Análisis y Mejora de Arquitectura para Vinotech

1. Análisis de Vulnerabilidades de Seguridad

- API pública sin WAF: riesgo de ataques como DDoS, SQLi o XSS.
- Bucket S3 público: posibilidad de exposición de datos sensibles.
- Secretos embebidos: fuga de credenciales.
- Gestión de usuarios sin MFA ni OAuth: autenticación débil.
- Roles IAM con permisos excesivos: acceso innecesario a servicios.

2. Evaluación de Componentes Costosos

- EC2 para recomendaciones corre 24/7 sin escalado: migrar a Lambda o Spot.
- ECS con escalado mal configurado: ajustar thresholds.
- RDS en modo on-demand: considerar instancias reservadas o Aurora Serverless.
- Tráfico de bots: añadir WAF con control de tasa y bloqueo de scraping.
- Recursos sin apagado nocturno: automatizar con EventBridge y Lambda.

3. Propuestas de Mejora en Seguridad

- Adoptar Amazon Cognito con MFA y OAuth2.
- Usar AWS Secrets Manager para gestión de secretos.
- Configurar WAF y Shield en servicios públicos.
- Aplicar principio de privilegio mínimo en IAM.

4. Herramientas para Control de Costos

- AWS Cost Explorer y Budgets para visibilidad.
- Trusted Advisor y Compute Optimizer para recomendaciones.

- Etiquetado de recursos por entorno (Dev, Prod, etc.).

5. Acciones Priorizadas

1. Quitar acceso público de S3.

2. Configurar WAF y proteger API.

3. Migrar secretos a Secrets Manager.

4. Implementar Cognito con MFA.

5. Optimizar uso de EC2 y RDS.

6. Automatizar apagado de recursos.

7. Aplicar tagging y seguimiento de costos.

Análisis y Mejora de Arquitectura para Vinotech

24 abil zel-2024

Análisis de Vulnerabilidades de Seguridad

Vulnerabilidad	Rlesgo	Reco mendacion
API publice eri WAF ni control de tráfiaa	Alto - Cricito - LAiilio IT-	Implementer AWS VVAF. Imitar rocubenatmente use API Garelway
Bucket ßo público sin restriceiores	Alto - Ríia --Criticito '	Ebĝua-e es rentilos de aWS Secrets Manager usa AWs Secreto Manager
Secretes embebidos en contervatorés	Alto - R/mlfo a aíno es mo	Úsar AWS Iferents Mans'get en heszas Magnra o udíhenás altromóltan e rahee)
Gostion do usuarios sin MFA al protocaluo estandar	Alto - 'Rilo - Réot comtilo	Aplicar a Ûemelpo de privíegie-mínimo, use (al J AF eli eus control
IAM con premops 'Administrado/Acces)	Critico - NHtro é'	- idopta (Amazon Cognito con MFA, OAuth2

Evaluación de Componentes Costosos

Componente	Problema	Costo Bd- nor (Acwlas	Altefnativó e Mejora.. j Mejora
ECZ o5 Marge (20/7)	Use consliante	S.EEI/ımesã	Implementa a Oĥá Lémo0a doat aímdh
ECS ñargate mal escalado	Sin instansae reuèano >	$ milló airon)	Ajusior es-sacling (hreóloldıes, cucear comonveero emabiles
RDS PostgreSQL on demand	Purchaloar ibreár dit	Metıór de a-- ãíío ui aimoro	Ustrat \/VAF een rate limitng y bot control

Diagramá de Arquitecturá Mejorada

- Adoptar Amazon Cognito con MFA y OAuth2
- Implementor AWS WAF

Diagrama de Arqutectura Mejorada