Sección:

Seguridad y Privacidad de Datos en la Nube

Por /in/lucastrubiano/

¿Qué veremos?

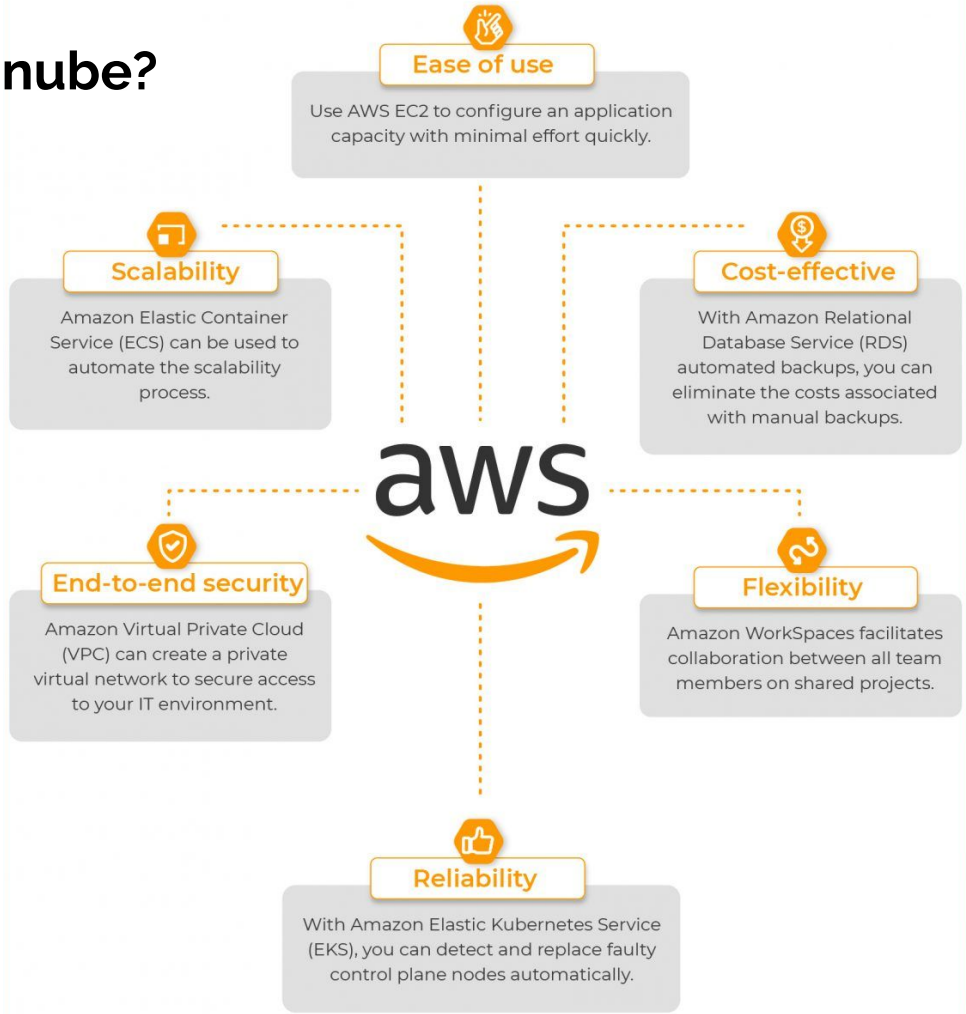
1. ¿Por qué la nube? AWS. Compliance y normativas.

2. Modelo de responsabilidad compartida.

3. Herramientas de seguridad en AWS:
   - IAM (Gestionar usuarios, roles y permisos).
   - Security Groups y NACLs (Para controlar el tráfico hacia y desde los recursos).
   - LakeFormation (Para controlar acceso a nuestros datos).
   - AWS CloudWatch vs CloudTrail (Para auditar y monitorear actividades en la cuenta).

4. Demostraciones prácticas.

1. ¿Por qué la nube?



1. ¿Por qué la nube? AWS

Liderazgo en el Mercado

- Dominio en la industria.
- Amplia base de clientes.

Innovación y Desarrollo Continuo

- Ritmo de innovación.
- Compromiso con la investigación.

Infraestructura Global

- Presencia global.
- Resiliencia y disponibilidad.

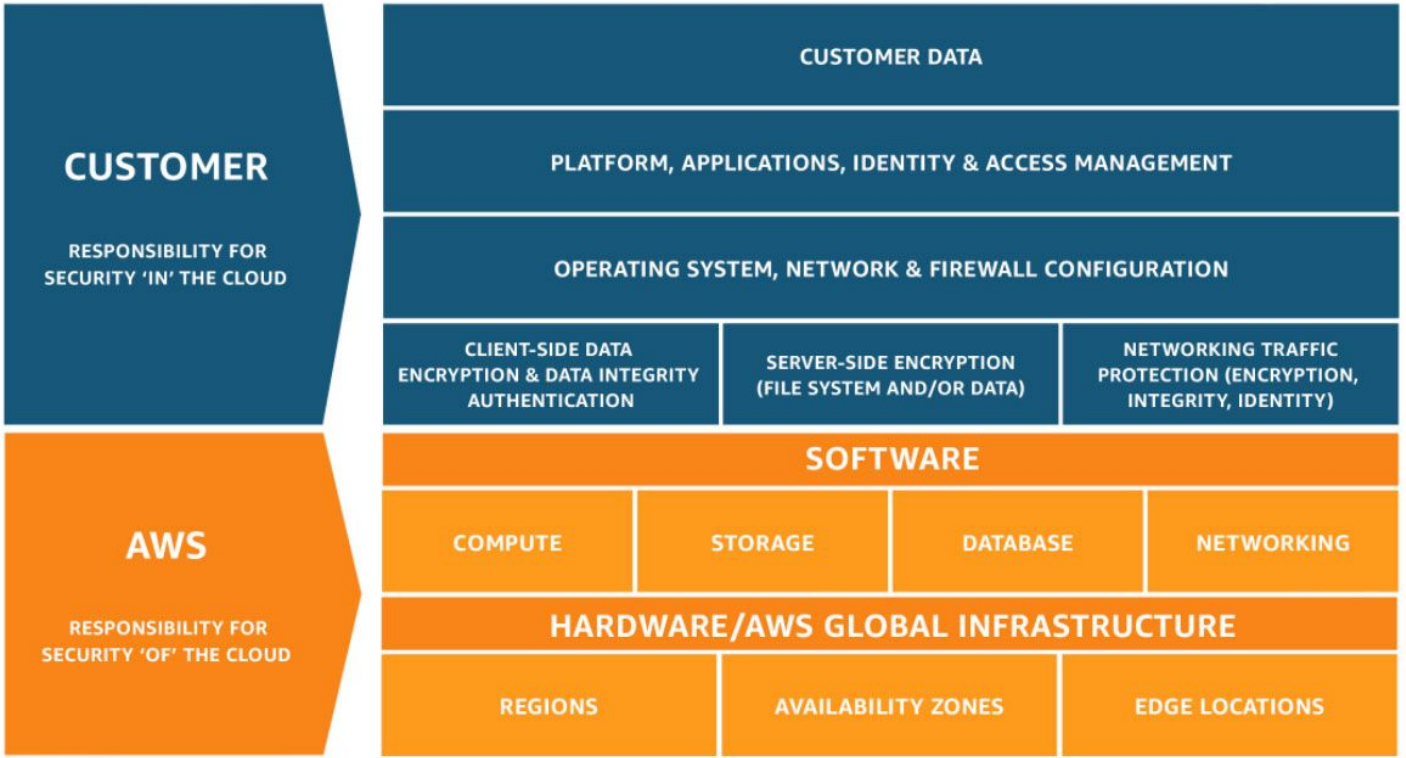
Seguridad y Cumplimiento

- Seguridad en capas.
- Cumplimiento normativo. ISO 27001, HIPAA, FedRAMP, y GDPR

Ecosistema y Comunidad

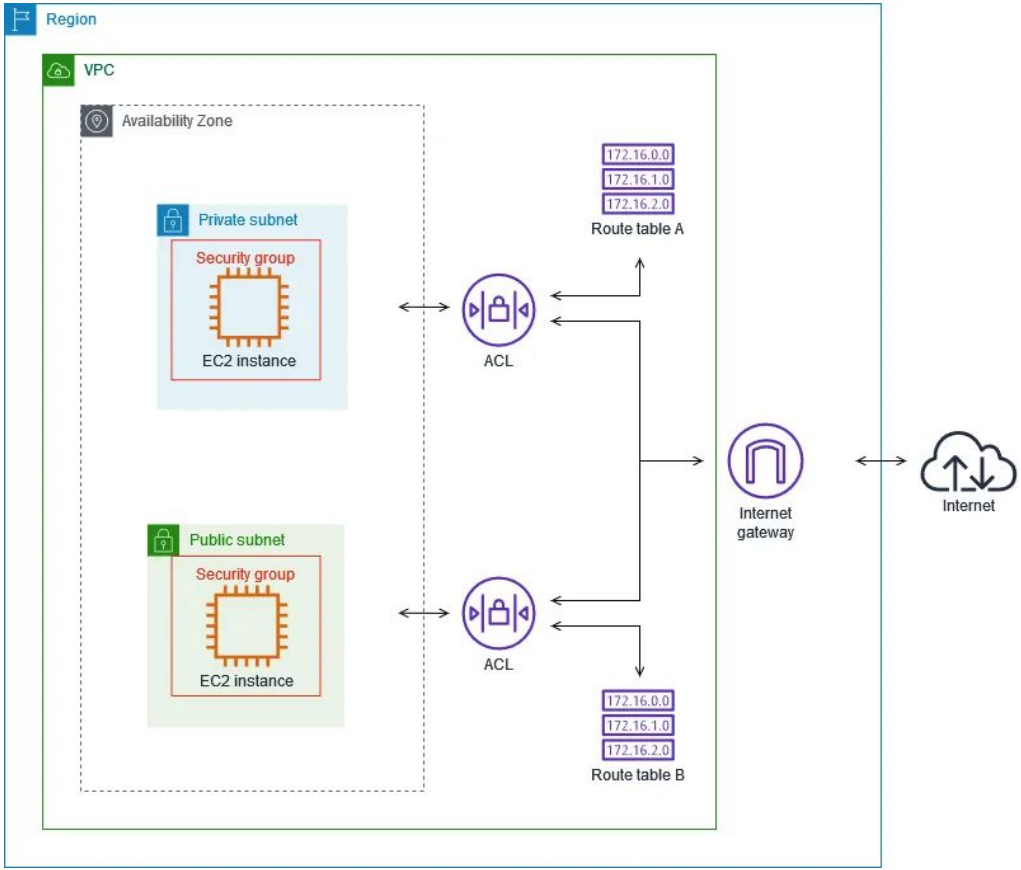
- Marketplace y socios.
- Soporte comunitario y educativo.

2. Modelo de responsabilidad compartida.



3. Herramientas de Seguridad en Amazon | IAM

3. Herramientas de Seguridad en Amazon | Security Groups. NACLs

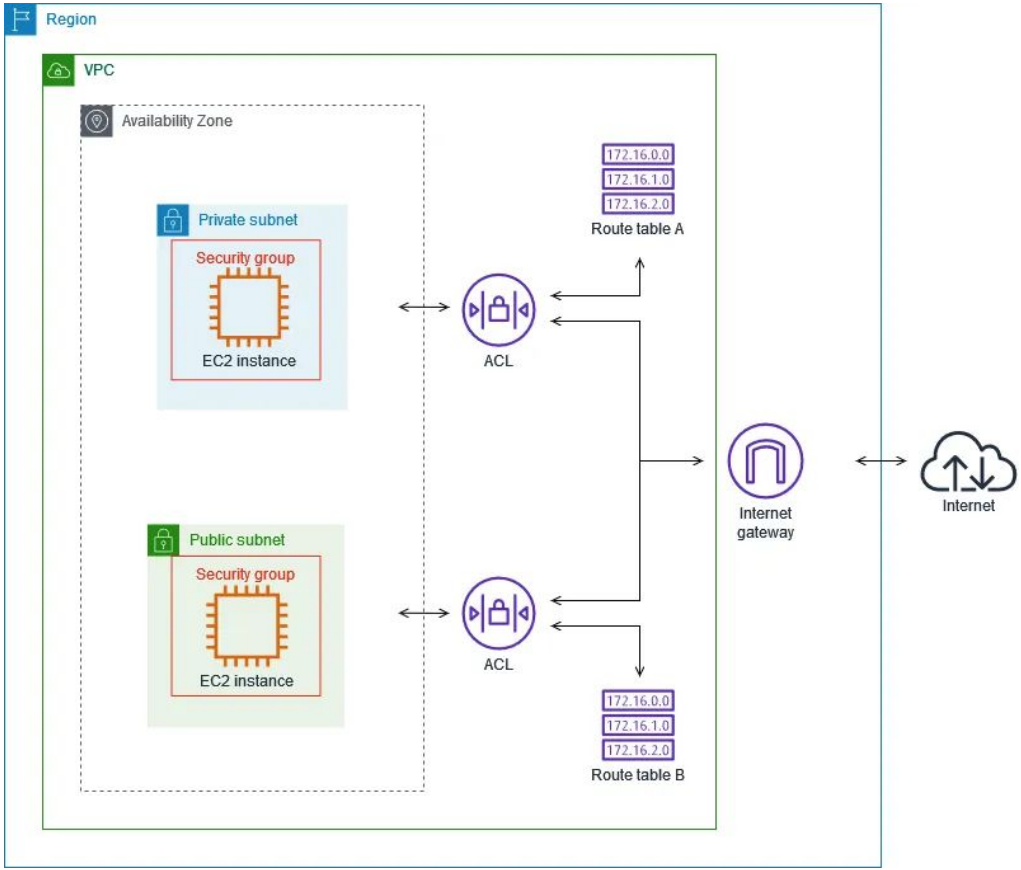


Alcance: Subred o Instancia (dónde aplicar)

Los **Grupos de Seguridad** operan a nivel de Instancia (Interfaz de Red). El Grupo de Seguridad debe asignarse explícitamente a la instancia.

ACL de Red a nivel de subred. Se aplica automáticamente a todas las instancias desplegadas en la subred asociada.

3. Herramientas de Seguridad en Amazon | Security Groups. NACLs

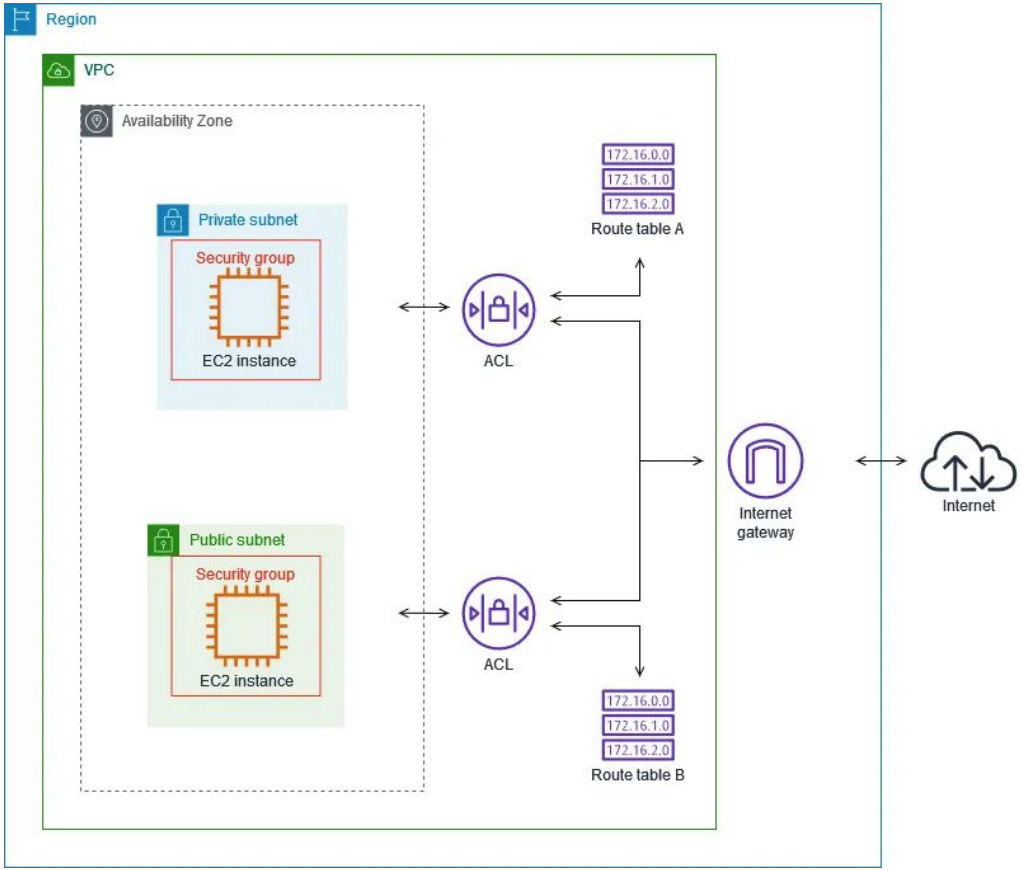


Estado: Con estado o Sin estado

Los **grupos de seguridad** son con estado. El tráfico de retorno está permitido, independientemente de las reglas.
Por ejemplo, si permites un tráfico entrante en el puerto 80, el tráfico saliente en el puerto 80 también será automáticamente permitido.

Las **ACL** de red son sin estado. El tráfico de retorno debe ser explícitamente permitido por las reglas. Esto significa que cualquier cambio aplicado a una regla entrante no se aplicará a la regla saliente. Si permites un puerto entrante 80, también necesitarás aplicar la regla para el tráfico saliente.

3. Herramientas de Seguridad en Amazon | Security Groups. NACLs

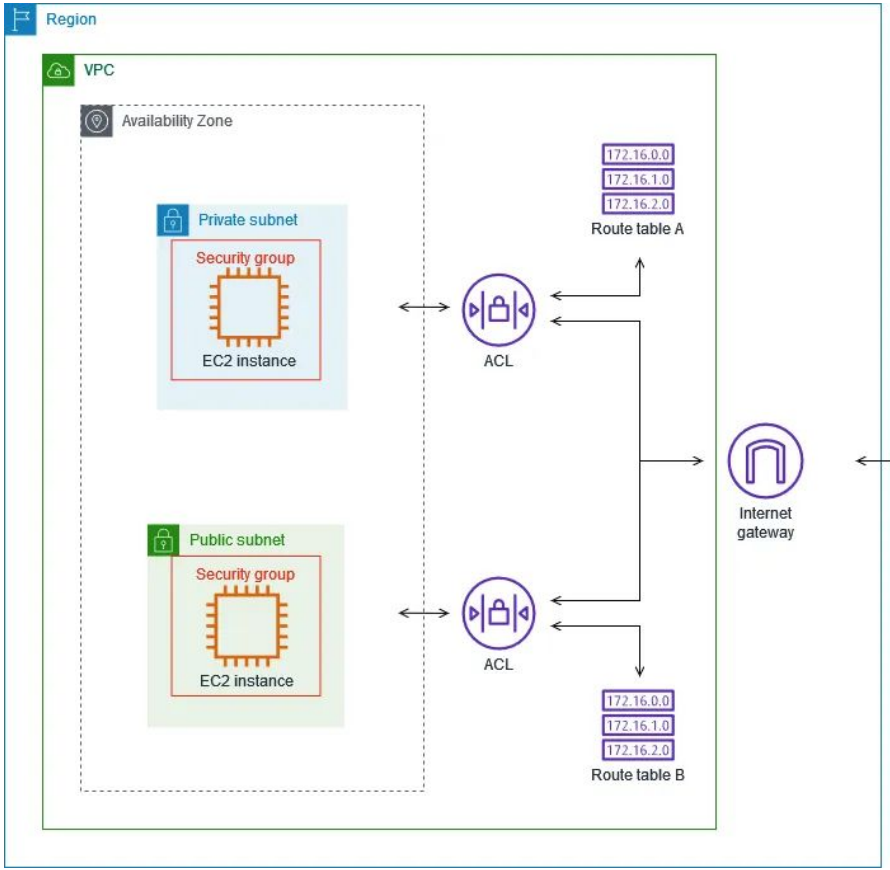


Tipo de Regla: Permitir o Denegar

El **grupo de seguridad** solo admite reglas de permitir (todo lo demás se deniega implícitamente). Puedes especificar reglas de permitir, pero no de denegar.
Por ejemplo, no puedes denegar a una cierta dirección IP establecer una conexión.

La **ACL** de red admite reglas de permitir y de denegar.
Por ejemplo, con reglas de denegar, podrías denegar explícitamente a una cierta dirección IP establecer una conexión con una instancia EC2.

3. Herramientas de Seguridad en Amazon | Security Groups. NACLs

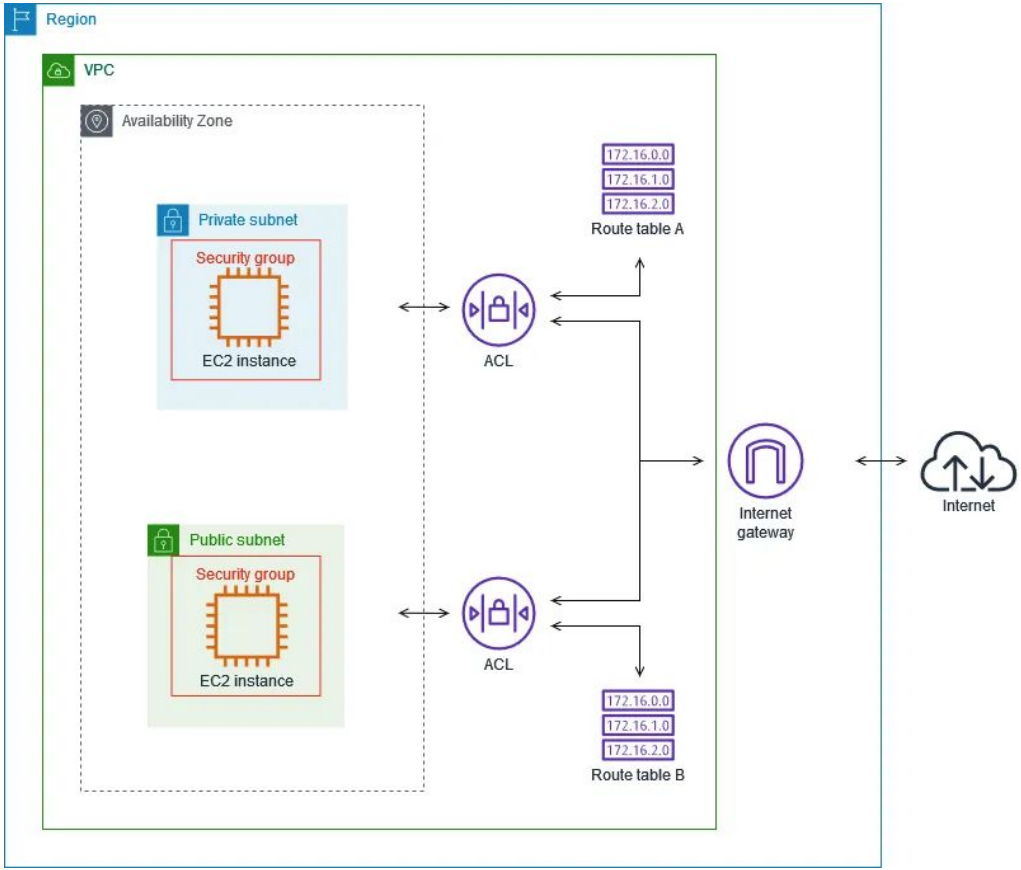


Destino de la Regla

La regla del **grupo de seguridad** permite CIDR, IP y Grupo de Seguridad como destinos.

La regla de la **ACL** de red sólo permite CIDR como destino.

3. Herramientas de Seguridad en Amazon | Security Groups. NACLs

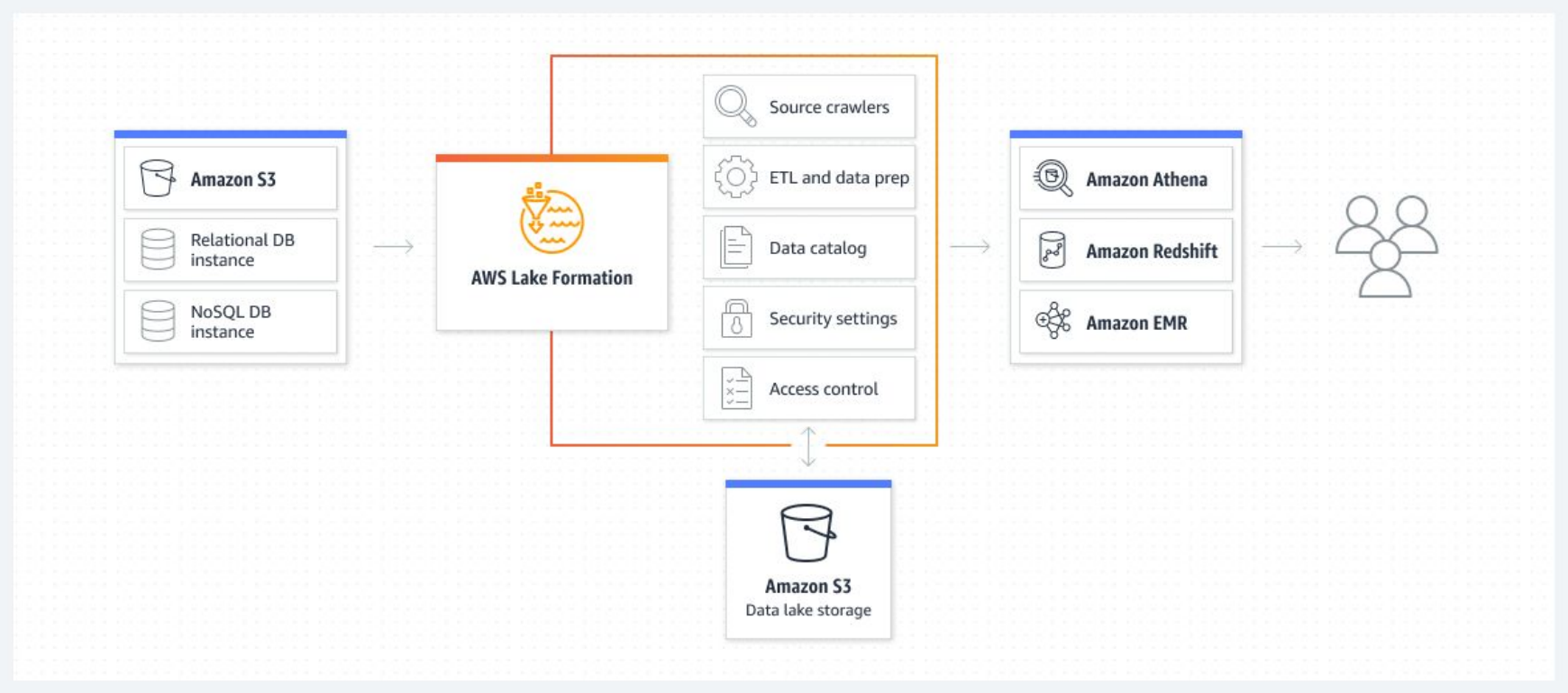


Orden de defensa

El **grupo de seguridad** es la primera capa de defensa, mientras que la ACL de red es la segunda capa de defensa para el tráfico saliente/egreso.

La **ACL** de red es la primera capa de defensa, mientras que el grupo de seguridad es la segunda capa de defensa para el tráfico entrante/ingreso.

3. Herramientas de Seguridad en Amazon | Lake Formation



https://docs.aws.amazon.com/es_es/lake-formation/latest/dg/lf-permissions-reference.html
https://docs.aws.amazon.com/es_es/lake-formation/latest/dg/tut-grant-data-permissions.html

3. Herramientas de Seguridad en Amazon | CloudTrail

La diferencia entre AWS CloudWatch y CloudTrail

AWS **CloudWatch** monitorea tus recursos y aplicaciones en AWS, mientras que **CloudTrail** monitorea la actividad en tu entorno de AWS. Por ejemplo, con CloudWatch, puedes escalar tus aplicaciones, mientras que con CloudTrail, puedes ver quién hizo qué en tus aplicaciones y podrías encontrar problemas. No son mutuamente excluyentes, y puedes configurar CloudTrail para enviar eventos a un log de CloudWatch, por ejemplo.

Nota:

CloudWatch monitorea el **rendimiento**.

CloudTrail monitorea las **acciones** en tu entorno de AWS.

4. Demostraciones Prácticas

¡Muchas Gracias!

Preguntas