DevOps Challenge.

1) ¿Cómo expondrías tu aplicación a internet?

R= Configuraría servicios de AWS para poder exponer mi App por ejemplo, Route53, Application Load Balancer (Subnets Publicas). Con estos servicios podría darle mayor seguridad a la aplicación y al host donde vive dicha aplicación, así como no exponer la data almacenada en un servicio de BD.

2) ¿Qué utilizarías para escalar tu aplicación de manera dinámica?

R= Utilizaria AutoScaling Group para tener la ayuda extra de poder contar con la cantidad correcta de instancias EC2 que albergan mi app mediante un Launch configuration que tenga una AMI semilla la cual tendría toda la configuración requerida para la App.
De esta forma podría obtener los beneficios de tener una App en Alta disponibilidad por la configuración de este AutoScaling.

3) ¿Cómo le darías acceso a un desarrollador a la base de datos?

R= 3 opciones:

3.1 El acceso se puede hacer por medio de una VPN site-to site desde el on-premise donde solo pueda tener acceso al puerto en específico del RDS desde la IP origen, todo manejado desde un Security Group y dentro de la BD un usuario con permisos solo de reading.

3.2 AWS Client VPN para acceder de forma segura a los recursos de nuestra VPC, este cliente de VPN funciona mediante una Autenticación mutua la cual mediante certificados puede configurarse el acceso a la VPN y a los recursos. De igual forma dentro de la BD un usuario con permisos solo de reading.

3.3 Bastion, implementar un bastion con una EIP para que puedan tener acceso todo manejado por conexión SSH con par de llaves y con permisos muy específicos. (No optaría por esta opción, pero la pongo por que también puede ser valido)

Adicional para esta solución agregaría servicios adicionales como:

WAF: Para protección del balanceador basado en el OWASP de AWS
RDS: Multi AZ para realizar un tema de FailOver
NatGateway: Para que las instancias que estarán privadas puedan salir a internet y obtener parches de seguridad.
GuardDuty: Para tener una capa extra de seguridad y así poder detectar amenazas y tenerlas en cuenta para tener las actividades maliciosas dentro de la cuenta.

4) Realiza la v2 de la infraestructura como código para implementar estas mejoras.

Como posibles mejoras se pueden realizar las siguientes adecuaciones:

- Configuraciones apropiadas en Route 53.
- AWS WAF basado en el OWASP de AWS.
- Segmentar VPC en Subredes públicas y privadas.
- Application Load Balancer, Autoscaling Group
- RDS multi AZ.
- GuardDuty
- Github
- Terraform

El punto más importante es que utilizaría EKS para la aplicación de esta forma salimos un poco de las infraestructuras comunes de AWS pero sobre todo poder tener un servicio que facilite el manejo del desarrollo de nuestra App a través del propio desarrollo de contenedores y una plataforma de orquestación.
Donde también podeos tener un seguimiento correcto de auditoría de eks, seguridad mediante roles de iam.

*El siguiente diagrama muestra el diseño de la infraestructura original antes de realizar las mejoras.
*En mi código de terraform de igual forma se tiene el contenido de la infraestructura original.