Presionar el título de cada tema para ver su contenido

Protección de las bases de datos de Amazon RDS

Recomendaciones

Ejecute la instancia de RDS en una nube privada virtual (VPC).

- Proporciona aislamiento de servicios y protección de firewall de IP.

Utilice las políticas de AWS Identity and Access Management (IAM) para la autenticación y el acceso.

- Los permisos determinan quién puede administrar los recursos de Amazon RDS.

Utilice grupos de seguridad para controlar qué direcciones IP o instancias EC2 pueden conectarse a sus bases de datos.

- De forma predeterminada, el acceso a la red está desactivado.

Utilice la capa de conexión segura (SSL) para el cifrado de tránsito.

Utilice el cifrado de Amazon RDS en instancias de base de datos e instantáneas para proteger los datos en reposo.

Utilice las características de seguridad del motor de base de datos para controlar quién puede iniciar sesión en las bases de datos de una instancia de base de datos.

Configure notificaciones de eventos para que se le informe cuando se produzcan eventos importante de Amazon RDS.

Protección de Amazon DynamoDB

Recomendaciones

Utilice los roles de IAM para autenticar el acceso

Utilice las políticas de IAM

- Para definir permisos de acceso detallados para usar API de DynamoDB
- Defina el acceso a nivel de tablas, elementos o atributos
- Siga el principio de concesión de privilegios mínimos

Configure puntos de enlace de la VPC

- Evita que el tráfico de conexión atraviese la Internet abierta
- Las políticas del punto de enlace de la VPC le permiten controlar y limitar el acceso de las API a una tabla de DynamoDB

Considere usar cifrado del lado del cliente.

- Cifre datos lo más cerca posible de su origen.

Seguridad proporcionada de forma predeterminada.

- Cifrado en reposo de todos los datos del usuario almacenados en tablas, índices, secuencias y copias de seguridad
- Cifrado en tránsito: todas la comunicaciones hacia y desde DynamoDB y otros recursos de AWS utilizan HTTPS

Protección de las bases de datos de Amazon RDS

La seguridad es una tarea compartida entre AWS y usted como usuario. AWS se encarga de la seguridad de la infraestructura en la nube, lo que implica proteger la infraestructura que soporta Amazon RDS. Por otro lado, usted es responsable de la seguridad en la nube.

Una práctica de seguridad recomendada para Amazon RDS es ejecutar las instancias en una Red Virtual Privada (VPC). La VPC permite colocar la instancia en una subred privada, lo que la protege de accesos desde Internet público. Además, la VPC proporciona un firewall IP que le permite controlar de manera segura la configuración de la red.

Además, se recomienda lo siguiente:

- Utilizar las políticas de IAM de AWS para gestionar la autenticación y controlar el acceso.
- Configurar grupos de seguridad para restringir las conexiones. Es importante abrir el puerto TCP para acceder a la base de datos, pero también es fundamental limitar desde dónde pueden originarse esas conexiones.
- Usar conexiones SSL para garantizar que todas las comunicaciones hacia y desde la base de datos estén encriptadas.
- Aplicar el cifrado de Amazon RDS para proteger los datos y las instantáneas de la base de datos.
- Aprovechar las funciones de seguridad proporcionadas por el motor de base de datos, como imponer políticas de complejidad para las contraseñas.
- Habilitar notificaciones para eventos importantes que ocurran en la instancia de RDS. Estos eventos pueden incluir cierres de instancia, inicio de copias de seguridad, conmutaciones por error, cambios en los grupos de seguridad o escasez de espacio de almacenamiento.

Página inicial

Protección de
Amazon DynamoDB

Para proteger Amazon DynamoDB, también se aplican muchas de las mismas prácticas recomendadas que debe utilizar para proteger Amazon RDS.

Por ejemplo, utilice los roles de IAM para proteger la autenticación y utilice las políticas de IAM para definir permisos de acceso.

Si solo necesita acceder a DynamoDB desde una nube privada virtual (VPC), debe utilizar un punto de enlace de la VPC para que solo se pueda acceder desde la VPC requerida. De este modo, se impide que el tráfico atraviese una red de Internet de acceso público y se someta a ese entorno.

Además, si almacena datos confidenciales o delicados en DynamoDB, es buena idea cifrar los datos lo más cerca posible de su origen de modo que sus datos estén protegidos a lo largo de su ciclo de vida.

Tenga en cuenta que DynamoDB proporciona ciertas características de seguridad de forma predeterminada. Por ejemplo, DynamoDB protege los datos del usuario almacenados en reposo y también los datos en tránsito entre clientes en las instalaciones y DynamoDB, y entre DynamoDB y otros recursos de AWS dentro de la misma región de AWS.

Lea la documentación de Prácticas recomendadas sobre seguridad de DynamoDB para obtener más detalles.

Página inicial