



IT-SRE-CHALLENGE

ABRIL 2025



¡Bienvenido al desafío SRE de Yoizen!

Los siguientes ejercicios están diseñados para simular las tareas habituales del perfil que estamos buscando. Queremos que te sientas libre de demostrar tus habilidades y que puedas resolverlo con tu impronta.

La idea es que puedas resolver las siguientes consignas de manera teórica y/ práctica (puede ser un entorno virtual local o cloud), si te animás!

Entrega

- Tiempo de resolución: hasta 1 semana.
- Entrega en un documento o repositorio Git con README técnico, código, diagramas e instrucciones.
- No es necesario que estén resueltos todos los puntos; buscamos visualizar tu impronta y personalidad técnica frente a situaciones reales del día a día del perfil. Valoramos la sinceridad y la disposición a investigar lo que aún no se domina.
- Deberás poder defender tu solución y decisiones técnicas.

¡Mucho éxito! Este challenge es tu oportunidad para mostrar tus capacidades y sumarte a los proyectos de Yoizen.

1. Diseño y Despliegue de Infraestructura

Objetivo: Demostrar capacidad para definir, desplegar y documentar una arquitectura orientada a servicios productivos.

Requisitos:

- Diseñar y desplegar un entorno básico con 2 VMs (Linux o Windows), 1 contenedor Docker con un servicio web y 1 base de datos.
- Incluir segmentación de red o reglas de firewall que reflejen buenas prácticas.
- Automatizar el despliegue parcial o totalmente con Ansible o Terraform.
- Documentar: diagrama de arquitectura, configuraciones de red, firewall o DNS.

2. Monitoreo y Seguridad

Objetivo: Validar experiencia con herramientas de observabilidad y seguridad.

Requisitos:

- Implementar monitoreo usando Prometheus, Grafana, Zabbix o Wazuh.
- Crear al menos 2 dashboards o alertas (una de disponibilidad y otra de errores/rendimiento).
- Documentar: métricas, configuración de alertas, capturas de dashboards.

3. Scripting y Resolución de Incidente

Objetivo: Evaluar capacidad de automatizar tareas y actuar ante incidentes.

Requisitos:

- Crear un script (Bash, PowerShell o Python) para automatizar una tarea típica (reinicio, limpieza, verificación de conectividad, etc.).
- Resolver un caso simulado a partir de logs o archivos con errores. Documentar causa raíz y solución.

4. Automatización de tareas en máquinas virtuales

1. Suponiendo que existe una aplicación web hosteada en un servidor IIS ejecutando sobre Windows Server.

La aplicación genera un volumen considerable de logs en el path "E:\Web Example\logs", y a su vez IIS tiene habilitados sus logs en el path "C:\inetpub\logs\LogFiles\W3SVC1".

Describe qué herramienta(s) utilizarías para automatizar tareas que aseguren:

- La depuración periódica de logs.
- El reinicio del servicio web en caso de que deje de responder.
- 2. ¿Podrías incluir un ejemplo de cómo resolverías ambas tareas (script, programación de tarea, etc.)?
- 3. ¿Qué configuraciones de seguridad considerarás más relevantes de aplicar en un entorno como el descrito? Incluí aspectos tanto del sistema operativo como del servicio web.

5. Troubleshooting y gestión de incidentes

1. Durante un pico de tráfico, varios usuarios reportan que una aplicación deja de responder. Desde el monitoreo se observan tiempos de respuesta elevados y uso alto de CPU en la VM Linux. ¿Qué pasos seguirías para diagnosticar y mitigar el problema?
2. ¿Qué herramientas o comandos utilizarías para validar que el servicio sigue funcionando correctamente a nivel de red, sistema operativo y aplicación?

6. Seguridad y cumplimiento

1. Como parte del proceso de certificación ISO 27001, ¿qué controles básicos implementarías en tu infraestructura para cumplir con los requerimientos de gestión de accesos y segmentación de red?
2. ¿Cómo auditarías y reportarías vulnerabilidades en máquinas Linux y Windows?

7. Automatización y despliegue

1. Describí brevemente cómo integrarías Ansible o Terraform en un pipeline CI/CD para automatizar el despliegue de infraestructura. ¿Qué buenas prácticas aplicarías?
2. En un entorno mixto (Linux/Windows), ¿qué desafíos has enfrentado para mantener la consistencia y seguridad en automatizaciones?

8. Diagnóstico de alerta en Windows

Supongamos que recibís una alerta crítica desde el sistema de monitoreo:

"Windows: High swap space usage (less than 20% free)".

1. ¿Cómo abordarías el diagnóstico y resolución de este incidente?
2. ¿Qué herramientas y acciones aplicarías para mitigar el problema y prevenir su recurrencia?

9. Troubleshooting de redes

1. Un servicio desplegado en una VM de Azure no logra conectarse a una base de datos alojada en otra red virtual dentro de la misma suscripción.
¿Qué pasos seguirías para diagnosticar el problema de conectividad? Menciona herramientas, comandos y configuraciones que revisarías (firewalls, rutas, NSG, etc.).
2. Un usuario reporta que desde una máquina Linux no puede resolver el nombre de un dominio interno ('api.empresa.local'). ¿Cómo diagnosticarías y resolverías un posible problema de resolución DNS?
3. ¿Qué herramientas o comandos utilizas con frecuencia para diagnosticar problemas de red entre contenedores, VMs o nodos Kubernetes?