# 2. Agile SysAdmin: Networking and Systems Administration

Instructor: Julián García-Sotoca Pascual

# Securing and monitoring networks

# Índice

- Seguridad y monitorización de redes
  - Seguridad Local (Hardening)
  - Monitorización
  - Alta disponibilidad

# Índice

- Seguridad y monitorización de redes
  - **Seguridad Local (Hardening)**
  - Monitorización
  - Alta disponibilidad

# Seguridad Local

- Basándose en las guías de CIS (Center for internet Security) describiremos las medidas básicas de seguridad a nivel local
  - https://www.cisecurity.org/cis-benchmarks/
- En función del tipo de máquina se definen varios perfiles:
  - Nivel 1 - Servidor: intenta aplicar medidas prácticas y prudentes que aporten claramente un beneficio
  - Nivel 2 - Servidor: extiende el perfil anterior para casos donde la seguridad deba ser una prioridad


# Seguridad Local

- Recomendaciones referentes a Filesystems
  - Separar los directorios que tienen un uso global por el sistema en particiones separadas (/boot, /usr, /bin, /var, /var/tmp, /var/log)
  - Separar los directorios de usuarios en particiones separadas con opciones de montaje más estrictas (/home)
  - Deshabilitar los módulos de filesystems que no se usen
  - Separar el directorio /tmp en otro filesystem y montarlo con las opciones nodev, nosuid, noexec, (también el /var/tmp)
  - Asegurarse de que el Sticky bit está activo en todos los directorios donde todo el mundo puede escribir

# Seguridad Local

- Sticky bit
  - La activación del sticky bit previene la capacidad de borrar o renombrar ficheros en directorios donde todos los usuarios tienen permisos de escritura y de los cuales otros usuarios son propietarios.

# Seguridad Local

- Setuid y setguid:
  - Permite a un usuario ejecutar con los permisos de otro usuario
  - Ejemplo el comando passwd
  - https://linoxide.com/how-tos/stickbit-suid-guid/

find / -perm -4000 -exec ls -ld {} \; 2>/dev/null → suid
find / -perm -2000 -exec ls -ld {} \; 2>/dev/null → sgid
find / -perm -1000 -exec ls -ld {} \; 2>/dev/null → Sticky bit

# Seguridad Local

# Seguridad Local

Efectos de permisos especiales en archivos y directorios:

- Permiso especial: u+s (suid)
  - Efecto en Archivos: el archivo se ejecuta como el usuario propietario del archivo, no el que ejecutó el archivo
  - Efecto en directorios: sin efecto
- Permiso especial: g+s (sgid)
  - Efecto en archivos: el archivo se ejecuta como el grupo que posee el archivo
  - Efecto en directorios: los archivos recién creados en el directorio tienen su propietario de grupo configurado para que coincida con el propietario del grupo del directorio
- Permiso especial: o+t (sticky)
  - Efecto en archivos: sin efecto
  - Efecto en directorios:: los usuario con acceso de escritura al directorio sólo pueden eliminar los archivos que les pertenecen; no pueden eliminar o forzar el guardado de archivos de propiedad de otros usuarios

# Seguridad Local

- Recomendaciones referente a Actualizaciones:
  - Dependiendo de la organización y el número de máquinas o entornos la política de actualizaciones variará
  - Se debe asegurar que los repositorios están configurados
  - Asegurarse de que las claves GPG están configuradas

# Seguridad Local

- Implementación de mecanismos de chequeo de integridad:
  - Herramientas que permiten detectar cambios no autorizados en los ficheros de configuración
  - Se recomienda tener instalado AIDE (disponible en la mayoría de distribuciones)
  - Además se debe programar periódicamente el chequeo de integridad

# Seguridad Local

- Securización del arranque:
  - Asegurarse de que los ficheros de configuración de grub solo los puede leer root ya que pueden almacenar contraseñas
  - Se recomienda también proteger el bootloader con contraseña para que no se puedan modificar las opciones de arranque
  - Habilitar la contraseña en el arranque en modo de recuperación

# Seguridad Local

- MAC - Mandatory Access Control (SELinux o AppArmor)
  - SELinux proporciona un sistema MAC donde cualquier llamada de sistema es denegada a no ser que se haya permitido específicamente
  - Lo recomendado es tener SELinux o AppArmor habilitado y en modo “Enforcing”, pero es complicado de configurar y puede traer problemas

# Seguridad Local

- Banners
  - Los ficheros /etc/motd, /etc/issue y /etc/issue.net se encargan de presentar mensajes a los usuarios que se conectan
  - No deben presentar demasiada información que pueda ayudar a un atacante a identificar el sistema
  - Estos ficheros deben tener permisos 644.

# Seguridad Local

- Servicios
  - Se deben deshabilitar los servicios que no son requeridos para la operación normal del sistema
  - No se deben utilizar servicios que transmitan información sin encriptar
  - Asegurarse de que está habilitado algún servicio de sincronización de tiempo

# Seguridad Local

- Configuración de red
  - Forwarding y redirección de paquetes en sistemas que no necesiten funcionar como un router
  - Parámetros de red en sysctl
  - IPv6 debe estar deshabilitados donde no sea necesario
  - Firewall:  habilitar algún mecanismo de filtrado de paquetes como iptables, UFW o Firewalld y que la política por defecto sea DENY

# Seguridad Local

- Logging y auditoría
  - Uso de rsyslog para el envío de los logs en la máquina local o reenviarlos a una máquina remota
  - Auditd permite la monitorización de intentos de intrusión y otros comportamientos sospechosos
  - Asegurarse de configurar una retención adecuada

# Índice

- Seguridad y monitorización de redes
  - Seguridad Local (Hardening)
  - **Monitorización**
  - Alta disponibilidad

# Monitorización

- Debería estar diseñada para detectar los precursores de una falla en tiempo para poder actuar antes de que ocurra

# Monitorización

- Terminología
  - **Medición** → el dato ( 0, 15, -5, “5.4.3”)
  - **Métrica** → medición, con nombre y timestamp
  - **Frecuencia** de medición → cada cuanto tiempo se toman las métricas. En función de la métrica
  - **Perspectiva** de monitorización → ubicación de la herramienta de monitorización. Determinadas métricas varían en función de la perspectiva

# Monitorización

- Usos
  - Visualización/Dashboards → disponer de múltiples métricas en una única pantalla
  - Tendencias → dirección de la serie de medidas de una métrica
  - Alertas → llamar la atención de alguien ante situaciones que pueden derivar en fallo

# Monitorización

- Usuarios:
  - Equipos de operaciones: detectan los fallos y actuan para resolverlos
  - Equipos de QA: análisis de tendencias y variabilidad
  - Gestión de Capacidad: predecir el uso de recursos en el futuro
  - Product Managers: métricas de negocio

# Monitorización

- Usuarios:

| | |
|---|---|
| Operational Health/Response (OH) | |
| (R+, L+, D+) | High resolution, low latency, high diversity. System health. The things we get paged about. |
| Quality Assurance/SLA (QA) | |
| (R+, L−, D+) | High resolution, high latency, high diversity. Longer-term analysis of jitter, latency, and other quality-related factors. |
| Capacity Planning (CP) | |
| (R−, L−, D+) | Low resolution, high latency, high diversity. Forecasting and purchasing more resources. |
| Product Management (PM) | |
| (R−, L−, D−) | Low resolution, high latency, low diversity. Determining the number of users, cost, and other resources. |

The Practice of Cloud System ADministration, Designing and operating large distributed systems Volume 2.
Thomas A. Limoncelli, strata R. Chanlup, Christina J. Hogan
Addison-Wesley

# Monitorización

- ¿qué monitorizar?
  - Disponibilidad
  - Latencia
  - Estabilidad del backend
  - User experience
  - Finanzas

# Monitorización

- Según Google, las 4 señales de oro son:
  - **Latencia**: tiempo que se tarda en servir una petición, tanto las peticiones correctas como las que devuelven error
  - **Tráfico**: cuanta demanda tiene el sistema
  - **Errores**: tasa de peticiones que fallan
  - **Saturación**: cómo de “lleno” está el servicio

# Monitorización

- Los mecanismos de monitorización se pueden categorizar en:
  - Blackbox vs Whitebox → blackbox las medidas pretenden emular un usuario. En whitebox las medidas se hacen a más bajo nivel
  - Medidas directas o sintetizadas (agregadas):
  - Tasas vs Capacidad: si la frecuencia de eventos es alta interesan medidas de tasas, si la frecuencia de eventos es baja intesa saber que el sistema puede realizar cierta función
  - Medidores vs Contadores: valor instantáneo o medida que únicamente incrementa

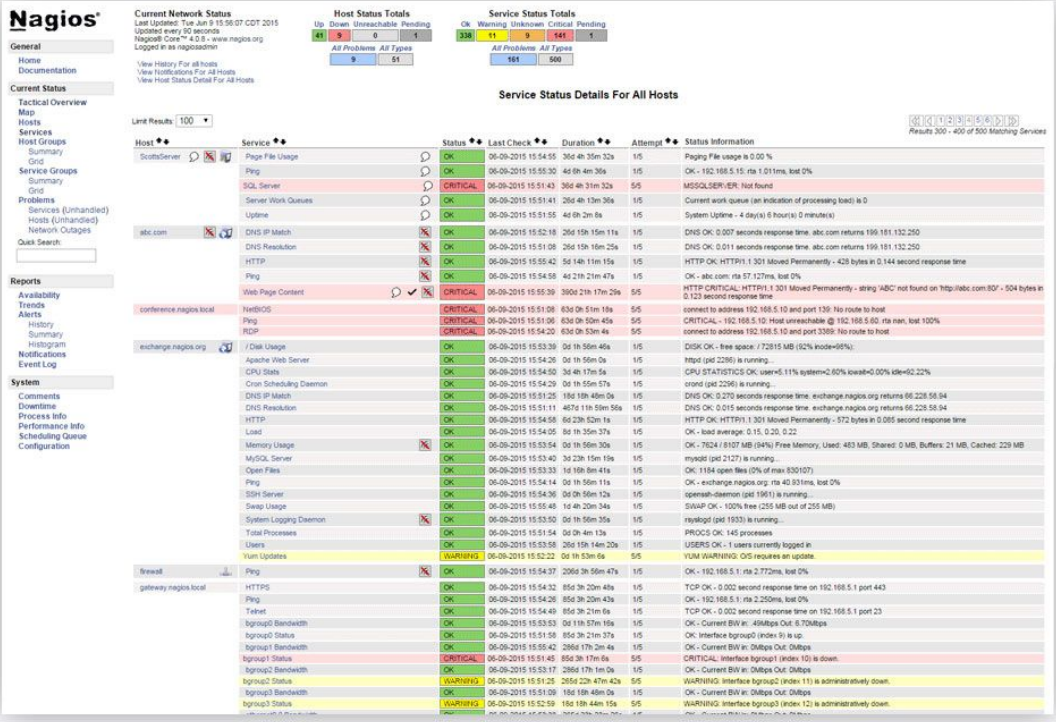
# Monitorización

- En función de los mecanismos de recolección, también tenemos varios tipos de sistemas:
  - Push vs Pull: con Push el sensor que toma la medida la transmite al servidor de monitorización, mientras que con Pull el servidor es el que consulta al agente y almacena el dato
  - Protocolo: SNMP o JSON over HTTP
  - Servidor vs agente vs poller
  - Centralizado o distribuido

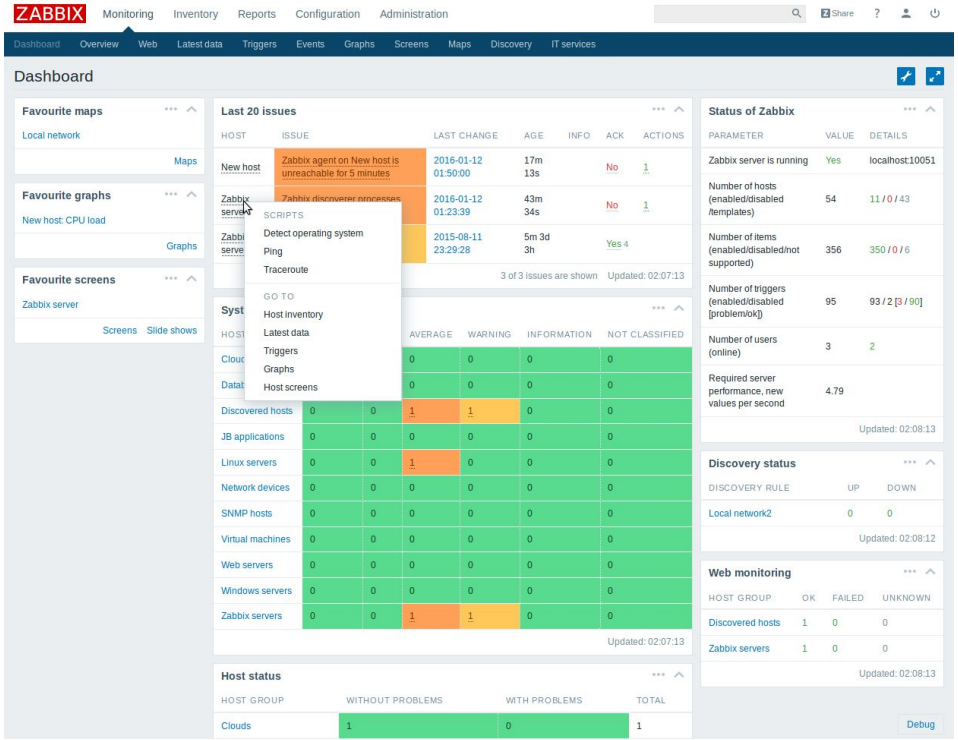
# Monitorización

- Ejemplos:
  - Nagios
  - Zabbix
  - LibreNMS
  - Prometheus
  - ELK
  - Grafana

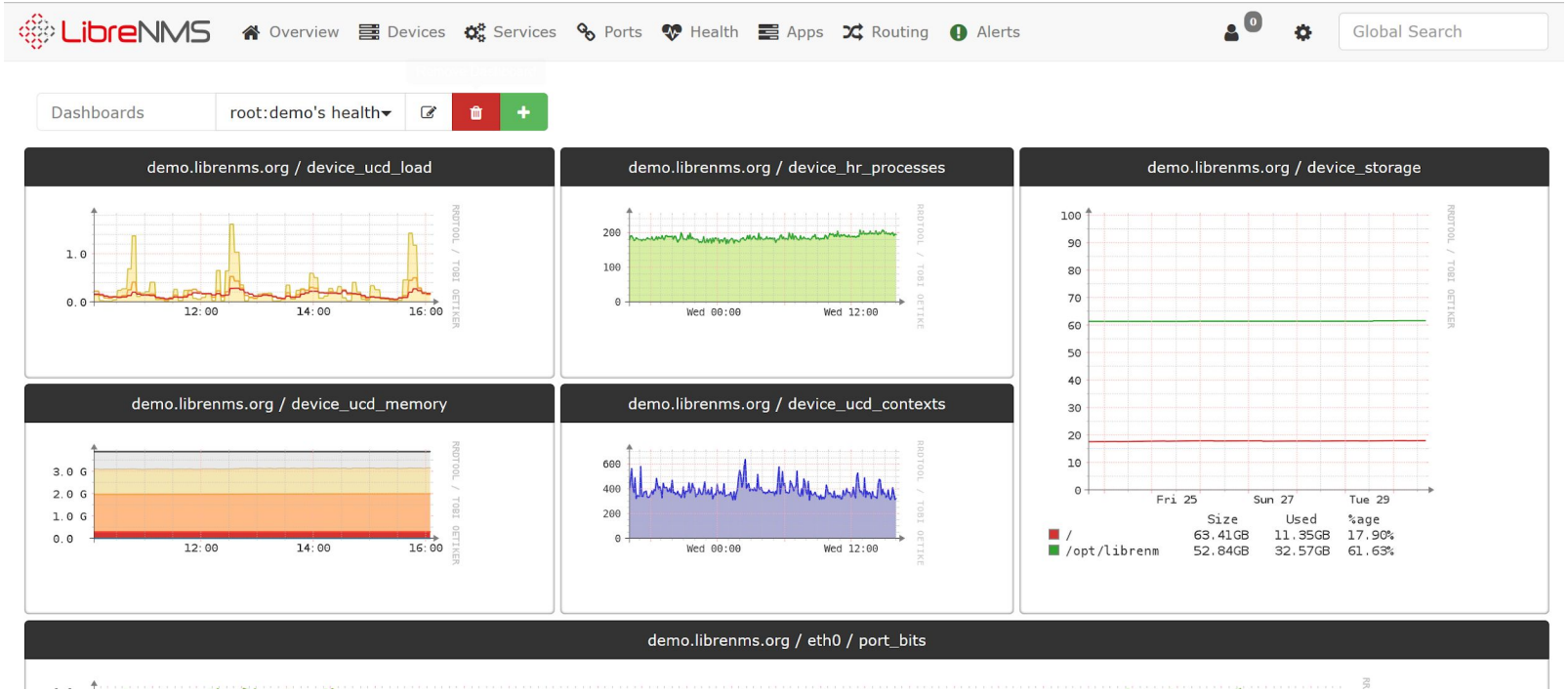
# Monitorización



# Monitorización



# Monitorización



# Monitorización

# Índice

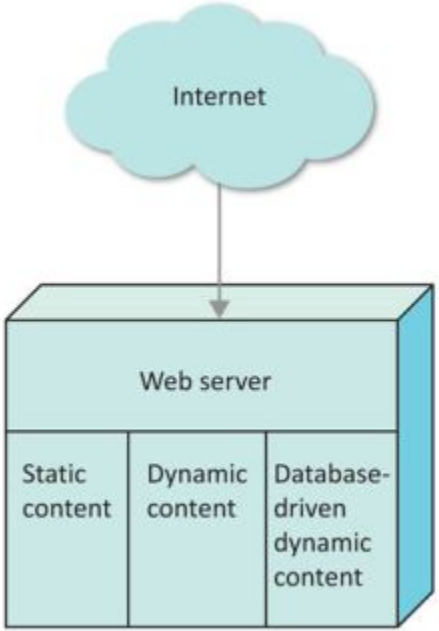
- Seguridad y monitorización de redes
  - Seguridad Local (Hardening)
  - Monitorización
  - **Alta disponibilidad**

# Alta Disponibilidad

- Diseños pensados en la resiliencia:
  - Resiliencia: capacidad de un sistema para lidiar con fallas
- Terminología:
  - Outage
  - Falla
  - Malfuncionamiento
  - Servicio
  - QPS
- Capacidad sobrante → spare capacity
- Load Sharing vs Hot Spares

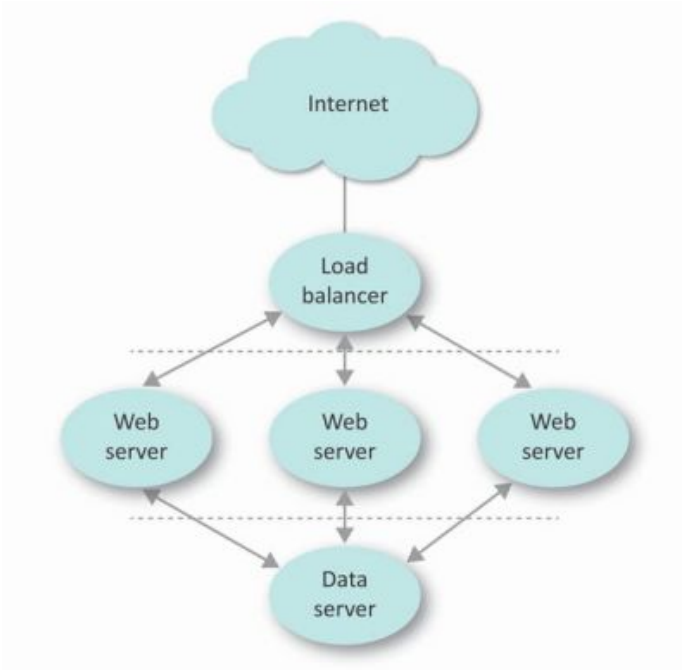
# Alta Disponibilidad

- Único servidor web



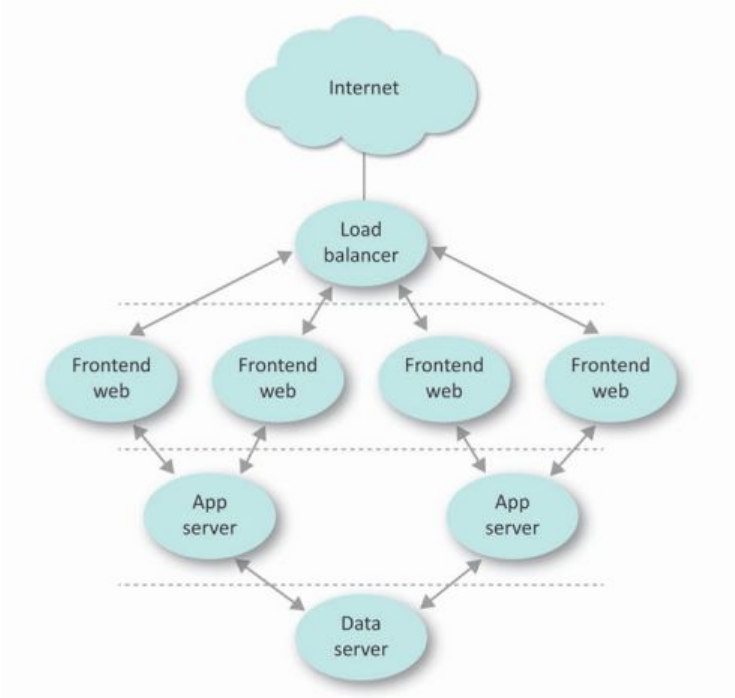

# Alta Disponibilidad

- Servicio web Tier-3




# Alta Disponibilidad

- Servicio web Tier-4

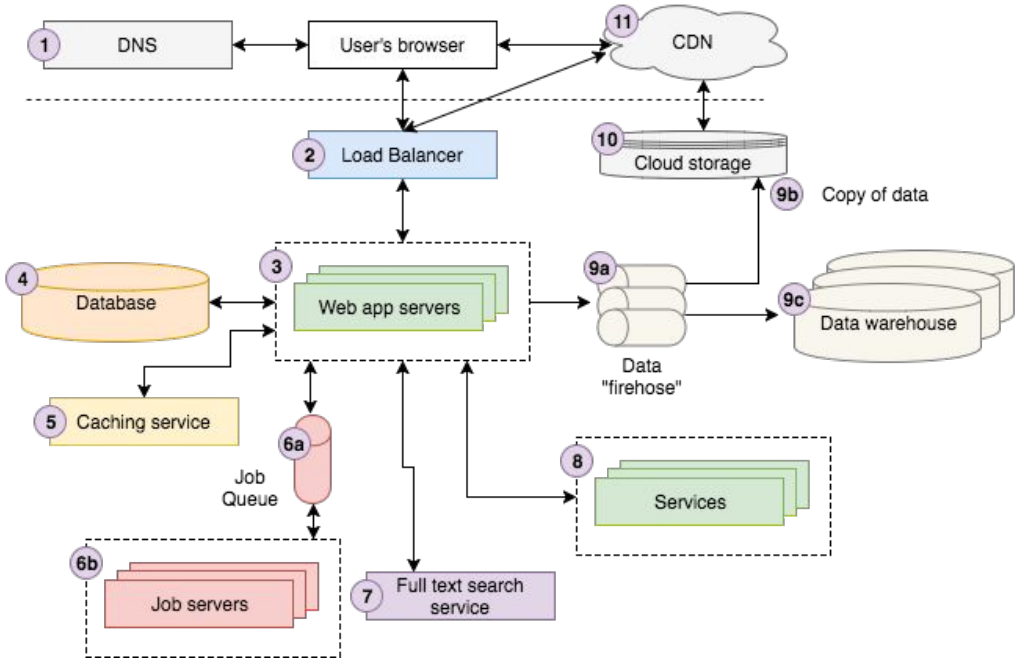



# Alta Disponibilidad

- Patrones de diseño para escalar
  - Identificar cuellos de botella
  - Escalado: escalado horizontal (nº de máquinas) o vertical (máquinas más grandes)
  - Service Splits → microservicios
  - Cacheo: persistencia, algoritmos de reciclaje, tamaño
  - Particionado (sharding)
  - Colas → Kafka
  - CDN

# Alta Disponibilidad

- Ejemplo real:
  - https://engineering.videoblocks.com/web-architecture-101-a3224e126947



# Alta Disponibilidad

- Ejemplos de soluciones de alta disponibilidad:
  - HAproxy → http://www.haproxy.org/
  - Patroni → https://github.com/zalando/patroni
  - Keepalived → https://www.keepalived.org/

# ¿Preguntas?

# GRACIAS

www.keepcoding.io