

Documento de Arquitectura

Proyecto Remove

Versión: Julio 2023

Autor: Cristian Gonzalez

Tabla de contenido

Proyecto Remove.....	0
Tabla de contenido.....	1
Versiones.....	2
Fecha.....	2
Responsable.....	2
Versión.....	2
Comentarios.....	2
Descripción General.....	3
Networking.....	4
Backend.....	5
Balanceadores de carga.....	14
Route 53 y DNS.....	17
Engine.....	18
FrontEnd.....	19
S3 – bucket.....	22
Bases de Datos.....	24
Redes.....	26
Alta Disponibilidad.....	28
Escalamiento.....	30
Sugerencias.....	32

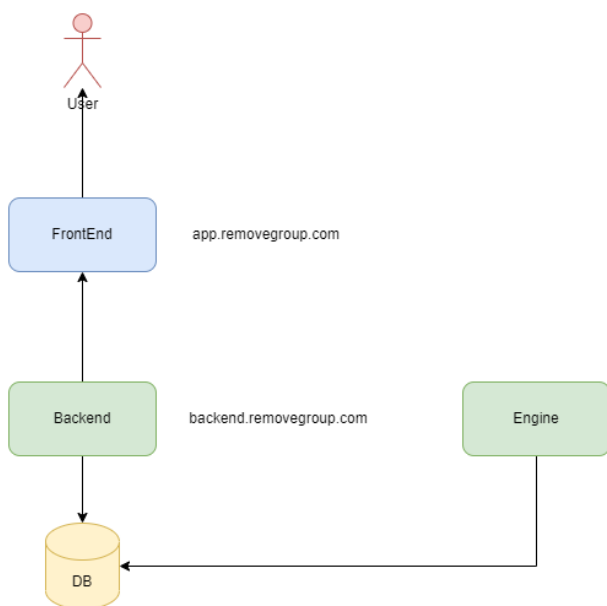
Versiones

Fecha	Responsable	Versión	Comentarios
17-07-2023	Cristian Gonzalez G	Borrador Inicial	

Este documento tiene como objetivo describir la solución cloud implementada, su arquitectura, piezas de software, las consideraciones utilizadas y como administrar los distintos productos usados en la solución. Hay que aclarar que no tiene el detalle de la solución de código fuente programada, y que no hay enfoque en el código fuente desarrollado.

Descripción General

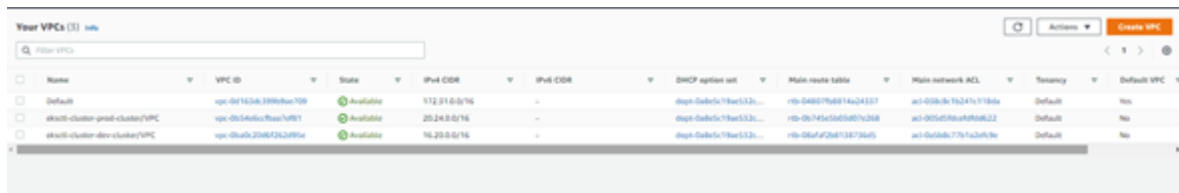
La solución del proyecto Remove cuenta de 3 artefactos de software. Estos artefactos están desplegados en AWS, mediante diferentes productos. En el siguiente esquema se representa la comunicación de estos artefactos.



Para el despliegue de los artefactos de backend, se generó una solución basada en Elastic Container Service (Fargate). En cambio, para el frontend existe una solución basada en Content Delivery Network (CloudFront).

Networking

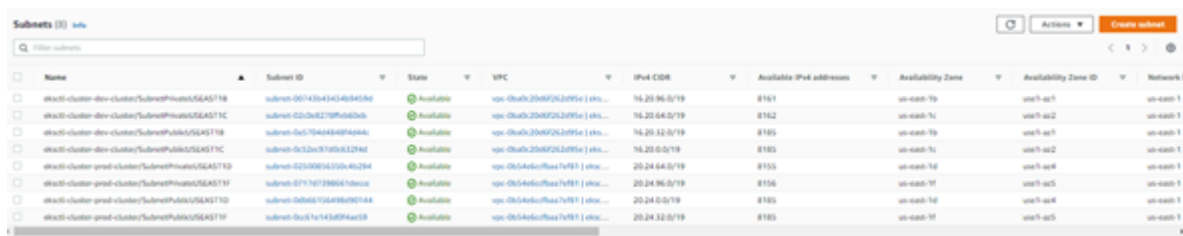
En esta etapa se reutilizo el networking proveniente del anterior cluster Kubernetes, por lo que el perímetro de red sigue contenido en las siguientes VPC



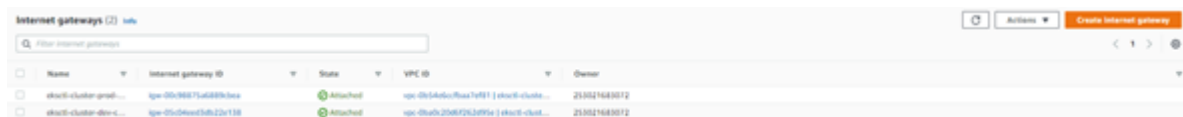
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DNAT rule set	Main route table	Main network ACL	Termination	Default VPC
Default	vpc-d0143d4b	Available	172.31.0.0/16	-	app-elasti-cluster-prod-cluster/VPC	rtb-0480176814a24327	acl-016d5c1b247c118da	Default	No
elasti-cluster-prod-cluster/VPC	vpc-0b54d6c1	Available	20.24.0.0/16	-	app-elasti-cluster-prod-cluster/VPC	rtb-0b741e5d5d5d5d5d	acl-016d5c1b247c118da	Default	No
elasti-cluster-dev-cluster/VPC	vpc-0b54d6c1	Available	16.20.0.0/16	-	app-elasti-cluster-dev-cluster/VPC	rtb-0b741e5d5d5d5d5d	acl-016d5c1b247c118da	Default	No

Subredes derivadas de la red principal (VPC) divididas en 4 grupos por ambiente, 2 subredes públicas.


Para efectos de lo implementado en Fargate estas subredes fueron reutilizadas. Incluyendo sus grupos de seguridad.



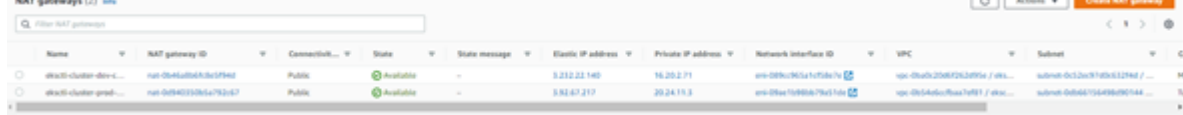
Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID	Network
elasti-cluster-dev-cluster/SubnetPrivate/SGAS118	subnet-00143d4b3434b343	Available	vpc-0b54d6c1	16.20.0.0/16	8161	us-east-1b	us-east-1b	us-east-1
elasti-cluster-dev-cluster/SubnetPublic/SGAS118	subnet-020d210f0d210f0d	Available	vpc-0b54d6c1	16.20.0.0/16	8162	us-east-1c	us-east-1c	us-east-1
elasti-cluster-prod-cluster/SubnetPrivate/SGAS118	subnet-0c12a84848484848	Available	vpc-0b54d6c1	20.24.0.0/16	8163	us-east-1b	us-east-1b	us-east-1
elasti-cluster-prod-cluster/SubnetPublic/SGAS118	subnet-0c12a84848484848	Available	vpc-0b54d6c1	20.24.0.0/16	8164	us-east-1c	us-east-1c	us-east-1
elasti-cluster-dev-cluster/SubnetPrivate/SGAS119	subnet-020d210f0d210f0d	Available	vpc-0b54d6c1	16.20.0.0/16	8165	us-east-1b	us-east-1b	us-east-1
elasti-cluster-dev-cluster/SubnetPublic/SGAS119	subnet-020d210f0d210f0d	Available	vpc-0b54d6c1	16.20.0.0/16	8166	us-east-1c	us-east-1c	us-east-1
elasti-cluster-prod-cluster/SubnetPrivate/SGAS119	subnet-0711717171717171	Available	vpc-0b54d6c1	20.24.0.0/16	8167	us-east-1b	us-east-1b	us-east-1
elasti-cluster-prod-cluster/SubnetPublic/SGAS119	subnet-0711717171717171	Available	vpc-0b54d6c1	20.24.0.0/16	8168	us-east-1c	us-east-1c	us-east-1
elasti-cluster-dev-cluster/SubnetPrivate/SGAS120	subnet-0b54d6c10b54d6c1	Available	vpc-0b54d6c1	16.20.0.0/16	8169	us-east-1b	us-east-1b	us-east-1
elasti-cluster-dev-cluster/SubnetPublic/SGAS120	subnet-0b54d6c10b54d6c1	Available	vpc-0b54d6c1	16.20.0.0/16	8170	us-east-1c	us-east-1c	us-east-1



Name	Internet gateway ID	State	VPC ID	Owner
elasti-cluster-prod-cluster	igw-0b54d6c10b54d6c1	Attached	vpc-0b54d6c1	213021683012
elasti-cluster-dev-cluster	igw-0b54d6c10b54d6c1	Attached	vpc-0b54d6c1	213021683012



Name	Allocated IPv4 add...	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP address	Association ID	Network interface owner acco...
elasti-cluster-dev-cluster/NetIP	3.212.22.140	Public IP	elasti-cluster-dev-cluster/NetIP	-	-	16.20.2.11	elasti-cluster-dev-cluster/NetIP	213021683012
elasti-cluster-prod-cluster/NetIP	3.212.22.141	Public IP	elasti-cluster-prod-cluster/NetIP	-	-	20.24.11.3	elasti-cluster-prod-cluster/NetIP	213021683012



Name	NAT gateway ID	Connectio...	State	State message	Elastic IP address	Private IP address	Network interface ID	VPC	Subnet
elasti-cluster-dev-cluster	nat-0b54d6c10b54d6c1	Public	Available	-	3.212.22.140	16.20.2.11	eni-0b54d6c10b54d6c1	vpc-0b54d6c1	subnet-0b54d6c10b54d6c1
elasti-cluster-prod-cluster	nat-0b54d6c10b54d6c1	Public	Available	-	3.212.22.141	20.24.11.3	eni-0b54d6c10b54d6c1	vpc-0b54d6c1	subnet-0b54d6c10b54d6c1

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
--	vpc-048076d814a24337	--	--	Yes	vpc-0d153a3398b8a708 (De...	253027683072
--	vpc-0b145e0c03d07a2d8	--	--	Yes	vpc-0b34edccf8a7a9b1 (vpc...	253027683072
--	vpc-0b0af2d813873d45	--	--	Yes	vpc-0b40e25d8f2d2d95a (vpc...	253027683072
ekr-ec2-cluster-dev-v-cluster/PrivateRouteTable/SGK718	vpc-0d73d8138a78d9d2	subnet-00743d43434b8...	--	No	vpc-0b40e25d8f2d2d95a (vpc...	253027683072
ekr-ec2-cluster-dev-v-cluster/PrivateRouteTable/SGK71C	vpc-0574d3d8138a78d9d2	subnet-025d8f2d2d95a...	--	No	vpc-0b40e25d8f2d2d95a (vpc...	253027683072
ekr-ec2-cluster-dev-v-cluster/PrivateRouteTable	vpc-070a6d7543854502d9	2 subnets	--	No	vpc-0b40e25d8f2d2d95a (vpc...	253027683072
ekr-ec2-cluster-prod-v-cluster/PrivateRouteTable/SGK71D	vpc-070a6d7543854502d9	2 subnets	--	No	vpc-0b34edccf8a7a9b1 (vpc...	253027683072
ekr-ec2-cluster-prod-v-cluster/PrivateRouteTable/SGK71F	vpc-05a0d95030a3b4d7	2 subnets	--	No	vpc-0b34edccf8a7a9b1 (vpc...	253027683072
ekr-ec2-cluster-prod-v-cluster/PrivateRouteTable	vpc-0c3d87a7291d9d8a	2 subnets	--	No	vpc-0b34edccf8a7a9b1 (vpc...	253027683072

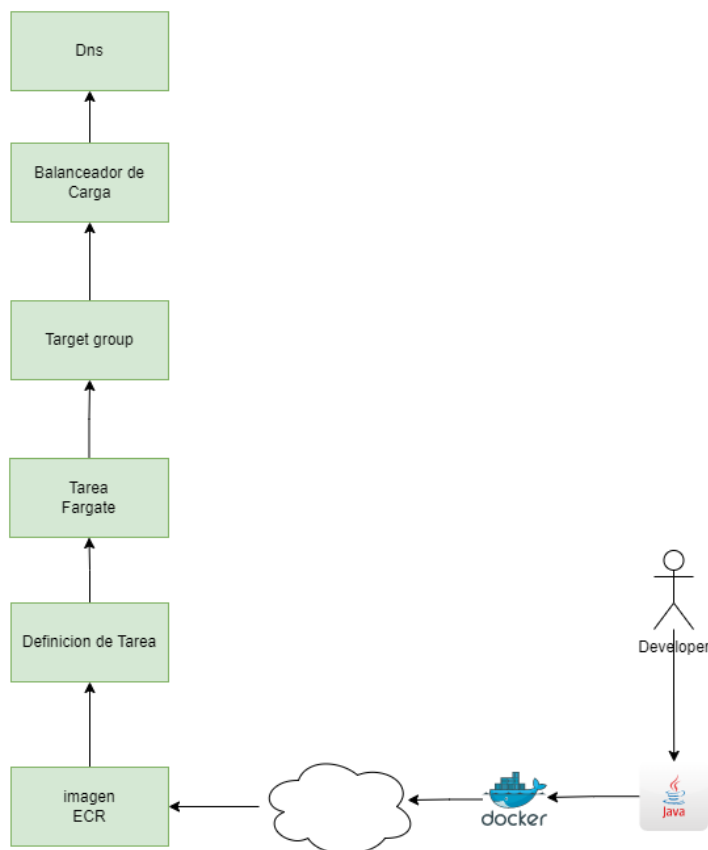
Sugerencia

Como recomendación se sugiere la posibilidad, dentro de lo posible, revisar y eliminar las subredes que no están en uso.

Backend

El Backend es un monolito escrito en Java que contiene la lógica de consultas a la base de datos, este monolito es encapsulado en una imagen Docker y servido mediante protocolo rest al frontend.

Para entender como es desplegado revisar el siguiente esquema



El desarrollador crea el código necesario en el backend, construye la imagen Docker y la publica en Elastic Container Registry (ECR), con la nueva imagen cargada. La definición de tarea fargate reconoce la nueva imagen y la deja disponible, para actualizar con la nueva imagen se debe volver a relanzar el servicio o actualizarlo, con esta acción el servicio deja disponible la imagen en los contenedores que tenga configurados.

Los contenedores o tareas son presentados en un target group el cual es alimentado por un balanceador de carga que recibe las peticiones desde el DNS (backend.removegroup.com)

A continuación, se explicará en detalle cada una de estas capas.

El primer elemento para definir es el clúster Fargate que es donde se publican los servicios, en este caso Engine y Backend. En las imágenes siguientes se puede apreciar los dos clúster creados, para QA y Producción. En la sección servicios se puede apreciar tanto el backend como el engine.

ClusterQA

Actualizar el clúster Eliminar clúster

Información general sobre el clúster

ARN ClusterQA	Estado Activo	Supervisión de CloudWatch Valor predeterminado	Instancias de contenedor registradas -
Servicios Vaciando -	Activo 2	Tareas Pendiente -	Ejecutando 2

Servicios Tareas Infraestructura Métricas Tareas programadas Etiquetas

Servicios (2) Información

Administrar etiquetas Actualizar Eliminar el servicio Crear

Filtrar servicios por valor

Todos los tipos de lanz... Todos los tipos de ser...

Nombre del servicio	Estado	ARN	Tipo de se...	Implementaciones y tareas	Última implementación
engineQA4	Activo	arn:aws:ecs:us...	REPLICA	1/1 tareas en ejecución	Completado
backend-qa-07	Activo	arn:aws:ecs:us...	REPLICA	1/1 tareas en ejecución	Completado

Amazon Elastic Container Service > Clústeres > produccion > Servicios

produccion Actualizar el clúster Eliminar clúster

Información general sobre el clúster

ARN arn:aws:ecs:us-east-1:123456789012:cluster/produccion	Estado Activo	Supervisión de CloudWatch Valor predeterminado	Instancias de contenedor registradas -
Servicios Vacando -	Activo 2	Tareas Pendiente -	Ejecutando 3

Servicios | Tareas | Infraestructura | Métricas | Tareas programadas | Etiquetas

Servicios (2) Información Administrar etiquetas Actualizar Eliminar el servicio Crear

Buscar servicios por valor Todos los tipos de lanz... Todos los tipos de ser... < 1 >

Nombre del servicio	Estado	ARN	Tipo de se...	Implementaciones y tareas	Última implementación
EngineProd2	Activo	arn:aws:ecs:us-east-1:123456789012:cluster/produccion/task-definition/EngineProd2	REPLICA	1/1 tareas en ejecución	Completado
removeProd	Activo	arn:aws:ecs:us-east-1:123456789012:cluster/produccion/task-definition/removeProd	REPLICA	2/2 tareas en ejecución	Completado

En la visión general de Fargate se puede ver ambos clúster y el estado de salud de sus servicios, si por algún motivo estos servicios dejan de funcionar el color verde pasará a rojo indicando el error. En el caso de que haya más de una tarea corriendo por servicio y solo una falla, se podrá ver un proporcional a las tareas que estén fallando en color rojo.

Amazon Elastic Container Service > Clústeres

Clústeres (2) Información Crear clúster

Buscar en clústeres < 1 >

Clúster	Servicios	Tareas	Instancias de contenedor registradas	Supervisión de CloudWatch	Estrategia de proveedor de capacidad
produccion	2	0 pendiente/s 3 en ejecución	0	Valor predeterminado	No se ha encontrado ningún valor predeterminado
ClusterQA	2	0 pendiente/s 2 en ejecución	0	Valor predeterminado	No se ha encontrado ningún valor predeterminado

Cuando entramos a un servicio se puede ver que balanceador de carga tiene asociado y cuantas tareas está ejecutando, en este caso 2 tareas.

También se aprecia la URL de estado de salud, que indica que todo está funcionando bien con el backend.

<https://backend.removegroup.com/remove/api/rest/healthcheck>

Sugerencia

Agregar esta URL a herramientas de alerta y monitoreo de forma que cuando el sistema tenga una interrupción avise a los administradores para su rápida acción.

removeProd Información

↻

Actualizar servicio

Eliminar el servicio

Estado y métricas

Tareas

Registros

Implementaciones

Eventos

Configuración

Redes

Etiquetas

Estado Información

ARN

📄

produccion/removeProd

Estado

🟢

Activo

Tareas (2 deseadas)

🟢

0 pendiente/s

|

2 en ejecución

Estado actual de las implementaciones

🟢

2 completado(s)

Periodo de gracia de comprobación de estado

0 seconds

▼ Estado del equilibrador de carga

(Balanceador de carga de aplicaciones) removeProdBL

Ver equilibrador de carga

Puerto del protocolo del agente de escucha

[HTTPS:443](#)

Nombre del grupo de destino: protocolo

[removeProdTG:HTTP](#)

Ruta de comprobación de estado

[/remove/api/rest/healthcheck](#)

Destinos (2 en total)

🟢

2 con estado correcto

🟡

0 con estado incorrecto

En caso de algún error de la aplicación, se puede seleccionar la pestaña registro y mostrará el log de errores.

Amazon Elastic Container Service > Clústeres > produccion > Servicios > removeProd > Registros

removeProd Información

↻

Actualizar servicio

Eliminar el servicio

Estado y métricas

Tareas

Registros

Implementaciones

Eventos

Configuración

Redes

Etiquetas

Registros (3996+) Información

Puede usar la barra de filtros de abajo para buscar y hacer coincidir términos, frases o valores en sus eventos de registro. [Más información sobre los patrones de filtrado](#)

📅 Desde hace 1 hora

Ver en CloudWatch

↻

🔍 Buscar eventos de registro con patrones de filtrado

removeProd

<

1

2

3

4

5

6

7

8

...

>

🔊

Marca temporal (Local)	Mensaje	Tarea	Contenedor
14/7/2023, 12:15:40 @HT-4	2023-07-14 16:15:40.815 INFO ContextId: [] Thread:[qtp2056190002-13082] UserId - [c.a.r.e.a.h.AdminHealthCheckController] - Consultando endpoint HEALTHCHECK	d710d1757fc5400ea45c450bc7015601	revomeProd
14/7/2023, 12:15:40 @HT-4	2023-07-14 16:15:40.815 INFO ContextId: [] Thread:[qtp2056190002-13082] UserId - [c.a.r.e.u.Filters] - REQUEST:	d710d1757fc5400ea45c450bc7015601	revomeProd
14/7/2023, 12:15:40 @HT-4	Url: /remove/api/rest/healthcheck	d710d1757fc5400ea45c450bc7015601	revomeProd
14/7/2023, 12:15:40 @HT-4	Url: http://20.24.54.211/remove/api/rest/healthcheck	d710d1757fc5400ea45c450bc7015601	revomeProd
14/7/2023, 12:15:40 @HT-4	Method: GET	d710d1757fc5400ea45c450bc7015601	revomeProd
14/7/2023, 12:15:40 @HT-4	Params:	d710d1757fc5400ea45c450bc7015601	revomeProd
14/7/2023, 12:15:40 @HT-4	agent: ELB-HealthChecker/2.0	d710d1757fc5400ea45c450bc7015601	revomeProd
2023-07-14 16:15:40.815 INFO ContextId: f1 Thread:[oto2056190002-13082] UserId - [c.a.r.e.a.h.AdminHealthCheckController] - GET: class	d710d1757fc5400ea		

Existe en la misma pantalla un botón ver en CloudWatch que es la herramienta especializada en AWS, para la visualización de logs, que contiene variadas herramientas de consulta para poder visualizar de diferentes formas los log de la aplicación.

En la pantalla Tareas se puede ver cada contenedor que se está ejecutando, su tiempo de vida y su estado general

8 Documento de Arquitectura: Proyecto Remove

Amazon Elastic Container Service > Clústeres > produccion > Servicios > removeProd > Tareas

removeProd Información Actualizar servicio Eliminar el servicio

Estado y métricas | **Tareas** | Registros | Implementaciones | Eventos | Configuración | Redes | Etiquetas

Tareas (1/2)

Tareas en ejecución Todos los tipos de lanz...

Tarea	Último estado	Estado de...	Definició...	Revisión	Estado	Iniciado a las	Instancias de co...	Tipo de lanz...
20fc161f78ae4d11a7821e2...	Ejecutando	Ejecutando	revomeProd	1	Desconocid	ayer	-	FARGATE
d710d1757fc5400ea45c450...	Ejecutando	Ejecutando	revomeProd	1	Desconocid	hace 8 días	-	FARGATE

En caso de que se desee publicar una nueva versión o sea necesario reiniciar los contenedores, se puede hacer en clic en actualizar servicio.

Se debe hacer clic en forzar nueva implementación si es un cambio de versión.

Si se desea aumentar por tráfico el número de contenedores que responden al servicio, se debe setear el nuevo número en tareas deseadas con base en la carga que tenga el sistema

Actualizar removeProd [Información](#)

Configuración de implementación

☐ Forzar una nueva implementación

Definición de tarea

Seleccione una definición de tarea existente. Para crear una nueva definición de tarea, vaya a [Definiciones de tareas](#).

☐ Especificar la revisión manualmente

Ingrese manualmente la revisión en lugar de elegir entre las 100 revisiones más recientes para la familia de definición de tareas seleccionada.

Familia

revomeProd

Revisión

1 (MÁS RECIENTE)

Tipo de servicio

REPLICA

Tareas deseadas

Especifique el número de tareas que se van a lanzar.

2

Porcentaje de cantidad mín. de tareas en

ejecución [Información](#)

Especifica el porcentaje mínimo de tareas en ejecución permitidas durante el despliegue de un servicio.

100

valores en %

Porcentaje de cantidad máx. de tareas en

ejecución [Información](#)

Especifica el porcentaje máximo de tareas en ejecución permitidas durante el despliegue de un servicio.

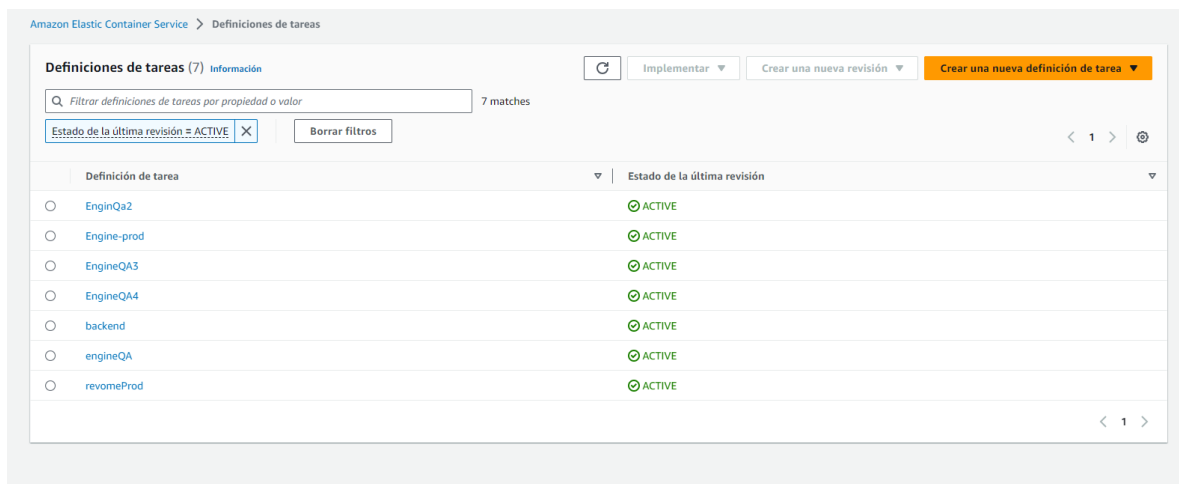
200

valores en %

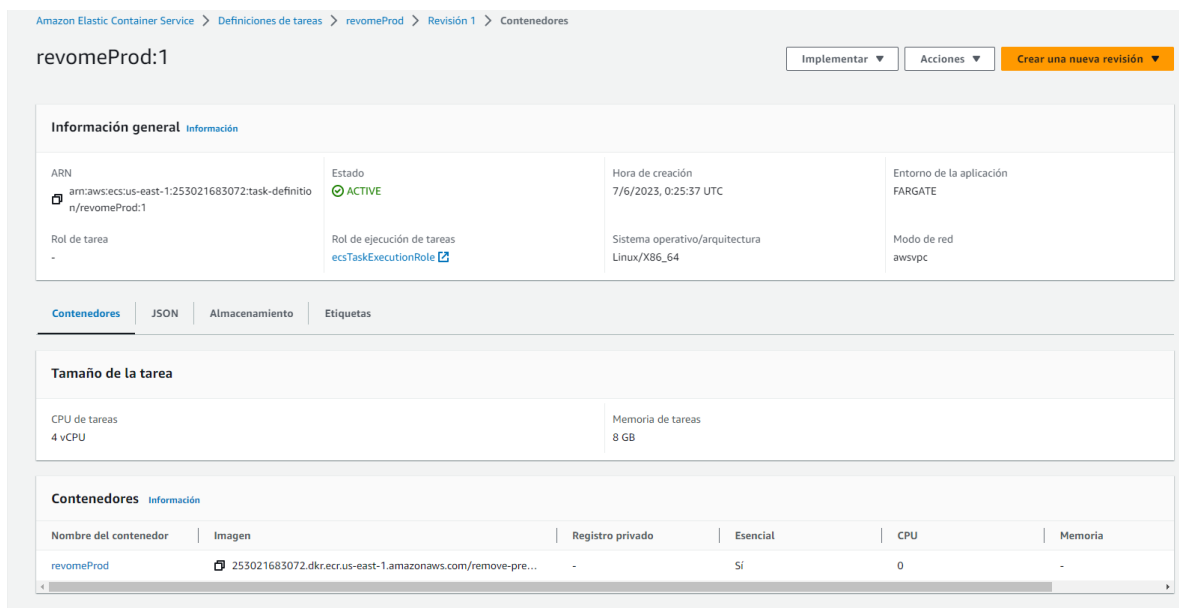
► [Detección de errores de despliegue](#) [Información](#)

► [Configuración informática \(avanzada\)](#)

Se pueden establecer diferentes revisiones, como diferentes definiciones de tareas, lo que puede utilizarse como rollback de versiones en caso de ser necesario. Basta con elegir una definición de tareas distinta o una revisión diferente y puede volverse a esa versión.



En la siguiente imagen se encuentra el botón para crear una nueva revisión.



Todas las definiciones de tareas, están asociadas a un repositorio de imágenes contenido en el ECR, que es donde se cargan las imágenes Docker a desarrollar. En la siguiente imagen se puede ver los repositorios asociados a cada artefacto y ambiente.

Amazon ECR > Repositorios

Private | Public

Repositorios privados (6)

Buscar repositorios

Ver comandos de envío Eliminar Acciones **Crear repositorio**

<input type="checkbox"/>	Nombre del repositorio	URI	Creado en	Inmutabilidad de etiqueta	Frecuencia de análisis	Tipo de cifrado	Caché de extracción
<input type="checkbox"/>	remove-back-prd	253021683072.dkr.ecr.us-east-1.amazonaws.com/remove-back-prd	17 de marzo de 2022, 12:34:08 (UTC-03)	Desactivado	Manual	AES-256	Inactivo
<input type="checkbox"/>	remove-dev	253021683072.dkr.ecr.us-east-1.amazonaws.com/remove-dev	28 de octubre de 2021, 12:44:33 (UTC-03)	Desactivado	Manual	AES-256	Inactivo
<input type="checkbox"/>	remove-engine-dev	253021683072.dkr.ecr.us-east-1.amazonaws.com/remove-engine-dev	28 de octubre de 2021, 15:01:51 (UTC-03)	Desactivado	Manual	AES-256	Inactivo
<input type="checkbox"/>	remove-engine-prd	253021683072.dkr.ecr.us-east-1.amazonaws.com/remove-engine-prd	17 de marzo de 2022, 12:34:27 (UTC-03)	Desactivado	Manual	AES-256	Inactivo
<input type="checkbox"/>	remove-preprod	253021683072.dkr.ecr.us-east-1.amazonaws.com/remove-preprod	06 de junio de 2023, 20:11:10 (UTC-04)	Desactivado	Manual	AES-256	Inactivo
<input type="checkbox"/>	remove-preprod-engine	253021683072.dkr.ecr.us-east-1.amazonaws.com/remove-preprod-engine	16 de junio de 2023, 15:14:20 (UTC-04)	Desactivado	Manual	AES-256	Inactivo

Para crear una nueva definición de tarea, se debe crear en la opción que entrega ECS (fargate) y verá el siguiente formulario.

Crear una nueva revisión de definición de tarea [Información](#)

Configuración de definición de tareas

Familia de definición de tareas [Información](#)
Especifique un nombre de familia de definición de tarea único.

revomeProd

Revisión
Revisión de fuente

1

Contenedor: 1 [Información](#) Contenedor esencial Eliminar

Detalles del contenedor
Especifique un nombre, una imagen de contenedor y si el contenedor debe marcarse como esencial. Cada definición de tarea debe tener al menos un contenedor esencial.

Nombre URI de imagen Contenedor esencial Sí

Registro privado [Información](#)
Almacene las credenciales en Secrets Manager y, a continuación, utilice las credenciales para hacer referencia a las imágenes en los registros privados.

☒ Autenticación de registro privado

Mapeos de puertos [Información](#)
Agregue mapeos de puertos para permitir que el contenedor obtenga acceso a los puertos del host para enviar o recibir tráfico. Cualquier cambio en la configuración de mapeos de puertos afecta a la configuración de conexión del servicio asociada.

Puerto del contenedor	Protocolo	Nombre del puerto	Protocolo de la aplicación	
<input type="text" value="80"/>	TCP	<input type="text" value="revomeprod-80-tcp"/>	HTTP	Eliminar

Agregar más mapeos de puertos

En ella se establece el nombre del servicio y la imagen que desea utilizar desde ECR, como se ve en la imagen siguiente, en este punto se establece el tamaño en hardware virtualizado que utilizara el servicio. En el apartado de hardware asociado, se dará un resumen de los servicios existentes.

▼ Entorno

Especifique los requisitos de infraestructura para la definición de tarea.

Tamaño de la tarea | Información

Especifique la cantidad de CPU y memoria que reservar para su tarea.

CPU

4 vCPU ▼

Memoria

8 GB ▼

► Tamaño del contenedor - *opcional* | Información

▼ Roles de tarea - *condicionales*

Rol de tarea | Información

Un rol de IAM de tarea permite a los contenedores de la tarea realizar solicitudes de API a los servicios de AWS. Puede crear un rol de IAM de tarea desde la [consola de IAM](#).

Ninguno ▼

Rol de ejecución de tareas | Información

El agente de contenedor utiliza un rol de IAM de ejecución de tareas para realizar solicitudes a la API de AWS en su nombre. Si aún no tiene un rol de IAM de ejecución de tareas creado, podemos crear uno por usted.

ecsTaskExecutionRole ▼

Modo de red | Información

El modo de red que se utiliza para sus tareas. Cuando se selecciona el tipo de lanzamiento AWS Fargate (sin servidor), debe utilizar el modo de red awsvpc. Si selecciona el tipo de lanzamiento de instancia de Amazon EC2, puede utilizar diferentes modos de red en Linux o Windows. En Linux, puede elegir entre bridge, awsvpc, host o none. En Windows, puede elegir entre default o awsvpc.

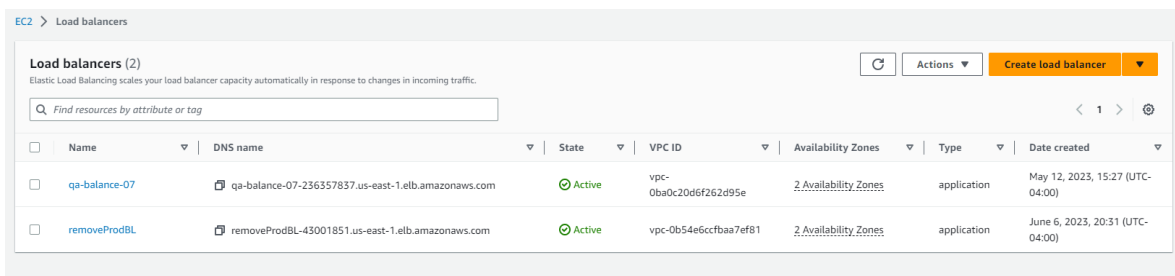
awsvpc ▼

Con todo esto configurado, solo basta la visibilidad del servicio de cara a internet, el cual es proporcionado por el balanceador de carga.

Balanceadores de carga

Cada ambiente de backend cuenta con un balanceador de carga que es esta asociada a la VPC de cada ambiente y a los grupos de seguridad con las reglas de tráfico asociadas a cada artefacto. Hay que recordar que solo el backend está expuesto de esta forma, ya que los servicios de engine no requieren salida a internet y por lo mismo solo corren como servicio fargate sin necesidad de balanceador de carga.

En la siguiente imagen se puede ver los dos balanceadores que sirven fargate, uno para cada servicio de backend, según ambiente.



EC2 > Load balancers

Load balancers (2)
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.


Find resources by attribute or tag

<input type="checkbox"/>	Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
<input type="checkbox"/>	qa-balance-07	qa-balance-07-236357837.us-east-1.elb.amazonaws.com	Active	vpc-0ba0c20d6f262d95e	2 Availability Zones	application	May 12, 2023, 15:27 (UTC-04:00)
<input type="checkbox"/>	removeProdBL	removeProdBL-43001851.us-east-1.elb.amazonaws.com	Active	vpc-0b54e6ccfbaa7ef81	2 Availability Zones	application	June 6, 2023, 20:31 (UTC-04:00)

En las reglas, existe un listener asociado al puerto 443 que redirige el tráfico al target group correspondiente, en este punto también está asociado el certificado de seguridad del dominio

EC2 > Load balancers > removeProdBL

removeProdBL

 Actions ▾

▼ Details

Load balancer type Application	Status Active	VPC vpc-0b54e6ccfbbaa7ef81	IP address type IPv4
Scheme Internet-facing	Hosted zone Z355XDOTRQ7X7K	Availability Zones subnet-0db66156498d90144 us-east-1d (use1-az4) subnet-0cc61e143d0f4ae59 us-east-1f (use1-az5)	Date created June 6, 2023, 20:31 (UTC-04:00)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:253021683072:loadbalancer/app/removeProdBL/4bfa6d329e21ae13		DNS name removeProdBL-43001851.us-east-1.elb.amazonaws.com (A Record)	

Listeners and rules | Network mapping | Security | Monitoring | Integrations | Attributes | Tags

Listeners and rules (1) 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.

☐ Protocol:Port ▾

☐ Default action ▾

☐ Rules ▾

☐ ARN ▾

☐ Security policy ▾

☐ Default SSL cert ▾

☐ Tags ▾


<input type="checkbox"/>	HTTPS:443	Forward to target group <ul style="list-style-type: none">removeProdTG: 1 (100%)Group-level stickiness: Off	1 rule	ARN	ELBSecurityPolicy-2016-08	*.removegroup.com (Certificat...	0 tags
--------------------------	-----------	--	--------	---------------------	---------------------------	--	--------

También se puede ver el networking asociado a las subredes públicas de la VPC.

En la pestaña de seguridad se puede ver el grupo de seguridad asociado al balanceador de carga.

EC2 > Load balancers > removeProdBL

removeProdBL

 Actions ▾

▼ Details

Load balancer type Application	Status Active	VPC vpc-0b54e6ccfbbaa7ef81	IP address type IPv4
Scheme Internet-facing	Hosted zone Z355XDOTRQ7X7K	Availability Zones subnet-0db66156498d90144 us-east-1d (use1-az4) subnet-0cc61e143d0f4ae59 us-east-1f (use1-az5)	Date created June 6, 2023, 20:31 (UTC-04:00)
Load balancer ARN arn:aws:elasticloadbalancing:us-east-1:253021683072:loadbalancer/app/removeProdBL/4bfa6d329e21ae13		DNS name removeProdBL-43001851.us-east-1.elb.amazonaws.com (A Record)	

Listeners and rules | Network mapping | Security | Monitoring | Integrations | Attributes | Tags

Security groups (1)

A security group is a set of firewall rules that control the traffic to your load balancer.

Security Group ID	Name	Description
sg-001cb3ce64c17f638	default	default VPC security group

En la pestaña de networking se puede ver el enlace a las subredes.

▼ Details

Load balancer type

Application

Status

Active

VPC

vpc-0b54e6ccfbba7ef81

IP address type

IPv4

Scheme

Internet-facing

Hosted zone

Z35SXDOTRQ7X7K

Availability Zones

subnet-0db66156498d90144 us-east-1d (use1-az4)
subnet-0cc61e143d0f4ae59 us-east-1f (use1-az5)

Date created

June 6, 2023, 20:31 (UTC-04:00)

Load balancer ARN

arn:aws:elasticloadbalancing:us-east-1:253021683072:loadbalancer/app/removeProdBL/4bfa6d329e21ae13

DNS name

removeProdBL-43001851.us-east-1.elb.amazonaws.com (A Record)

Listeners and rules

Network mapping

Security

Monitoring

Integrations

Attributes

Tags

Network mapping Info

Edit IP address type

Edit subnets

Targets in the listed zones and subnets are available for traffic from the load balancer using the IP addresses shown.

VPC

vpc-0b54e6ccfbba7ef81

IP address type

IPv4

IPv4: 20.24.0.0/16

IPv6 :-

Mappings

Selecting two or more Availability Zones and corresponding subnets increases the fault tolerance of your applications.

Zone	Subnet	IPv4 address	Private IPv4 address	IPv6 address
us-east-1d (use1-az4)	subnet-0db66156498d90144	Assigned by AWS	Assigned from CIDR 20.24.0.0/19	Not applicable
us-east-1f (use1-az5)	subnet-0cc61e143d0f4ae59	Assigned by AWS	Assigned from CIDR 20.24.32.0/19	Not applicable

En la pestaña de monitoreo, se puede ver el estado de las diferentes request que se hagan al balanceador de carga. Si el API empieza a generar errores de programación, en este panel se verán como errores 500.

Listeners and rules

Network mapping

Security

Monitoring

Integrations

Attributes

Tags

1h 3h 12h 1d 3d 1sem. Personalizado

🔄

▼

Añadir al panel

Target Response Time

Seconds

8e-3

4e-3

0

14:00 15:00 16:00

removeProdBL

Requests

Count

4

2

0

14:00 15:00 16:00

removeProdBL

Rule Evaluations

None

1

0.5

0

14:00 15:00 16:00

removeProdBL

HTTP 5XXs

Count

2

1

0

14:00 15:00 16:00

removeProdBL

HTTP 4XXs

None

1

0.5

0

14:00 15:00 16:00

removeProdBL

ELB 5XXs

None

1

0.5

0

14:00 15:00 16:00

removeProdBL

ELB 4XXs

Count

2

1

0

14:00 15:00 16:00

removeProdBL

HTTP 500s

None

1

0.5

0

14:00 15:00 16:00

removeProdBL

16 Documento de Arquitectura: Proyecto Remove

En los listener, se puede ver el targetgroup, que corresponde a los contenedores fargate que sirven el servicio. También se puede ver su estado de salud por contenedor.

En Registered targets, se puede ver los contenedores que sirven al servicio con las IP privadas de cada subnet que tiene asociado. También se puede observar su estado de salud de forma individual y sus respuestas en la pestaña de monitoreo se puede ver de forma individual cada contenedor.

EC2 > Target groups > removeProdTG

removeProdTG

Actions ▾

Details
arn:aws:elasticloadbalancing:us-east-1:253021683072:targetgroup/removeProdTG/f962fb63b1cf7e9

Target type IP	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-0b54e6ccfbba7ef81
IP address type IPv4	Load balancer removeProdBL		

Total targets	Healthy	Unhealthy	Unused	Initial	Draining
2	🟢 2	🔴 0	🔴 0	🕒 0	🕒 0

► **Distribution of targets by Availability Zone (AZ)**
Select values in this table to see corresponding filters applied to the Registered targets table below.

Targets | Monitoring | Health checks | Attributes | Tags

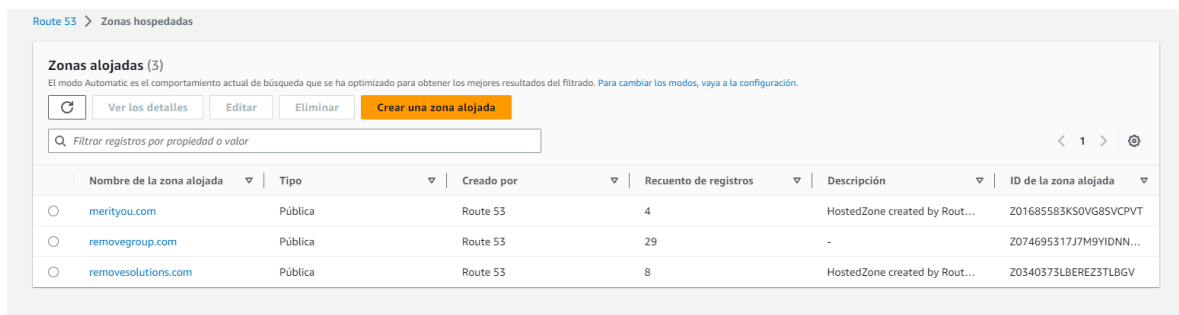
Registered targets (2)

🔄 Deregister Register targets

<input type="checkbox"/>	IP address	Port	Zone	Health status	Health status details
<input type="checkbox"/>	20.24.54.211	80	us-east-1f	🟢 healthy	
<input type="checkbox"/>	20.24.11.56	80	us-east-1d	🟢 healthy	

Route 53 y DNS

Existen 3 zonas alojadas actualmente, pero para el sistema solo se está usando el dominio removegroup.com. En el caso del backend, está expuesto por la URL backend.removegropu.com, que apunta al balanceador de carga anterior.



En esta imagen se ve el registro de DNS que utiliza el backend.

	Nombre de la zona alojada	Tipo	Creado por	Recuento de registros	Descripción	ID de la zona alojada
<input type="radio"/>	merityou.com	Pública	Route 53	4	HostedZone created by Rout...	Z01685583KS0VG8SVCPT
<input type="radio"/>	removegroup.com	Pública	Route 53	29	-	Z074695317J7M9YIDNN...
<input type="radio"/>	removesolutions.com	Pública	Route 53	8	HostedZone created by Rout...	Z0340373LBEREZ3TLBGV

	Nombre de la zona alojada	Tipo	Creado por	Recuento de registros	Descripción	ID de la zona alojada
<input type="checkbox"/>	removegroup.com	SOA	Simple	-	No	ns-877.awsdns-45.net. awsd...
<input type="checkbox"/>	removegroup.com	TXT	Simple	-	No	"v=spf1 include:_spf.google.c...
<input type="checkbox"/>	@.removegroup.com	TXT	Simple	-	No	"google-site-verification=CW...
<input type="checkbox"/>	_amazonses.removegroup.com	TXT	Simple	-	No	"wSxMOD/wix8Th27olQOqd...
<input type="checkbox"/>	_dmarc.removegroup.com	TXT	Simple	-	No	"v=DMARC1; p=none; rua=m...
<input type="checkbox"/>	1522905495316_domainkey.removegroup....	TXT	Simple	-	No	"k=rsa; p=MIGfMA0GC5qGSI...
<input type="checkbox"/>	awoasxogz_domainkey.removegroup.com	TXT	Simple	-	No	"v=DKIM1; k=rsa; p=MIGfMA...
<input type="checkbox"/>	b7nfuq2dcywhgceivly7tphkqifb3y_domain...	CNAME	Simple	-	No	b7nfuq2dcywhgceivly7tphk...
<input type="checkbox"/>	google_domainkey.removegroup.com	TXT	Simple	-	No	"v=DKIM1; k=rsa; p=MIGfMA...
<input type="checkbox"/>	tfbuf4m3kjbzbh3ve7gwsnn3srmxojf_dom...	CNAME	Simple	-	No	tfbuf4m3kjbzbh3ve7gwsnn...
<input type="checkbox"/>	u2iiz5vpof73d4jztsrjhxcenwbns_domaink...	CNAME	Simple	-	No	u2iiz5vpof73d4jztsrjhxcen...
<input type="checkbox"/>	api.removegroup.com	A	Simple	-	Sí	dualstack.k8s-removepr-bac...
<input type="checkbox"/>	app.removegroup.com	A	Simple	-	Sí	d3penzrugjvg4.cloudfront.net.
<input checked="" type="checkbox"/>	backend.removegroup.com	A	Simple	-	Sí	dualstack.removeprodbl-430...
<input type="checkbox"/>	backendqa.removegroup.com	A	Simple	-	Sí	dualstack.qa-balance-07-236...
<input type="checkbox"/>	formula.removegroup.com	A	Simple	-	No	178.33.167.50

Detalles del registro

[Editar el registro](#)

Nombre del registro
backend.removegroup.com

Tipo de registro
A

Valor
dualstack.removeprodbl-43001851.us-east-1.elb.amazonaws.com.

Alias
Sí

TTL (segundos)
-

Política de direccionamiento
Simple

Con esto el ciclo desde el DNS hasta el contenedor está descrito capa por capa.

Engine

El caso del engine es distinto, como no requiere salida a internet solo vive como contenedor fargate, pero tiene todos los elementos de log y escalamiento de un servicio normal.

FrontEnd

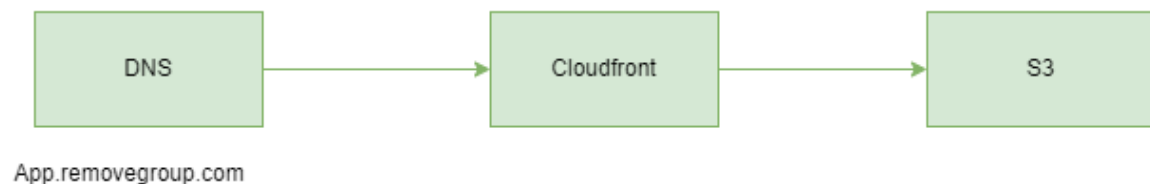
El frontend es contenido servido como static, por lo que no requiere de una infraestructura de servicios para ser desplegado. En el caso del frontend, el enfoque será desde el DNS hasta donde queda alojado el contenido.

En route53 podemos ver el registro `app.removegroup.com`, que es la url pública de la aplicación.

<input type="checkbox"/>	removegroup.com	SOA	Simple	-	No	ns-877.awsdns-45.net. awsd...	900	-
<input type="checkbox"/>	removegroup.com	TXT	Simple	-	No	*v=spf1 include:_spf.google.c...	300	-
<input type="checkbox"/>	@.removegroup.com	TXT	Simple	-	No	*google-site-verification=CW...	3600	-
<input type="checkbox"/>	_amazonses.removegroup.com	TXT	Simple	-	No	*wSxMOD/wix8Th27oIQOqd...	300	-
<input type="checkbox"/>	_dmarc.removegroup.com	TXT	Simple	-	No	*v=DMARC1; p=none; rua=m...	3600	-
<input type="checkbox"/>	1522905495316._domainkey.removegroup....	TXT	Simple	-	No	*k=rsa; p=MIGfMA0GCsGSI...	300	-
<input type="checkbox"/>	awoasxogz._domainkey.removegroup.com	TXT	Simple	-	No	*v=DKIM1; k=rsa; p=MIGfMA...	300	-
<input type="checkbox"/>	b7nfuq2dcywhgceivly7ltpkqifb3y._domai...	CNAME	Simple	-	No	b7nfuq2dcywhgceivly7ltpk...	1800	-
<input type="checkbox"/>	google._domainkey.removegroup.com	TXT	Simple	-	No	*v=DKIM1; k=rsa; p=MIGfMA...	300	-
<input type="checkbox"/>	tfbuf4m3kzwbh3ve7gwsnn3smyxof._dom...	CNAME	Simple	-	No	tfbuf4m3kzwbh3ve7gwsnn...	1800	-
<input type="checkbox"/>	u2liz5vpof73d4jjztsrnhjxcenwbns._domaink...	CNAME	Simple	-	No	u2liz5vpof73d4jjztsrnhjxcen...	1800	-
<input type="checkbox"/>	api.removegroup.com	A	Simple	-	Sí	dualstack.k8s-removepr-bac...	-	-
<input checked="" type="checkbox"/>	app.removegroup.com	A	Simple	-	Sí	d3penzrugjvg4.cloudfront.net.	-	-
<input type="checkbox"/>	backend.removegroup.com	A	Simple	-	Sí	dualstack.removeprodbl-430...	-	-
<input type="checkbox"/>	backendqa.removegroup.com	A	Simple	-	Sí	dualstack.qa-balance-07-236...	-	-
<input type="checkbox"/>	formula.removegroup.com	A	Simple	-	No	178.33.167.50	300	-

Detalles del registro
[Editar el registro](#)
Nombre del registro
app.removegroup.com
Tipo de registro
A
Valor
d3penzrugjvg4.cloudfront.net.
Alias
Sí
TTL (segundos)
-
Política de direccionamiento
Simple

Este registro enlaza a una distribución cloud front, como se puede ver en el siguiente esquema.



Existen 3 distribuciones, se mantuvo la antigua distribución de producción frontend, ya que es necesaria para la redirección desde el dominio `removesolution` a `removegroup`.

CloudFront > Distributions

Distributions (3) [Info](#) [Refresh](#) [Enable](#) [Disable](#) [Delete](#) [Create distribution](#)

Search all distributions

<input type="checkbox"/>	ID	Description	Type	Domain name	Alternate domain names	Origins
<input type="checkbox"/>	EQKUFR9BNNYPO	Produccion	Production	d3penzrugjvg4.cloudfront...	app.removegroup.com	removeapp-prod.s3.us-east-1.amazonaws.com
<input type="checkbox"/>	E2INGSWLNVB5N	Prod -old	Production	dggexk8qf5wz8.cloudfront...	removesolutions.com	remove-solution-temp.s3.us-east-1.amazonaws.com
<input type="checkbox"/>	EQKHTNXS14QK	QA	Production	d28dvc1jp16302.cloudfro...	qa.removegroup.com	removedevs3-0000.s3.us-east-1.amazonaws.com

En el caso de la distribución cloudfront productiva se tiene asociado su certificado de seguridad correspondiente.

CloudFront > Distributions > EQKUFR9BNNYPO

EQKUFR9BNNYPO [View metrics](#)

[General](#) [Origins](#) [Behaviors](#) [Error pages](#) [Geographic restrictions](#) [Invalidations](#) [Tags](#)

Details

Distribution domain name d3penzrugjvg4.cloudfront.net	ARN arn:aws:cloudfront::253021683072:distribution/EQKUFR9BNNYPO	Last modified July 12, 2023 at 2:22:27 PM UTC
--	--	--

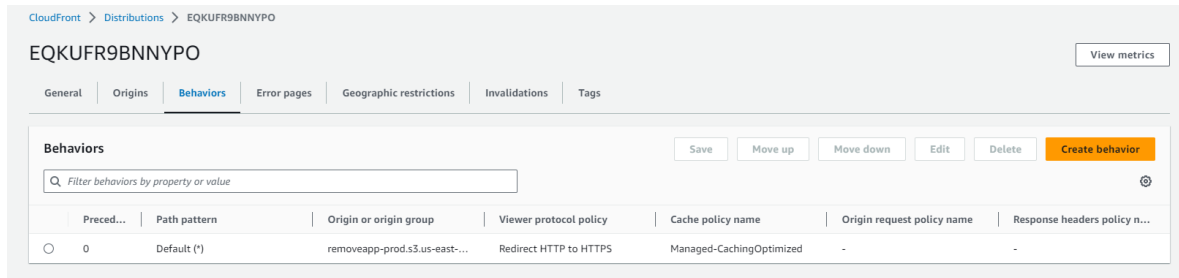
Settings [Edit](#)

Description Produccion	Alternate domain names app.removegroup.com	Standard logging Off
Price class Use all edge locations (best performance)	Custom SSL certificate *.removegroup.com	Cookie logging Off
Supported HTTP versions HTTP/2, HTTP/1.1, HTTP/1.0	Security policy TLSv1.2_2021	Default root object index.html
AWS WAF CreatedByCloudFront-d5a3523c-d1ca-4fcd-84db-f964e8632a5 (WAFv2)		

Continuous deployment [Info](#)

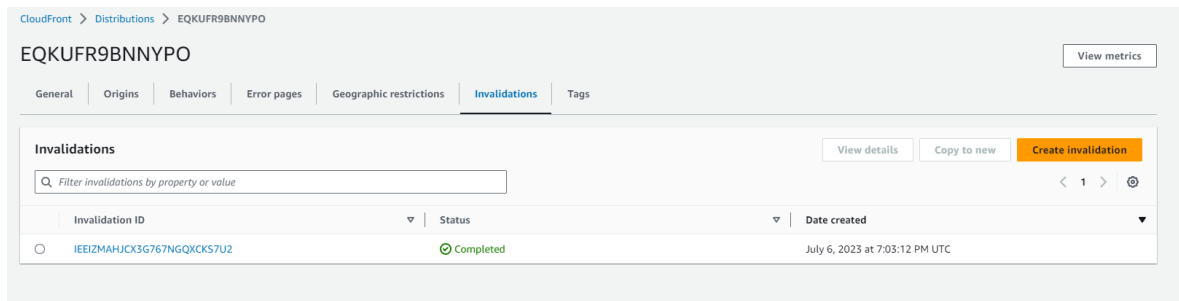
[Create staging distribution](#)

En la opción Behaviors, esta el origen de los archivos en S3 con la redirección del tráfico http a https, de esta forma toda comunicación por la distribución es resuelta mediante protocolo https.



Para publicar una nueva versión es necesario invalidar la anterior, ya que cloudfront al ser un CDN, mantiene un caché con el contenido para acelerar su carga. Para desplegar una nueva versión debe cargarse el contenido en S3, entrar en la distribución y seleccionar la pestaña de invalidaciones.

En esta pestaña se puede crear una nueva invalidación.



Se puede purgar contenido específico, pero para mantener correctamente versionado el sistema se recomienda purgar desde la raíz "/".

Create invalidation

Object paths

Add object paths

Add the path for each object that you want to remove from the CloudFront cache. You can use wildcards (*).

```
/example/path/object1  
/example/path/object2  
/examplePathWithWildcard*
```

 To add object paths individually, use the [standard editor](#).

[Cancel](#)[Create invalidation](#)

Esta invalidación puede tardar unos 5 minutos.

S3 – bucket

El front end vive dentro de un bucket s3, el cual es de acceso público, ya que su contenido es el sitio web en sí, existen diferentes buckets, que incluyen el productivo anterior y los ambientes de QA

Amazon S3

▼ Instantánea de la cuenta

Actualización más reciente: 13 Jul 2023 por Storage Lens. Las métricas se generan cada 24 horas. [Más información](#)

Almacenamiento total

13.7 GB

Recuento de objetos

24,9 k

Tamaño medio de los objetos

575.6 KB

Puede habilitar las métricas avanzadas en la Configuración de "default-account-dashbord".

Buckets (9) Información

Los buckets son contenedores de datos almacenados en S3. [Más información](#)

Q







Buscar buckets por nombre

<

1

>

🔍

Nombre	Región de AWS	Acceso	Fecha de creación
cf-templates-1n8hnb4qbn0q-us-east-1	EE. UU. Este (Norte de Virginia) us-east-1	Los objetos pueden ser públicos	14 Oct 2021 4:52:58 PM -03
qa.removeolutions.com	EE. UU. Este (Norte de Virginia) us-east-1	 Público	18 Mar 2022 11:32:31 AM -03
remove-solution-temp	EE. UU. Este (Norte de Virginia) us-east-1	 Público	5 Jul 2023 6:57:48 PM -04
removeapp-logs	EE. UU. Este (Norte de Virginia) us-east-1	Bucket y objetos que no son públicos	22 Mar 2022 11:56:18 AM -03
removeapp-prod	EE. UU. Este (Norte de Virginia) us-east-1	 Público	16 Jun 2023 3:27:21 PM -04
removedevs3-0000	EE. UU. Este (Norte de Virginia) us-east-1	 Público	6 Oct 2021 2:57:48 PM -03
removefilearchive	EE. UU. Este (Norte de Virginia) us-east-1	 Público	23 Nov 2021 4:00:10 PM -03
removefilearchive-prd	EE. UU. Este (Norte de Virginia) us-east-1	 Público	25 Mar 2022 2:11:26 PM -03
removesolutions.com	EE. UU. Este (Norte de Virginia) us-east-1	Público	25 Mar 2022 2:10:39 PM -03

En el caso del bucket del sitio productivo, se puede ver el contenido estático que corresponde al frontend. Para cargar nuevo contenido se puede hacer desde esta consola o mediante alguna herramienta SFTP con soporte s3 AWS.

Amazon S3 > Buckets > removeapp-prod

removeapp-prod

Información

Accesible públicamente

Objetos

Propiedades

Permisos

Métricas

Administración

Puntos de acceso

Objetos (545)

Los objetos son las entidades fundamentales que se almacenan en Amazon S3. Puede utilizar el [inventario de Amazon S3](#) para obtener una lista de todos los objetos de su bucket. Para que otras personas obtengan acceso a sus objetos, tendrá que concederles permisos de forma explícita. [Más información](#)

Copiar URI de S3

Copiar URL

Descargar

Abrir

Eliminar

Acciones

Crear carpeta

Cargar

Buscar objetos por prefijo

< 1 2 > ⌕


<input type="checkbox"/>	Nombre	Tipo	Última modificación	Tamaño	Clase de almacenamiento
<input type="checkbox"/>	3rdpartylicenses.txt	txt	6 Jul 2023 2:54:10 PM -04	122.4 KB	Estándar
<input type="checkbox"/>	4.1591baba2bb7bf8446e0.js	js	6 Jul 2023 2:54:11 PM -04	211.3 KB	Estándar
<input type="checkbox"/>	5.c4500601dd262bc241e3.js	js	6 Jul 2023 2:54:12 PM -04	17.6 KB	Estándar
<input type="checkbox"/>	ad.45026b922ec57f969a0a.svg	svg	6 Jul 2023 2:54:13 PM -04	32.7 KB	Estándar
<input type="checkbox"/>	ad.94e810253dbc84702e9a.svg	svg	6 Jul 2023 2:54:13 PM -04	31.5 KB	Estándar
<input type="checkbox"/>	ae.23c174705b39d649ba43.svg	svg	6 Jul 2023 2:54:15 PM -04	262.0 B	Estándar
<input type="checkbox"/>	ae.2c530f6449f3e5abd04b.svg	svg	6 Jul 2023 2:54:14 PM -04	254.0 B	Estándar
<input type="checkbox"/>	af.458ab7e0c32d14aefe33.svg	svg	6 Jul 2023 2:54:16 PM -04	20.6 KB	Estándar
<input type="checkbox"/>	af.867627c537fd29812532.svg	svg	6 Jul 2023 2:54:16 PM -04	20.4 KB	Estándar
<input type="checkbox"/>	ag.3f18bb58815f1eb37b60.svg	svg	6 Jul 2023 2:54:17 PM -04	761.0 B	Estándar
<input type="checkbox"/>	ag.5929ca9ff0f160f96fb5.svg	svg	6 Jul 2023 2:54:18 PM -04	749.0 B	Estándar
<input type="checkbox"/>	ai.546a12e334b3f4d8967c.svg	svg	6 Jul 2023 2:54:19 PM -04	47.1 KB	Estándar
<input type="checkbox"/>	ai.c4699001b99c1638c765.svg	svg	6 Jul 2023 2:54:19 PM -04	47.1 KB	Estándar

Una vez cargado el nuevo contenido y creada la invalidación, la nueva versión de frontend estará disponible.

Para que el bucket sea válido como distribución cloudfront debe agregarse la siguiente política de seguridad. Esto se puede hacer en la pestaña seguridad del bucket.

Información general sobre los permisos

Acceso




Bloquear acceso público (configuración del bucket)

Se concede acceso público a buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos de S3, active Bloquear todo acceso público. Esta configuración se aplica en exclusiva a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo acceso público pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que sus aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a sus buckets u objetos, puede personalizar los valores de configuración individuales a continuación para que se ajusten mejor a sus necesidades específicas de almacenamiento. [Más información](#)

Editar

Bloquear todo el acceso público

 Desactivado

► Configuración de bloqueo de acceso público individual para este bucket

Política de bucket

La política del bucket, escrita en JSON, proporciona acceso a los objetos almacenados en el bucket. Las políticas de bucket no se aplican a los objetos que pertenecen a otras cuentas. [Más información](#)

EditarEliminar

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1405592139000",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::removeapp-prod/*"
    }
  ]
}
```

Copiar

Bases de Datos

Las bases de datos son instancias RDS, basadas en PostgreSQL, existe una para cada ambiente.

Amazon RDS

Panel

Bases de datos

Editor de consultas

Información sobre rendimiento

Instantáneas de

Exportaciones en Amazon S3

Copias de seguridad automatizadas

Instancias reservadas

Proxies

Grupos de subredes

Grupos de parámetros

Grupos de opciones

Versiones de motor personalizadas

Integraciones sin extracción, transformación y carga (ETL)

Vista previa

Eventos

Suscripciones a eventos

Recomendaciones

Probar la nueva opción de implementación Multi-AZ de Amazon RDS para MySQL y PostgreSQL

For your Amazon RDS for MySQL and PostgreSQL workloads, improve transactional commit latencies by 2x, experience faster failover typically less than 35 seconds and, get read scalability with two readable standby DB instances by deploying the Multi-AZ DB cluster [Más información](#)

Crear base de datos

Or, Restore Multi-AZ DB Cluster from Snapshot

Recursos

Actualizar

Está usando los siguientes recursos de Amazon RDS en la región US East (N. Virginia) (usados/cuota).

Instancias de base de datos (2/40)

Almacenamiento asignado (0.3 TB/100 TB)

Aumentar el límite de instancias de base de datos

Clústeres de base de datos (0/40)

Instancias reservadas (0/40)

Instantáneas de (55)

Manual

Clúster de base de datos (0/100)

Instancia de base de datos (12/100)

Automatizado

Clúster de base de datos (0)

Instancia de base de datos (43)

Eventos recientes (27)

Suscripciones a eventos (0/20)

Grupos de parámetros (5)

Predeterminado (5)

Personalizada (0/100)

Grupos de opciones (3)

Predeterminado (3)

Personalizada (0/20)

Grupos de subredes (6/50)

Plataformas compatibles VPC

Red predeterminada vpc-0d163dc399b9ae709

Información adicional

Introducción a RDS

Información general y características

Documentación

Artículos y tutoriales

Guía de importación de datos para MySQL

Guía de importación de datos para Oracle

Guía de importación de datos para SQL Server

Anuncios de nuevas características de RDS

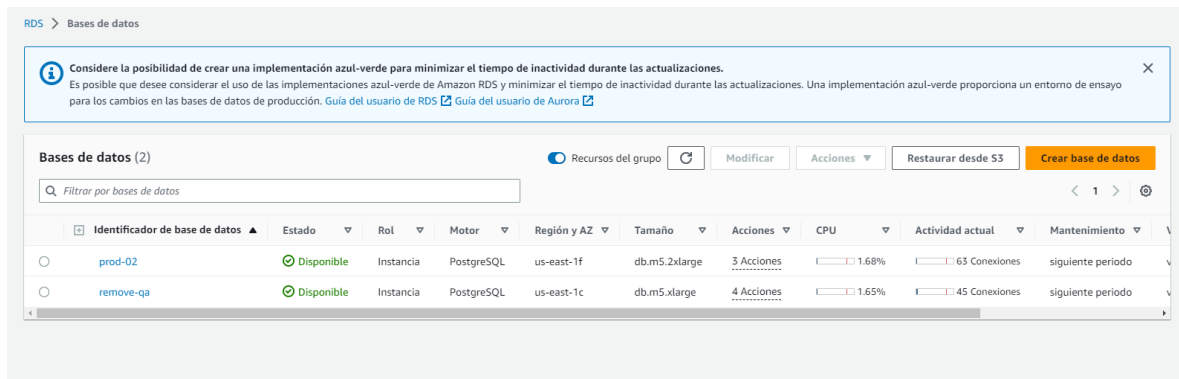
Precios

Foros

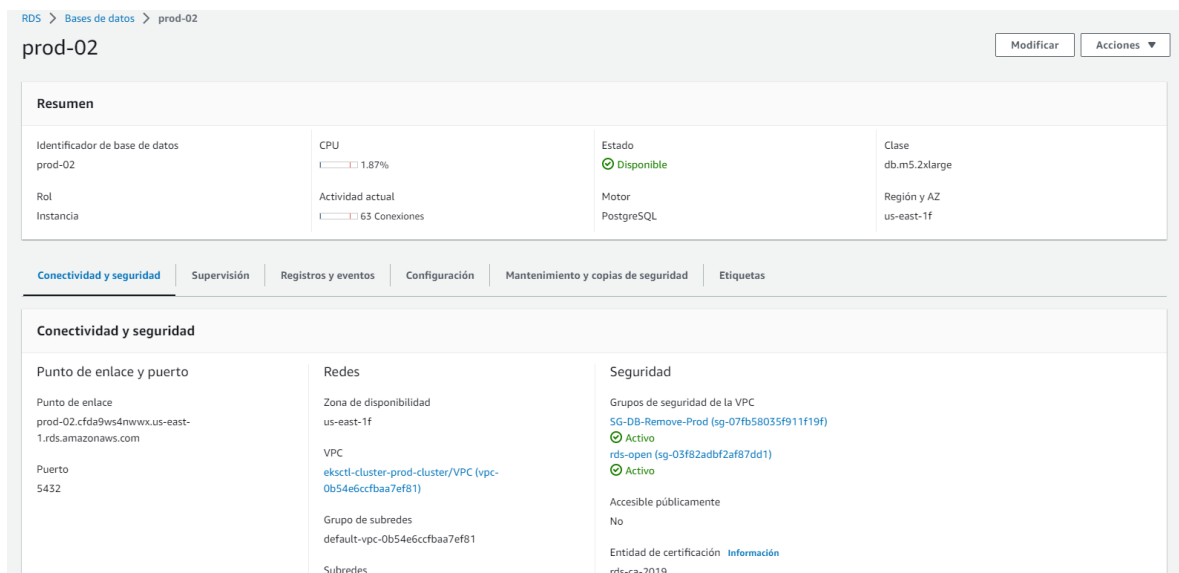
Database Preview Environment

Obtenga acceso anticipado a las nuevas versiones del motor de base de datos, antes de que estén disponibles de manera general. El entorno de vista previa de la base de datos de RDS permite trabajar con las próximas versiones beta, las candidatas a lanzamiento y las versiones de producción temprana de los motores PostgreSQL. Las instancias de entorno de vista previa son totalmente funcionales, por lo que puede

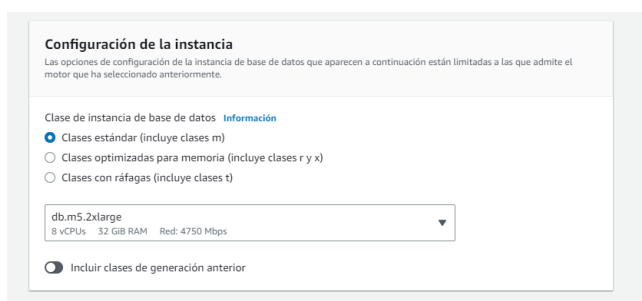
24 Documento de Arquitectura: Proyecto Remove



Están asociadas a una vpc específica.



En la siguiente imagen se puede revisar el hardware asociado a la instancia productiva actual



En la pestaña de mantenimiento, está el plan de respaldo asociado a la base de datos.

RDS > Bases de datos > prod-02

prod-02

Modificar Acciones

Resumen

Identificador de base de datos
prod-02

CPU
1.87%

Estado
Disponible

Clase
db.m5.2xlarge

Rol
Instancia

Actividad actual
61 Conexiones

Motor
PostgreSQL

Región y AZ
us-east-1f

Conectividad y seguridad

Supervisión

Registros y eventos

Configuración

Mantenimiento y copias de seguridad

Etiquetas

Mantenimiento

Actualización automática de la versión secundaria
Habilitado

Periodo de mantenimiento
July 14, 2023 23:00 - July 15, 2023 03:00 UTC-4

Mantenimiento pendiente
siguiente periodo

Modificaciones pendientes

En la sección inferior de esta pestaña se pueden ver los respaldos disponibles, si son manuales o automáticos y se puede realizar su restauración.

Filtrar por snapshots

< 1 2 > ⚙

<input type="checkbox"/>	Nombre de la instantánea	Hora de creación de la instantánea	Estado	Tipo de instantánea	Hora de la base de datos de la instantánea
<input type="checkbox"/>	backup17112022	November 17, 2022, 17:26 (UTC-03:00)	Disponible	Manual	-
<input type="checkbox"/>	prod-02-07-11-2022	November 07, 2022, 14:49 (UTC-03:00)	Disponible	Manual	-
<input type="checkbox"/>	prod-02-snapshot	November 17, 2022, 18:59 (UTC-03:00)	Disponible	Manual	-
<input type="checkbox"/>	rds:prod-02-2023-06-15-23-11	June 15, 2023, 19:11 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-16-23-10	June 16, 2023, 19:10 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-17-23-10	June 17, 2023, 19:10 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-18-23-11	June 18, 2023, 19:11 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-19-23-10	June 19, 2023, 19:10 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-20-23-10	June 20, 2023, 19:10 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-21-23-10	June 21, 2023, 19:10 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-22-23-10	June 22, 2023, 19:10 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-23-23-11	June 23, 2023, 19:11 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-24-23-11	June 24, 2023, 19:11 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-25-23-10	June 25, 2023, 19:10 (UTC-04:00)	Disponible	Automatizado	-
<input type="checkbox"/>	rds:prod-02-2023-06-26-23-11	June 26, 2023, 19:11 (UTC-04:00)	Disponible	Automatizado	-

Para cambiar la instancia de la BD y agregar o quitar hardware, hay que utilizar la opción modificar, esta acción tarda aprox 15 a 20 min, considerar eso si se desea aumentar las capacidades del servidor RDS.

Redes

En este punto, se re utilizó la infraestructura asociada a Kubernetes, que, si bien quedó obsoleto, su infraestructura fue reutilizada, para no generar incrementos en costo hundido de redes, pero en este punto se recomienda un proceso de limpieza.

Sus VPC (3) Información									
Find resources by attribute or tag									
<input type="checkbox"/>	Name	ID de la VPC	Estado	CIDR IPv4	CIDR IPv6	Conjunto de opción...	Tabla de enrutamiento ...		
<input type="checkbox"/>	Default	vpc-0d163dc399b9ae709	Available	172.31.0.0/16	-	dopt-0a8e5c19ae532ce82	rtb-04807fb8814a24337	ac	
<input type="checkbox"/>	eksctl-cluster-prod-cluster/VPC	vpc-0b54e6ccfbaa7ef81	Available	20.24.0.0/16	-	dopt-0a8e5c19ae532ce82	rtb-0b745e5b03d07e268	ac	
<input type="checkbox"/>	eksctl-cluster-dev-cluster/VPC	vpc-0ba0c20d6f262d95e	Available	16.20.0.0/16	-	dopt-0a8e5c19ae532ce82	rtb-08afaf2b8138736d5	ac	

Existen varias sub redes sin uso y lo mismo pasa con los grupos de seguridad.

Subredes (8) Información									
Filtrar subredes									
<input type="checkbox"/>	Name	ID de subred	Estado	VPC	CIDR IPv4	CIDR IPv6	Direcciones IPv4 disponibles		
<input type="checkbox"/>	eksctl-cluster-dev-c...	subnet-0c52ec97d0c632f4d	Available	vpc-0ba0c20d6f262d95e eks...	16.20.0.0/19	-	8183	us-e	
<input type="checkbox"/>	eksctl-cluster-prod-...	subnet-0db66156498d90144	Available	vpc-0b54e6ccfbaa7ef81 eks...	20.24.0.0/19	-	8183	us-e	
<input type="checkbox"/>	eksctl-cluster-dev-c...	subnet-00743b43434b9459d	Available	vpc-0ba0c20d6f262d95e eks...	16.20.96.0/19	-	8187	us-e	
<input type="checkbox"/>	eksctl-cluster-dev-c...	subnet-02c0e8278ffeb60eb	Available	vpc-0ba0c20d6f262d95e eks...	16.20.64.0/19	-	8186	us-e	
<input type="checkbox"/>	eksctl-cluster-dev-c...	subnet-0a5704d4848f4d44c	Available	vpc-0ba0c20d6f262d95e eks...	16.20.32.0/19	-	8185	us-e	
<input type="checkbox"/>	eksctl-cluster-prod-...	subnet-02500856350c4b294	Available	vpc-0b54e6ccfbaa7ef81 eks...	20.24.64.0/19	-	8186	us-e	
<input type="checkbox"/>	eksctl-cluster-prod-...	subnet-0717d7398661decce	Available	vpc-0b54e6ccfbaa7ef81 eks...	20.24.96.0/19	-	8187	us-e	

Grupos de seguridad (21) Información									
Filtrar grupos de seguridad									
<input type="checkbox"/>	Name	ID del grupo de segu...	Nombre del grupo ...	ID de la VPC	Descripción	Propietario	Número de reglas d...	Número de reglas d...	
<input type="checkbox"/>	-	sg-03f82adb2af87dd1	rds-open	vpc-0b54e6ccfbaa7ef81	security group abierto ...	253021683072	2 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	eks-cluster-sg-clust...	sg-0ca99cd752de180fa	eks-cluster-sg-cluster-...	vpc-0b54e6ccfbaa7ef81	EKS created security gr...	253021683072	1 Entrada de permiso	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-09fc50089904548b3	launch-wizard-1	vpc-0b54e6ccfbaa7ef81	launch-wizard-1 create...	253021683072	1 Entrada de permiso	1 Entrada de permiso	
<input type="checkbox"/>	eks-cluster-sg-clust...	sg-0a3cd73c1e5284479	eks-cluster-sg-cluster-...	vpc-0ba0c20d6f262d95e	EKS created security gr...	253021683072	1 Entrada de permiso	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-0c324c2d4a752535	k8s-traffic-clusterprod...	vpc-0b54e6ccfbaa7ef81	[k8s] Shared Backend ...	253021683072	0 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-053b73fc703849edd	k8s-traffic-clusterdev...	vpc-0ba0c20d6f262d95e	[k8s] Shared Backend ...	253021683072	0 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-0ed1d8404c7f63939	default	vpc-0ba0c20d6f262d95e	default VPC security gr...	253021683072	2 Entradas de permisos	2 Entradas de permiso	
<input type="checkbox"/>	-	sg-0d3b05a57acfe310c	k8s-removepr-backen...	vpc-0b54e6ccfbaa7ef81	[k8s] Managed Securit...	253021683072	2 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-07fb58035f911f19f	SG-DB-Remove-Prod	vpc-0b54e6ccfbaa7ef81	Created by RDS manag...	253021683072	7 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-00e2ce65ac666f87d	k8s-remove-de-backen...	vpc-0ba0c20d6f262d95e	[k8s] Managed Securit...	253021683072	2 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-09e3ecd6cb5394023	launch-wizard-3	vpc-0ba0c20d6f262d95e	launch-wizard-3 create...	253021683072	1 Entrada de permiso	1 Entrada de permiso	
<input type="checkbox"/>	eksctl-cluster-prod-...	sg-0bd55b150ee24a5f2	eksctl-cluster-prod-clu...	vpc-0b54e6ccfbaa7ef81	Communication betwe...	253021683072	0 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-001cb3ce64c17f638	default	vpc-0b54e6ccfbaa7ef81	default VPC security gr...	253021683072	2 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-009413c0597b3695e	launch-wizard-2	vpc-0ba0c20d6f262d95e	launch-wizard-2 create...	253021683072	1 Entrada de permiso	1 Entrada de permiso	
<input type="checkbox"/>	eksctl-cluster-dev-c...	sg-01d6d2e53d548a1bf	eksctl-cluster-dev-clus...	vpc-0ba0c20d6f262d95e	Communication betwe...	253021683072	0 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	eksctl-cluster-dev-...	sg-0c609f7b1dad986a2	eksctl-cluster-dev-nod...	vpc-0ba0c20d6f262d95e	Allow SSH access	253021683072	1 Entrada de permiso	1 Entrada de permiso	
<input type="checkbox"/>	eksctl-cluster-prod-...	sg-0eb320a2378661a0d	eksctl-cluster-prod-no...	vpc-0b54e6ccfbaa7ef81	Allow SSH access	253021683072	1 Entrada de permiso	1 Entrada de permiso	
<input type="checkbox"/>	eksctl-cluster-prod-...	sg-0917650bede9050a	eksctl-cluster-prod-clu...	vpc-0b54e6ccfbaa7ef81	Communication betwe...	253021683072	2 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	SG-BD-Remove-Dev	sg-02972ab7dfda8a8e	SG-BD-remove-Dev	vpc-0ba0c20d6f262d95e	Created by RDS manag...	253021683072	7 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	-	sg-0741cf72536343f6	default	vpc-0d163dc399b9ae709	default VPC security gr...	253021683072	0 Entradas de permisos	1 Entrada de permiso	
<input type="checkbox"/>	eksctl-cluster-dev-c...	sg-0700dbd68348d177b	eksctl-cluster-dev-clus...	vpc-0ba0c20d6f262d95e	Communication betwe...	253021683072	2 Entradas de permisos	1 Entrada de permiso	

Si bien esto no afecta a ningún artefacto y no genera impacto a nivel de software, si hace más compleja la administración y no se ha levantado, es esta instancia de consultoría la topología de red asociada al cloud en general. Si bien no genera impacto económico en la plataforma, ya que su costo es despreciable, si ordenar esto tendrá un ahorro en el largo plazo.

Alta Disponibilidad.

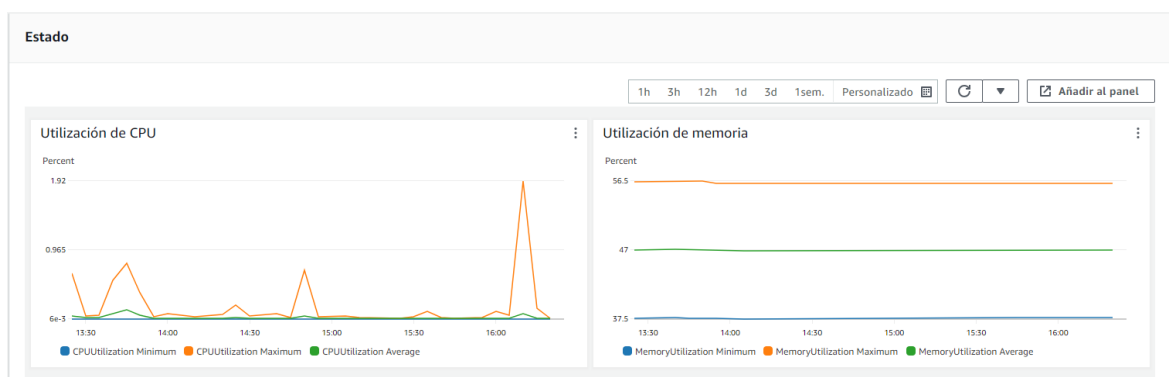
Fargate por si mismo ofrece alta disponibilidad, y en el caso del backend se tienen 2 instancias ejecutando en sub-redes que corren en zonas de disponibilidad distinta.

Cada instancia tiene el siguiente hardware asociado.

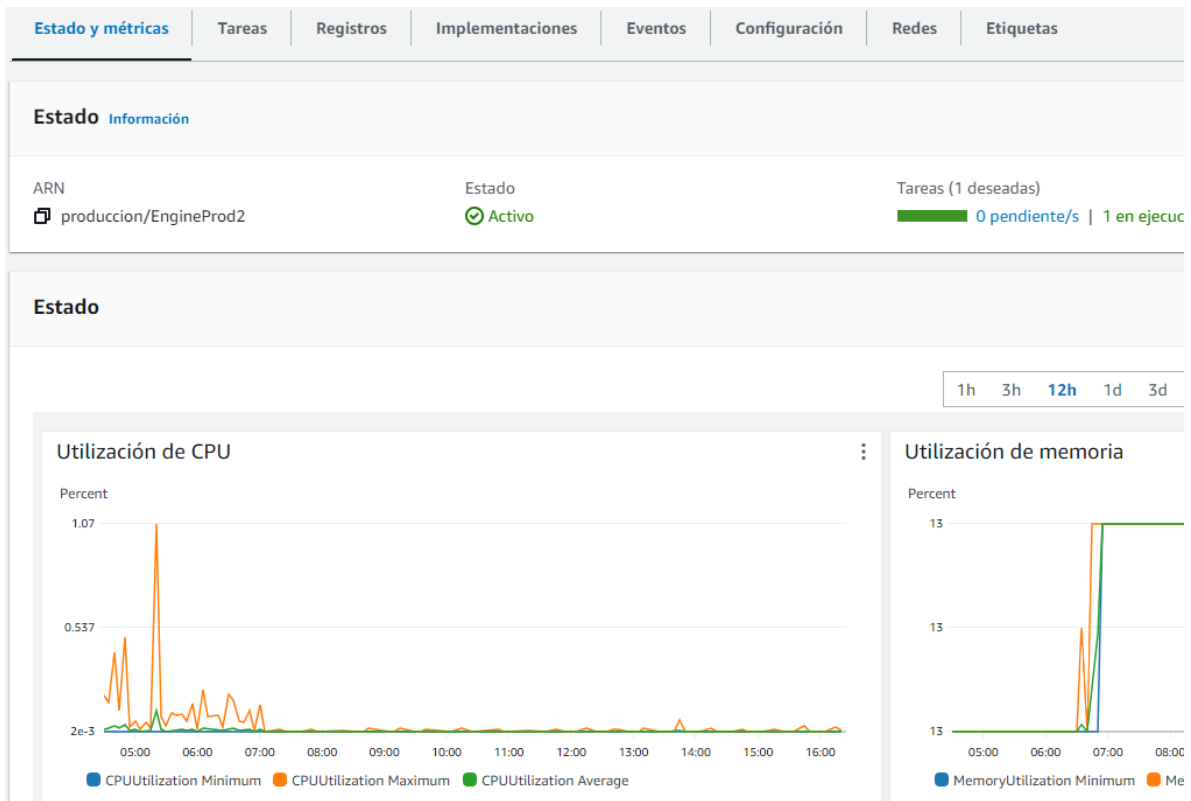
Configuración			
Sistema operativo/arquitectura Linux/X86_64	Proveedor de capacidad FARGATE	ID de ENI eni-094fac535e8032f51	IP pública 54.145.180.166 dirección abierta
CPU Memoria 4 vCPU 8 GB	Tipo de lanzamiento FARGATE	Modo de red awsipc	IP privada 20.24.11.56
Versión de la plataforma 1.4.0	Definición de tarea revomeProd:1	ID de subred subnet-0db66156498d90144	Dirección MAC 0a:52:9a:80:28:71
	Grupo de tareas service:removeProd		

Este hardware puede ser modificado en la definición de tarea, si bien esta solución no es serverless por definición, todo este hardware es administrado directamente por AWS y es transparente a la solución.

En el contexto actual este es el estado de salud de un contenedor, no se llega al 60% de ram y la cpu no tiene carga excesiva.



En el caso del Engine, se puede ver el peak de la ejecución de los scanner y ver su comportamiento como contenedor



Este es su Hardware asociado

Configuración			
Sistema operativo/arquitectura Linux/X86_64	Proveedor de capacidad FARGATE	ID de ENI eni-0b32d0aa331ad6ba0	IP pública ☐ 18.206.13.184 dirección abierta
CPU Memoria 8 vCPU 32 GB	Tipo de lanzamiento FARGATE	Modo de red awsipc	IP privada ☐ 20.24.44.234
Versión de la plataforma 1.4.0	Definición de tarea Engine-prod:2	ID de subred subnet-0cc61e143d0f4ae59	Dirección MAC ☐ 16:2b:a5:72:3e:9d
	Grupo de tareas service:EngineProd2		

Como se puede ver, el contenedor asociado al escáner es mucho mayor, ya que no se espera que pueda ejecutarse múltiples instancias de él, pero en el caso del backend se pueden lanzar múltiples instancias de servicio que serán organizadas por el balanceador de carga.

Escalamiento

En este momento el escalamiento es manual, considerando dos instancias de servicio backend. Estas pueden ser modificadas desde la opción actualizar servicio.

Actualizar removeProd [Información](#)

Configuración de implementación

☐ Forzar una nueva implementación

Definición de tarea

Seleccione una definición de tarea existente. Para crear una nueva definición de tarea, vaya a [Definiciones de tareas](#).

☐ Especificar la revisión manualmente

Ingrese manualmente la revisión en lugar de elegir entre las 100 revisiones más recientes para la familia de definición de tareas seleccionada.

Familia

revomeProd ▼

Revisión

1 (MÁS RECIENTE) ▼

Tipo de servicio

REPLICA

Tareas deseadas

Especifique el número de tareas que se van a lanzar.

2

Porcentaje de cantidad mín. de tareas en ejecución [Información](#)

Especifica el porcentaje mínimo de tareas en ejecución permitidas durante el despliegue de un servicio.

100

valores en %

Porcentaje de cantidad máx. de tareas en ejecución [Información](#)

Especifica el porcentaje máximo de tareas en ejecución permitidas durante el despliegue de un servicio.

200

valores en %

En caso de ser necesario se puede activar el servicio de auto escalado

▼ **Escalado automático de servicios - *opcional***

Ajuste automáticamente el recuento deseado del servicio hacia arriba y hacia abajo dentro de un rango especificado en respuesta a las alarmas de CloudWatch. Puede modificar la configuración del escalado automático de servicios en cualquier momento para satisfacer las necesidades de la aplicación.

☐ Utilizar el escalado automático del servicio

Configurar el escalado automático de servicios para ajustar el recuento deseado del servicio

Este servicio mide como parámetros CPU, tps y memoria para definir si lanzar o eliminar instancias de contenedores en el servicio.

Sugerencias.

Si bien la plataforma en este momento tiene un alto grado de estabilidad y su despliegue se ha visto normalizado, se sugiere avanzar en los siguientes puntos.

- Integración continua: Actualmente, no existen pipelines o automatizaciones de pruebas de calidad y seguridad en el desarrollo y el despliegue hasta ECR es manual, se propone iniciar la construcción de pipelines y automatizaciones que mejoren el estándar de desarrollo y mejoren TTL de las nuevas versiones, reduciendo el impacto de nuevas versiones en producción y generando nuevas funcionalidades más rápido.
- WAF: Si bien la seguridad general básica de AWS es bastante buena, frente a ataques dirigidos o de mayor complejidad se sugiere proteger los artefactos con la implementación de un WAF.
Se propone hacer un estudio de seguridad, para evaluar todas las opciones con sus respectivos costos, compatibilidad y viabilidad.
- Limpieza de Redes: Este punto ya se mencionó, pero se deja en este listado para su consideración.
- Monitoreo y Alertas: En este momento no existen notificaciones de caída de servicio o similares.
- Refactor de componentes: Si bien este documento está enfocado en la solución cloud, se sugiere romper el backend monolito y visualizar la posibilidad de una arquitectura en microservicios; con la finalidad de a futuro optimizar a infraestructura donde se encuentra el proyecto.