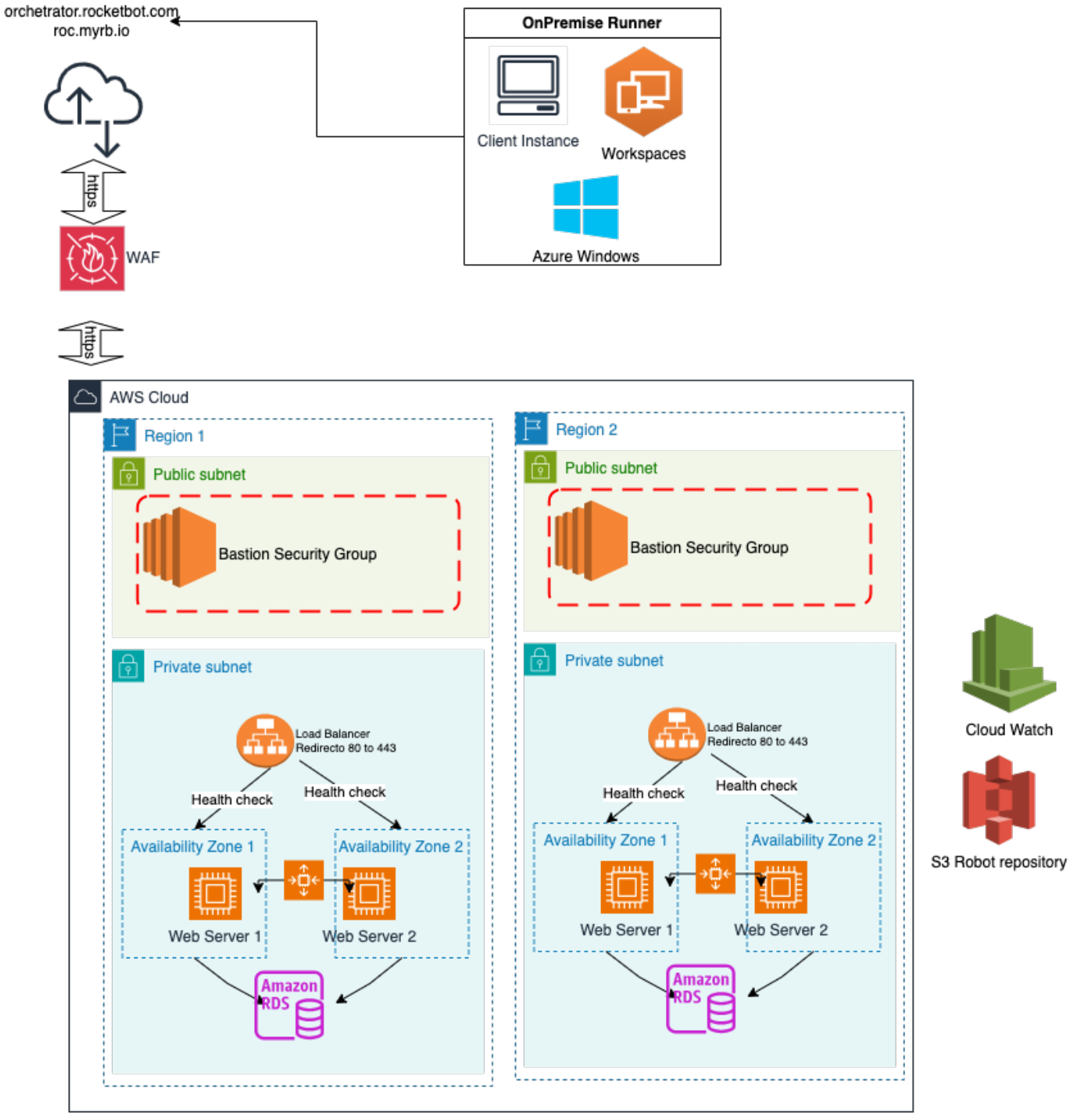
# Orquestador Rocketbot – R.O.C. Infraestructura

El Orquestador Rocketbot (R.O.C.) es un sistema SaaS web diseñado bajo una arquitectura escalable, resiliente y multiplataforma para su runner, aprovechando las distintas Availability Zones que ofrece AWS.

## Infraestructura de Rocketbot Orchestrator Center



## Base

- La infraestructura está diseñada para ser escalable y resiliente, aprovechando las distintas Availability Zones que ofrece AWS.
- Monitoreo constante de la utilización de recursos para poder escalar la infraestructura arriba o abajo según sea necesario.
- Amazon CloudWatch para monitorear la salud y el rendimiento de las instancias EC2, ELB y RDS.
- S3 para almacenar los robots encriptados.
- Conexión HTTPS / TLS 1.2.
- JWT en cabeceras.
- El sistema soporta multiplataforma para su runner, el Orquestador es un sistema SaaS.

## Load Balancer – WAF

- Tipo: Elastic Load Balancer (ELB)
- Configuración adicional: Web Application Firewall (WAF) para protección contra ataques comunes como SQL Injection, Cross-Site Scripting, etc.

## Instancias EC2

Estas instancias actuarán como los servidores de aplicaciones principales. Utilizar diferentes Availability Zones aumenta la resiliencia del sistema.

- Tipo: t3.small
- CPU: 2 vCPUs
- RAM: 2GB
- Cantidad: 2 instancias

## Base de Datos RDS

La base de datos RDS con configuración Multi-AZ asegura que la información esté siempre disponible, incluso si una zona de disponibilidad sufre un fallo. Para el Orquestador se utiliza Amazon RDS con motor MySQL, configurado en Multi-AZ para alta disponibilidad.

| Componente | Motor | Clase de Instancia | Especificaciones de Hardware | Configuración |
|---|---|---|---|---|
| **Base de Datos RDS** | MySQL | db.m5.2xlarge | 8 vCPUs y 32GB de RAM | Multi-AZ para alta disponibilidad |

# Seguridad, Integridad y Gestión de Vulnerabilidades

El Orquestador utiliza controles de seguridad e integridad para la comunicación entre componentes:

- La comunicación entre el Orquestador y las instancias/robots se realiza mediante canales cifrados HTTPS/TLS 1.2.
- El intercambio de datos está protegido mediante JWT, lo que permite validar la autenticidad e integridad de la sesión.
- El Orquestador cuenta con control de acceso basado en roles (RBAC), auditoría/logs de ejecución, logs del sistema y trazabilidad de acciones, lo que permite reducir riesgos de uso indebido, errores operativos y modificaciones no autorizadas.
- Para el Orquestador se implementan controles perimetrales y de defensa en capas como firewalls, servicios de detección y prevención de intrusiones, monitoreo de seguridad, controles de acceso, restricción de acceso público directo a componentes críticos y servicios de seguridad de infraestructura cloud como Amazon GuardDuty y AWS Security Hub.
- Rocketbot cuenta con un proceso formal de gestión de vulnerabilidades y mejora continua. Se realizan análisis de vulnerabilidades, seguimiento de hallazgos, planes de remediación priorizados por riesgo y pruebas de Ethical Hacking periódicas sobre componentes expuestos, incluyendo el Orquestador SaaS.

# Continuidad del Servicio y Control de Versiones

## Procedimientos de Respaldo (ISO 27001)

- Rocketbot mantiene procedimientos de respaldo para la información crítica del Orquestador, incluyendo base de datos, configuración y datos necesarios para la continuidad del servicio.
- Se realizan respaldos periódicos, retención definida y pruebas de restauración, declarado en nuestras políticas de la norma ISO27001.

## Repositorio Centralizado y Rollback

- El Orquestador actúa como repositorio centralizado de proyectos/robots.
- Al cargar o modificar proyectos, permite mantener versiones históricas y gestionar el despliegue de una versión específica.
- También contempla la posibilidad de rollback a versiones anteriores ante fallos en producción.

# Nomenclatura

- **SaaS:** Software as a Service (Software como Servicio) es un modelo de distribución de software donde el soporte y los datos se alojan en servidores de una compañía de tecnologías de la información y se accede a través de la web.
- **JWT:** JSON Web Token es un estándar abierto (RFC 7519) que define una forma compacta y autónoma para transmitir de forma segura información entre las partes como un objeto JSON. Más información: https://auth0.com/docs/jwt
- **TLS 1.2:** Transport Layer Security (TLS; en español seguridad de la capa de transporte) y su antecesor Secure Sockets Layer (SSL; en español capa de puertos seguros) son protocolos criptográficos, que proporcionan comunicaciones securas por una red, comúnmente Internet. Más información: https://es.wikipedia.org/wiki/Transport_Layer_Security
- **WAF:** AWS WAF lo ayuda a protegerse de los exploits y bots web comunes que podrían afectar la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos. Más información: https://aws.amazon.com/es/waf/
- **RDS:** Amazon Relational Database Service (Amazon RDS) es una colección de servicios administrados que facilita las tareas de configuración, operación y escalado de una base de datos en la nube. Más información: https://aws.amazon.com/es/rds/

**EC2:** Amazon Elastic Compute Cloud (Amazon EC2) ofrece la plataforma de computación más amplia y completa. Más información: https://aws.amazon.com/es/rds/