo VPC Peering entre la cuenta original y la VPC de QA para poder migrar los datos dentro de la región y zona de disponibilidad de manera privada:

**Peering connection settings**

Name - *optional*  
Create a tag with a key of 'Name' and a value that you specify.

PeeringToQA

**Select a local VPC to peer with**

VPC ID (Requester)

vpc-03394cd5c3aaec08b (VPC-Produccion) ▼

VPC CIDRs for vpc-03394cd5c3aaec08b (VPC-Produccion)

CIDR	Status	Status reason
192.168.0.0/16	✔ Associated	-

### Select another VPC to peer with

Account

- ☐ My account  
☒ Another account

Account ID

Account ID

Region

- ☒ This Region (us-east-1)  
☐ Another Region

VPC ID (Accepter)

VPC ID

### NAT Gateway

Se realizará la siguiente configuración para la NAT Gateway:

### Tablas de Ruteo

### Configuración de SG

### Configuración de Instancias de EC2

- **Nombre de la instancia:** Alamo-Prod-CMS\_Blog
  - **VPC ID:** (Alamo-Prod)
  - **Subnet ID:** (Alamo-Prod-Public-1a)
  - **Grupo de Seguridad:** Sí
  - **IP Elástica:** Sí (IPE-CMS\_Blog)
  - **Llave PEM:** pem1.pem
  - **Tipo de Instancia:** t3.medium
  - **SO:** Linux
  - **Almacenamiento:**
  - **Rol de IAM:** Rol-Alamo-Prod-EC2-conexionSSM
- **Nombre de la instancia:** Alamo-Prod-Bastion\_Host

- **VPC ID:** (Alamo-Prod)
- **Subnet ID:** (Alamo-Prod-Public-1a)
- **Grupo de Seguridad:** Sí
- **IP Elástica:** No
- **Llave PEM:** pem2.pem
- **Tipo de Instancia:** t3.small
- **SO:** Windows Server 2019 Base
- **Almacenamiento:** 30 GB
- **Rol de IAM:** Rol-Alamo-Prod-EC2-conexionSSM